Confidence in the Connected World

Center for Internet Security®

CIS Controls™

Version 7

CIS Controls Mobile Companion Guide

Contents

Acknowledgments

CIS® (Center for Internet Security, Inc.®) would like to thank the many security experts who volunteer their time and talent to support the CIS Controls™ and other CIS work. CIS products represent the effort of a veritable army of volunteers from across the industry, generously giving their time and talent in the name of a more secure online experience for everyone.

Editors: Sean Frazier, Duo, and Joshua M Franklin, CIS

Contributors:

Tim LeMaster, Lookout
Angelos Stavrou, Kryptowire
Paul Campbell, Whitepages
Tyler Desjardins, CISSP , Blackberry
Stephen Campbell, Non-State Threat Intelligence, LLC
Joseph Martella, American Airlines
Jenifer Bauer, Now Secure
Phil Langlois, CIS
Jordan Rakoske, CIS
Robin Regnier, CIS

Introduction

The CIS Controls™ are a prioritized set of actions that collectively form a defense-in-depth set of best practices that mitigate the most common attacks against systems and networks. The CIS Controls are developed by a community of information technology (IT) experts who apply their first-hand experience as cyber defenders to create these globally accepted security best practices. The experts who develop the CIS Controls come from a wide range of sectors including retail, manufacturing, healthcare, education, government, defense, and others. So, while the CIS Controls address the general practices that most organizations should take to secure their systems, some operational environments may present unique requirements not addressed by the CIS Controls.

The Center for Internet Security, Inc. (CIS) is a 501(c)(3) nonprofit organization whose mission is to identify, develop, validate, promote, and sustain best practices in cybersecurity; deliver world-class cybersecurity solutions to prevent and rapidly respond to cyber incidents; and build and lead communities to enable an environment of trust in cyberspace.

For additional information, go to https://www.cisecurity.org/

The security challenges facing the usage of mobile devices in the enterprise are an example where additional attention is warranted. While many of the core security concerns of enterprise IT systems are shared by mobile devices and their management systems, unique challenges do exist. For instance, mobile devices leave the physical and logical boundaries defined by an organization where normal workstations are maintained. The small form factor of a mobile device makes device loss or theft a real concern, especially when these devices store proprietary and sensitive enterprise information that may also be governed by additional regulations (e.g., healthcare data). Although mobile devices are not the only type of device that generally transcends the traditional enterprise network boundary (e.g., laptops), users frequently connect phones and tablets to unsafe networks, perform work tasks, and then bring the device back to the enterprise. Many devices automatically connect to unsafe networks without the user's knowledge, are exposed to unsafe environments, and are then brought back into the enterprise. Finally, users generally feel empowered to install mobile applications that a system administrator may have no knowledge of, yet will need to defend against.

System administrators provisioning, configuring, and monitoring mobile device usage often rely heavily upon centralized management technologies such as Enterprise Mobility Management (EMM) and Mobile Device Management (MDM). Many mobility management systems work to leverage the technologies built into mobile devices, and supplement this with their own proprietary approaches. System administrators face an important decision early on – how much control do they want users to have over these devices? A deployment model must be selected. Although requiring users to keep two phones on their person may be the easiest way to keep business information separate and secure, it is more expensive and reduces usability. Decreasing usability can lead to shadow IT. The Bring Your Own Device (BYOD) model is often attractive to both administrators and users as it is a quick way to get users access to the information they need to perform their job. But to properly secure this device usage model requires planning and the implementation of multiple layers of security defenses. BYOD also makes it easy to infringe upon user privacy, leading some employees to request two distinct devices. Often times, one model may not be chosen for an entire organization. Different employees will have different needs and tolerances for security, privacy, and ease of use. Supporting multiple models, alongside dealing with the legal and policy issues affecting BYOD, can be a headache.

Besides how devices are deployed (e.g., given to users), the apps that will be allowed to run on these devices are a major concern. Modern devices make it very easy to download and acquire new apps – in fact they actively encourage users to reach out and download apps. But downloading insecure or dangerous apps is a primary avenue for malware to infect a phone or tablet. The mobile application stores try to prevent malware within their stores, but cannot stop everything. Systems known as Mobile Threat Defense (MTD) can notify users and admins of dangerous apps as they are installed, and also detect attacks against the device itself. This technology can proactively help users make good security decisions about their devices, and the apps they install. MTD can also help to detect phishing emails and text messages, alongside dangerous sites that a user may unintentionally be visiting. MTD often is developed and sold by a company distinct from, but partnering with, an EMM company and is a natural complement to that technology.

Mobile devices and apps face unique attacks and security concerns, and differ from traditional IT environments. The overriding themes for applying security for mobile devices are device management and configuration alongside the practical usage of cryptography, and careful controls and policy around the installation and usage of mobile applications.

Methodology

A consistent approach is needed for analyzing CIS Controls in the context for mobile. For each of the 20 CIS Controls, the following information is provided:

- Applicability – The applicability field assesses the degree to which a CIS Control functions within the mobile space.
- Deployment Considerations – Deployment Considerations analyze if specific mechanisms are needed for a particular mobile deployment model, such as BYOD or Corporate Owned, Personally Enabled (COPE)
- Additional Discussion – This is a general area for any guidance that also needs to be noted. For instance, relevant tools, products, or threat information that could be of use can be placed here.

Relevant Enterprise Technology

The following section defines and describes the technology used to manage mobile devices.

- Enterprise Mobility Management (EMM) – In its simplest form, an EMM is an overarching term describing the plethora of systems available to manage, configure, track, and administer mobile devices in an enterprise. Oftentimes, MDM and Mobile Application Management (MAM) are components of an EMM. Security Information and Event Management (SIEM) and MTD commonly integrate with EMMs. EMM systems can have full (e.g., admin, privileged) or partial control of a device. The Apple® Device Enrollment Program (DEP) would be an example of a fully managed deployment scenario.
- Mobile Device Management (MDM) – MDMs are the administration application primarily used to configure devices and set policies for mobile devices. MDMs typically have an on-device application that acts as the enterprise's foothold on an employee's device. MDMs may come with a suite of applications, including a secure container.
- Secure Container – A secure container is a device-side mobile app that provides a secure working environment to store enterprise data and prevent access from third-party apps. These containers are a completely different technology from server-side containers such as Docker or Rocket. Secure containers can be deployed on managed or unmanaged devices, and often have multiple apps contained within them from the same developer, such as a browser or email client. Containers may be implemented at the application level or integrated into the operating system itself.
- Mobile Application Management (MAM) – MAM systems generally configure and manage mobile applications, and their focus rarely moves to the device itself. MAMs may integrate with an EMM, but may also be completely stand-alone solutions.
- Mobile Threat Defense – MTD is a form of mobile endpoint protection that generally identifies malware and attacks on the device. Additionally, they can be used to monitor links and messages for social engineering attacks or identify network-based attacks such as Secure Sockets Layer (SSL) / Transport Layer Security (TLS) stripping or Address Resolution Protocol (ARP) poisoning. The usefulness of MTD does vary from platform to platform with MTD providing maximum impact on Android.

Mobility Deployment Model Descriptions

Organizations can choose to utilize a variety of device deployment models. These models offer varying degrees of control and visibility to administrators and privacy to users. The technologies mentioned above can all be used within any scenario listed below. The mobile deployment model to select for an organization varies based on risk appetite and job function. Other relevant factors to the decision include data sensitivity, who ultimately owns the device, and the degree of separation necessary between enterprise and user data. It is possible that hybrid deployments will be necessary, giving some users a greater degree of latitude based on their job function. Apple and Google both provide detailed guidance on managing their products. There are a large number of possible deployment models, but some of the more popular ones are:

- Unmanaged – Administrators can provide access to enterprise services, such as email, contacts, and calendar, to employee users without inspecting the device. Although a popular model for small companies and startups, this is the most dangerous scenario in terms of enterprise risk and it should be avoided.
- Bring Your Own Device (BYOD) – Devices are owned by the end-user, or employee, but occasionally are used for work purposes. These devices should be permitted the least access to organization resources. BYOD devices could be joined directly to an MDM with end-user consent, but are more often managed through a mail and calendaring system such as Exchange ActiveSync. Access from BYOD devices to organizational resources

should be strictly controlled and limited. Common controls such as encryption and a passcode should be enforced. Employees own the device and can expect access to their organization's enterprise with little to no limitations on their overall device capabilities. In some situations depending on the sensitivity of an organization's data and the threat environment, BYOD can be safely achieved with a secure container.

- Corporate Owned, Personally Enabled (COPE) – COPE devices work in a similar fashion to BYOD, except the organization owns and furnishes the mobile device. Restrictions will be applied to the device but generally do not prevent most of what the user intends to do with the device. Although a COPE device is personally enabled, it ultimately belongs to the enterprise – *as does the information on the device*. These devices should be joined directly to an MDM with applications and access provisioned according to the user's role. Additionally, containerization can be employed to separate the work and personal areas of the device. Despite containerization, automatic updating of both operating systems (OS) and applications should be enforced to the extent possible.
- Fully managed – Devices within this deployment scenario are typically locked down and only permitted to perform business functions. Fully managed devices are often owned by the organization as are all data residing on the device, necessitating that employees have a second device for personal use. These devices are often heavily centrally managed, which provides important security benefits but also presents usability barriers to employees. Devices owned and distributed for solely work purposes should be both the most controlled and most trusted devices. These devices should be provisioned directly to an EMM before a user has the device, and access provisioned according to the user's role. Automatic updating of both OS and applications should be enforced to the extent possible, and the user should not be able to install unapproved software.

Definition and Scope

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4 defines a mobile device as:

> *"A portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the devices to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smartphones, tablets and e-readers*."

The Cloud Security Alliance Mobile Working Group defines mobile computing as:

> "A *very broad term which can be used to define any means of using a computer while outside of the corporate office. This could include working from home or on the road at an airport or hotel. The means to perform mobile computing could include kiosks used to remotely connect to the corporate office, home computers, laptops, tablets or smartphones. Specialized or integrated devices could also be considered as mobile computing devices*."

Both definitions are fairly broad and encompasses a plethora of systems within their umbrella including smartphones and tablets. Ultimately, this document defines mobile devices as distinct from the Internet of Things (IoT). Laptops, specifically 2-in-1 laptops, bridge the divide between traditional enterprise systems and tablets. Enterprises must choose whether these systems fall within the definition of mobile. It may be best to draw the distinction at whether a system can be managed by an EMM.

V7

Basic

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

Foundational

7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

Organizational

17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

Applicability Overview

More than 60% of CIS Sub-Controls Apply
Between 60% and 0% of the CIS Sub-Controls Apply
0%

Control	CIS Control Title	Applicability
1	Inventory and Control of Hardware Assets	
2	Inventory and Control of Software Assets	
3	Continuous Vulnerability Management	
4	Controlled Use of Administrative Privileges	
5	Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers	
6	Maintenance, Monitoring and Analysis of Audit Logs	
7	Email and Web Browser Protections	
8	Malware Defenses	
9	Limitation and Control of Network Ports, Protocols, and Services	
10	Data Recovery Capabilities	
11	Secure Configuration for Network Devices, such as Firewalls, Routers and Switches	
12	Boundary Defense	
13	Data Protection	
14	Controlled Access Based on the Need to Know	
15	Wireless Access Control	
16	Account Monitoring and Control	
17	Implement a Security Awareness and Training Program	
18	Application Software Security	
19	Incident Response and Management	
20	Penetration Tests and Red Team Exercises	

CIS Control 1: Inventory and Control of Hardware Assets

Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

Mobile Applicability

It is important to track which systems have access to the network and are accessing data and organizational resources, and mobile devices are no different. Similar to traditional workstations, insecure mobile devices can be used as a foothold within an enterprise network as a way to pivot to other devices. This creates unique challenges for mobile devices as they are not perpetually attached to the corporate network like other IT systems. They may be connected for part of a day, gone for a week, or periodically checked-in when a virtual private network (VPN) is enabled. This necessitates using different methods to maintain the hardware asset inventory.

Mobile Deployment Considerations

All deployment models require hardware asset tracking. Organizations may wish to consider additional asset tracking mechanisms for BYOD devices. BYOD devices are sufficiently difficult to track that the *CIS Controls Version 7* document specifically calls out BYOD as presenting unique challenges. One reason is due to high device turnover. Devices should be tracked alongside their deployment model (e.g., BYOD) and detailed device type.

Mobile Additional Discussion

Typical asset tracking tools may not work out of the box with mobile devices. In order to obtain this feature, an additional plugin or purchase may be necessary. Mobile devices will respond to Network Mapper (Nmap) scans but not always in a reliable or useful manner. Tracking media access control (MAC) addresses can be difficult due to the MAC address randomization built into some mobile devices, which helps to protect a user's privacy on the network. Unfortunately this feature can also actively prevent hardware asset management tools from properly tracking the device. At the very least, organizations can procedurally make a listing of mobile device hardware, device type, serial number, phone number, and other relevant information. All of that information can be tied to an individual user account.

Organizations may use email accounts, or ActiveSync, to determine which mobile devices are used to access email. Email is one of the most popular enterprise use cases for mobile devices. Also, EMMs can support hardware asset tracking by installing agents on the mobile devices to push down configurations and security profiles, monitor devices for configuration changes, and monitor private access controls based on policy. Privileged EMM agents can obtain and report fairly detailed hardware configuration information back to the enterprise that can be obtained via the primary EMM console. Device location via Global Positioning System (GPS) can also be tracked within an EMM, but this can infringe on a user's privacy. The EMM console may be able to integrate with an organization's primary asset management platform.

CIS Control 1: Inventory and Control of Hardware Assets			Applicability	
Sub-Control	Control Title	Control Descriptions	Included	Justification
1.1	Utilize an Active Discovery Tool	Utilize an active discovery tool to identify devices connected to the organization's network and update the hardware asset inventory.	•	Although active discovery tools may not always work perfectly for mobile devices, they can generally be upgraded and further configured in order to function as needed. A better path forward for active discovery would be to place an EMM or other application onto the device to obtain hardware inventory and other useful enterprise information.
1.2	Use a Passive Asset Discovery Tool	Utilize a passive discovery tool to identify devices connected to the organization's network and automatically update the organization's hardware asset inventory.	•	A passive asset discovery tool would likely be suboptimal, but still provide useful information for mobile devices.
1.3	Use DHCP Logging to Update Asset Inventory	Use Dynamic Host Configuration Protocol (DHCP) logging on all DHCP servers or IP address management tools to update the organization's hardware asset inventory.	•	Mobile devices may not always respond in a similar and predictable manner as traditional workstations, but this can still be a useful Sub-Control to track devices. Although this is possible, it is not considered an industry-accepted method of tracking mobile device inventory and should not be the primary method in which mobile devices are tracked.

CIS Control 1: Inventory and Control of Hardware Assets			Applicability	
Sub-Control	Control Title	Control Descriptions	Included	Justification
1.4	Use DHCP Logging to Update Asset Inventory	Use Dynamic Host Configuration Protocol (DHCP) logging on all DHCP servers or IP address management tools to update the organization's hardware asset inventory.	•	This Sub-Control ensures that mobile devices never intended to be connected to the enterprise network, or only connected to an internal non-internet connected network, are still properly tracked.
1.5	Maintain Asset Inventory Information	Ensure that the hardware asset inventory records the network address, hardware address, machine name, data asset owner, and department for each asset and whether the hardware asset has been approved to connect to the network.	•	Unique information about a device can be tracked such as the International Mobile Equipment Identifier (IMEI).
1.6	Address Unauthorized Assets	Ensure that unauthorized assets are either removed from the network, quarantined, or the inventory is updated in a timely manner.	•	Unknown mobile devices connected to enterprise assets should be quickly removed via an approved process. Devices as well as authorized services should be addressed, such as logging into an email account on an unauthorized device.
1.7	Deploy Port Level Access Control	Utilize port level access control, following 802.1x standards, to control which devices can authenticate to the network. The authentication system shall be tied into the hardware asset inventory data to ensure only authorized devices can connect to the network.	•	Both Android and internet operating system (iOS) support port level access control.
1.8	Utilize Client Certificates to Authenticate Hardware Assets	Use client certificates to authenticate hardware assets connecting to the organization's trusted network.	•	Both Android and iOS contain certificate storage locations that can store and use a digital certificate to support 802.1x. These are most often provisioned in person by an IT administrator using some form of EMM.

CIS Control 2: Inventory and Control of Software Assets

Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that all unauthorized and unmanaged software is found and prevented from installation or execution.

Mobile Applicability

Software assets to be tracked include a mobile device's firmware, OS, and apps. Mobile OS are tailor-made for smartphones and tablets, but still leverages firmware from a variety of sources in order to enable peripherals and sensors. Expanding to the larger mobile ecosystem, there are millions of mobile applications available for download and install across the mobile platforms. Although the Apple's App Store and Google's Play Store often screen mobile apps for security issues, their application vetting mechanisms are not foolproof. Additionally third-party or jailbroken / cracked mobile appstores exist that users may download apps from. Regardless of their provenance, mobile apps from any source can threaten the security of enterprise data and credentials. Being able to know what is installed, and which version, is important to protect the organization. Outdated firmware and software often contain exploitable vulnerabilities that an attacker could leverage to access enterprise data.

Mobile Deployment Considerations

BYOD deployments using a secure container application may be unable to obtain versioning information for installed apps without administrative access. A secure container alone may be insufficient. Within iOS, unprivileged applications cannot read the listing of apps on a device. An EMM / MDM with an agent installed on the device is necessary to obtain both a listing of apps, and app version information. An EMM agent will also be able to provide detailed operating system information. On Android, an MTD application will be able to obtain the necessary information.

There are privacy considerations in BYOD scenarios, as the company may not need to know which apps an individual has installed on their personal device for personal use.

Mobile Additional Discussion

Mobile devices have firmware and software running across the device stack. It can be difficult to obtain baseband and other firmware information and this will likely be untracked by an enterprise. Operating system versions can be more easily tracked via network scanning but the results of these tools on mobile devices are not necessarily trustworthy or accurate. Obtaining specific application version numbers can be difficult as the OS sandbox works to prevent apps from obtaining information about each other. EMM / MDM tools can inventory apps and alert an administrator when an unauthorized app is installed.

Tracking OS and application versions of Bluetooth and wireless fidelity (WiFi) devices can be quite difficult and may not be possible using traditional scanning methods. Applications like Airmon for WiFi devices and hcitool or ubertooth-scan for Bluetooth devices will at best provide broadcast advertisements and MAC addresses. Note that for Bluetooth devices, MAC addresses do not conform to typical conventions and are often represented as the device WiFi MAC address incremented by 1 bit.

Whitelisting is a built-in capability on iOS and Android, but this is only for mobile apps. It is not extended to external software libraries and scripts. On Apple iOS, applications are digitally signed

with that signature checked on install. With Google Android, apps are digitally signed but the signature might not necessarily be checked. Additional information is available via the Android Developer Page on Application Signing and within Apple's iOS Security Guide.

CIS Control 2: Inventory and Control of Software Assets			Applicability	
Sub-Control	Control Title	Control Descriptions	Included	Justification
2.1	Maintain Inventory of Authorized Software	Maintain an up-to-date list of all authorized software that is required in the enterprise for any business purpose on any business system.	•	At the bare minimum, mobile device operating system and application information should be tracked. This is most easily done if an enterprise has a presence on the mobile device via an EMM or similar technology.
2.2	Ensure Software Is Supported by Vendor	Ensure that only software applications or operating systems currently supported and receiving vendor updates are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.	•	Some EMMs have the capability to alert administrators if an app is out-of-date or no longer supported. MTD agents may also have this capability. A mobile application vetting process can also assist with this, as detailed in this document under CIS Control 18.
2.3	Utilize Software Inventory Tools	Utilize software inventory tools throughout the organization to automate the documentation of all software on business systems.	•	EMMs act as a software inventory tool to help track and coordinate mobile devices with enterprise access.
2.4	Track Software Inventory Information	The software inventory system should track the name, version, publisher, and install date for all software, including operating systems authorized by the organization.	•	Tracking this level of detail may be difficult, and some systems may only allow you to track real-time inventory data, not historical information.

CIS Control 2: Inventory and Control of Software Assets			Applicability	
Sub-Control	Control Title	Control Descriptions	Included?	Justification
2.5	Integrate Software and Hardware Asset Inventories	The software inventory system should be tied into the hardware asset inventory so all devices and associated software are tracked from a single location.	•	EMMs generally do this by default, but this information is not often easily integrated with external asset tracking systems for traditional workstations and networking equipment. Unified Endpoint Management (UEM) software can help to bridge that gap, tracking both traditional IT systems and mobile devices within the same application.
2.6	Address Unapproved Software	Ensure that unauthorized software is either removed or the inventory is updated in a timely manner.	•	Software that is not approved by the enterprise should be removed. Doing this in an automated fashion is most realistic in fully managed scenarios.
2.7	Utilize Application Whitelisting	Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets.	•	The major mobile operating systems generally perform some degree of application whitelisting by default. This can be subverted by malicious MDM profiles or insecure system settings. Malicious MDM profiles can trick a user into providing access to an unauthorized entity or allow the installation of dangerous applications. Insecure OS settings, such as the "Allow Unknown Sources" on Android, can allow for the installation of dangerous and insecure apps.
2.8	Implement Application Whitelisting of Libraries	The organization's application whitelisting software must ensure that only authorized software libraries (such as *.dll, *.ocx, *.so, etc.) are allowed to load into a system process.		Whitelisting individual libraries is typically not available on a mobile OS, as the OS typically whitelists at the application level.
2.9	Implement Application Whitelisting of Scripts	The organization's application whitelisting software must ensure that only authorized, digitally signed scripts (such as *.ps1, *.py, macros, etc.) are allowed to run on a system.		Whitelisting individual scripts is typically not available on a mobile OS, as the OS typically whitelists at the application level.

CIS Control 2: Inventory and Control of Software Assets			Applicability	
Sub-Control	Control Title	Control Descriptions	Included?	Justification
2.10	Physically or Logically Segregate High Risk Applications	Physically or logically segregated systems should be used to isolate and run software that is required for business operations but incurs higher risk for the organization.	•	Systems like Samsung KNOX or Android for Work / Android Enterprise can provide low-level enforcement of logical separation. A secure container is most often another application that runs under a separate user and provides less logical segregation than the aforementioned strategy. Turned to the highest degree, a separate, fully managed phone can be a form physical segregation.

CIS Control 3: Continuous Vulnerability Management

Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.

Mobile Applicability

Mobile vulnerabilities are often linked to versions of the mobile OS or apps installed on the device. Misconfigurations of the mobile OS or installed apps are also within the scope of this CIS Control. Since mobile devices are not always attached to the corporate network, it is difficult to identify and manage vulnerabilities in a manner similar to how one would on desktop workstations, servers, or network appliances. Traditional vulnerability management products may not act in a predictable manner unless the products are specifically geared toward mobile. These traditional tools often require additional plugins that must be separately purchased to enable mobile device vulnerability scanning. Separate products may exist for scanning the EMM and MDM systems and mobile devices themselves. Some vulnerability scanners may only function by directly integrating with an EMM for device access or may require an agent-based solution to be installed. Understanding the limitations and bounds of use for mobile device scanning is necessary before purchasing a product.

Mobile Deployment Considerations

Organizations may wish to utilize additional agent-based MTD tools with devices that are not provisioned into an EMM. Organizations with privileged access on the device can install agents that can access the name, and possibly developer, of each app installed on the device. In fully managed scenarios, these apps can be pushed and configured for the device. From a network scanning perspective, the deployment model does not make a difference.

Mobile Additional Discussion

Vulnerabilities and misconfigurations within mobile devices can apply to many layers of the device stack:

- Hardware – Such as within a processor improperly utilizing speculative execution.
- Firmware – As would be the case within the firmware used to power a camera.
- Operating system – Such as a memory management error within an OS kernel.
- OS library or subsystem – For instance, if a file header was improperly read and sanitized, executing instructions contained within the header.
- Application – Over-privileged mobile apps may steal sensitive information, such as a user's contacts, and send it back to a central storage location.
- Communications protocol – Any communications protocol utilized by the device, such as [e.g., Cellular, Bluetooth, WiFi, and Near Field Communications (NFC)].

These are a few examples, with the mobile threat surface expanding out to the entire ecosystem used to empower mobile devices nowadays. Many intrusions use valid credentials obtained through external means, such as social engineering. One important consideration in mobile is protecting credentials stored on the device, because a user’s email account could also serve as their system or Domain Admin account.

MDM tools can scale to hundreds of thousands of devices, and provide the necessary monitoring to be alerted when devices are out of compliance; for instance, if someone installs an unauthorized application, turns off encryption, or jailbreaks or roots their device. By default, these

monitoring tools do not continuously scan, instead scanning at a predetermined interval. Successful attacks on a device occurring during this period of time between scans would not be noticed by the enterprise until the next scan is run. The scan period is configurable, but frequent scans can come at a cost of significant power utilization. Mobile vulnerability assessments must incorporate threat modeling, and an understanding of the devices, data, users, and their behaviors. MDMs can play a key role in gathering the information for the “what” and “who” for mobile management, listed in CIS Controls 1 and 2, that provide the foundation for this CIS Control. Vulnerabilities can sometimes be identified and managed within EMMs and MDMs via traditional vulnerability managed scanners and other tools.

Mobile security tools using an agent-based approach give a view to threats on and to the mobile device, such as malicious applications and profiles, and malicious WiFi networks or Man-in-the Middle (MitM) web proxy attacks. There are also tools and approaches that funnel mobile traffic through filtering cloud infrastructures that perform web gateway filtering and security functions. Some EMM vendors may use browsers that they have additional control over. These browsers may be home-brewed, or utilize important libraries and kits from other on-device browsers.

Mobile operating systems, email clients, browsers, and all apps must be kept up-to-date in order to remain effective because the OS manufacturer, Original Equipment Manufacturer (OEM), and baseband provider (e.g., Qualcomm, Intel) all have to work together to develop, approve, and authorize mobile OS updates. It can take significant time to receive these updates, if they will be made available at all. When an update is available, admins cannot generally force an update, but can let a user know that an update is available and that they should install it. This can be done via an on-device notification through the management app / secure container, or through more traditional means (e.g., email, word-of-mouth).

CIS Control 3: Continuous Vulnerability Management			Applicability	
Sub-Control	Control Title	Control Descriptions	Included	Justification
3.1	Run Automated Vulnerability Scanning Tools	Utilize an up-to-date Security Content Automation Protocol (SCAP) compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.	•	Vulnerability assessment tools can be utilized in an automated manner.
3.2	Perform Authenticated Vulnerability Scanning	Perform authenticated vulnerability scanning with agents running locally on each system or with remote scanners that are configured with elevated rights on the system being tested.		Accounts for these types of scans are unavailable on mobile devices. Authenticated accounts are generally associated with managing configurations and settings on the device. On-device vulnerability scanning apps can be used, but the enterprise may need to approve or sign them before they are used as they are sometimes unsafe.
3.3	Protect Dedicated Assessment Accounts	Use a dedicated account for authenticated vulnerability scans, which should not be used for any other administrative activities and should be tied to specific machines at specific IP addresses.	•	Accounts used within vulnerability scanning tools dedicated to mobile devices need to be protected in a manner similar to other high-value administrative accounts. The vulnerability scanning tools may be integrated with the EMM, and could cause service disruptions if improperly used.
3.4	Deploy Automated Operating System Patch Management Tools	Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.		Unless a particular fully managed scenario is used, external tools are often unable to force updates to the mobile OS. Administrators are often able to remind users to update their phone via a notification.

CIS Control 3: Continuous Vulnerability Management			Applicability	
Sub-Control	Control Title	Control Descriptions	Included	Justification
3.5	Deploy Automated Software Patch Management Tools	Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.		Unless a particular fully managed scenario is used, external tools are often unable to force updates to the application. Administrators are often able to remind users to update their apps via a notification.
3.6	Compare Back-to-Back Vulnerability Scans	Regularly compare the results from consecutive vulnerability scans to verify that vulnerabilities have been remediated in a timely manner.	•	Mobile devices will also benefit from checking current vulnerabilities against historical data and trends.
3.7	Utilize a Risk-Rating Process	Utilize a risk-rating process to prioritize the remediation of discovered vulnerabilities.	•	Administrators and security professionals will benefit from rating mobile device vulnerabilities. The Common Vulnerability Scoring System (CVSS) does not differentiate between system types and is applicable to mobile devices and their associated management systems (https://www.first.org/cvss/specification-document).

CIS Control 4: Controlled Use of Administrative Privileges

The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

Mobile Applicability

Administrative privilege is different within mobile operating systems. Both Android and iOS allow for EMMs and MDMs to take administrative control of a device. The user can generally override administrative access by revoking their control, while in other situations this is not possible (such as with the Apple® Device Enrollment Program). Administrators do not need to input an administrator password into a mobile device. Instead, the EMM dashboard is used to extend invitations to individual users and their devices. This dashboard is typically a publicly accessible web application and should be the focus of protecting the administrative level privileges over mobile devices.

- Overview of Android Management
- Overview of iOS management
- Apple DEP Program

Mobile Deployment Considerations

Administrators should be extremely careful when first working with a completely unmanaged device. If there is no EMM, MDM, or MTD agent on the device, it may already be rooted or jailbroken. Other technologies might also be able to check for rooting or jailbreaking prior to allowing login, such as two-factor authentication (2FA) solutions. This can be used in conjunction with an MDM/MTD solution or when those tools are not deployed. It is very important to not let a compromised device on the network (for obvious reasons) but there are different ways to do the assessment depending on the use case. A device with a compromised security architecture may already be under surveillance by a malicious party via keylogging and/or screen catching. Therefore, any administrative credentials or passwords used to configure applications may be susceptible to compromise. Consider installing an MTD application first in order to mitigate this threat.

Fully managed scenarios obviate many of the risks associated with administrative credentials.

Mobile Additional Discussion

Malicious apps are taking advantage of unfamiliarity with the mobile admin levels, and there are malicious apps that obtain admin rights via OS or firmware level vulnerabilities so that they can hide themselves from the user. Additionally, malicious MDM profiles are an ongoing issue, which attempt to trick a user into providing administrative access to a malicious entity. This ultimately depends on the user, who makes the final decision to accept a profile or not. Finally, some users may intentionally install a third-party profile onto their system. iOS signing profiles allow applications that lack an approved digital signature to be installed on a device, effectively bypassing the system whitelisting process. This allows users to enjoy cracked apps without paying for them.

Keep in mind that this entire CIS Control is difficult to enforce on a rooted or jailbroken device. Doing this completely subverts the security model of the mobile device, but also makes the user a

root. When devices are jailbroken or rooted, they often have default admin credentials that users do not take care to change.

CIS Control 4: Controlled Use of Administrative Privileges			Applicability	
Sub-Control	Control Title	Control Descriptions	Included	Justification
4.1	Maintain Inventory of Administrative Accounts	Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.		An administrative EMM account is used, obviating the need for local administrative accounts on mobile.
4.2	Change Default Passwords	Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.		There are no default passwords used system-wide.
4.3	Ensure the Use of Dedicated Administrative Accounts	Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not Internet browsing, email, or similar activities.	•	Administrative accounts for management applications should have dedicated passwords. Scheduled auditing of administrative accounts should be regularly performed to assess if admin accounts/privileges are still required.
4.4	Use Unique Passwords	Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.	•	Administrative accounts for management applications should use unique passwords.
4.5	Use Multi-Factor Authentication for All Administrative Access	Use multi-factor authentication and encrypted channels for all administrative account access.		2FA is not generally used when provisioning a device into an EMM.

CIS Control 4: Controlled Use of Administrative Privileges			Applicability	
Sub-Control	Control Title	Control Descriptions	Included	Justification
4.6	Use Dedicated Workstations For All Administrative Tasks	Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading email, composing documents, or browsing the Internet.	•	This is especially important for the system involved in automated provisioning. For accessing the EMM / MDM dashboard, this presents significant challenges as many dashboards are publicly accessible web applications. Organizations with a limited risk appetite may wish to host their EMM on-premises.
4.7	Limit Access to Scripting Tools	Limit access to scripting tools (such as Microsoft® PowerShell and Python) to only administrative or development users with the need to access those capabilities.		Mobile operating systems generally do not offer these types of environments in a stock operating system. Jailbroken and rooted systems do, and access should be limited in those situations.
4.8	Log and Alert on Changes to Administrative Group Membership	Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.	•	This can be accomplished via compliance policies within the EMM.
4.9	Log and Alert on Unsuccessful Administrative Account Login	Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.	•	This can be accomplished via compliance policies within the EMM.

CIS Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

Establish, implement, and actively manage (track/report on/correct) the security configuration of mobile devices, laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

Mobile Applicability

The correct configurations and monitoring of these configurations are critical to maintain trust and secure a mobile device deployment. Configurations apply to devices, EMMs, applications, and the platforms used to develop them. Configurations could also be stored within standardized profiles containing configurations and compliance actions.

Mobile Deployment Considerations

The National Information Assurance Partnership (NIAP) approves EMM and MDM products, and may have detailed configuration guidance for the EMMs if a product's developer decides to achieve certification. The following link is the NIAP Approved Product List. Note that these configurations only apply to "on-prem" EMM deployments.

Devices provisioned into an EMM, or fully managed, can be significantly more "locked down" than unmanaged or partially managed scenarios. When developing mobile policies and creating configuration baselines, each organization should consider the usability impacts of the configuration settings before pushing them to devices. The CIS Benchmarks for iOS and Android can be used for managed scenarios.

Mobile Additional Discussion

EMMs can configure application and operating system settings on mobile devices. Additionally, in fully supervised situations they can restrict user access to mobile device functionality such as cameras, whitelist WiFi networks, apply password policy enforcement, and inventory which apps are installed. Organizations obtaining privileged access to user devices should be aware of the privacy concerns associated with doing so. A company may not want the liability of knowing or having access to an employee's personal email, apps that track health information or financial data, personal contacts and calendars, apps used in their personal lifestyle, or their location.

CIS Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers			Applicability	
Sub-Control	Control Title	Control Descriptions	Included	Justification
5.1	Establish Secure Configurations	Maintain documented security configuration standards for all authorized operating systems and software.	•	Organizations may choose to use the CIS Benchmarks for iOS and Android (linked above) to begin configuring the mobile operating systems. The U.S. government NIAP program can assist with configurations for EMM and MDM applications.
5.2	Maintain Secure Images	Maintain secure images or templates for all systems in the enterprise based on the organization's approved configuration standards. Any new system deployment or existing system that becomes compromised should be imaged using one of those images or templates.		This is generally not possible on iOS, as all images must be signed by Apple before installation. On Android this is possible, but not often done.
5.3	Securely Store Master Images	Store the master images and templates on securely configured servers, validated with integrity monitoring tools, to ensure that only authorized changes to the images are possible.		Maintaining secure images is not typically associated with mobile environments, and therefore images cannot be securely stored.
5.4	Deploy System Configuration Management Tools	Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.	•	EMM and MDM can help to deploy and manage device configurations.
5.5	Implement Automated Configuration Monitoring Systems	Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.	•	EMM and MDM can help to monitor for configuration and policy violations.

CIS Control 6: Maintenance, Monitoring, and Analysis of Audit Logs

Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.

Mobile Applicability

Mobile devices do not generate logs in the same manner as traditional desktop devices. If and when logs are generated, they are not necessarily made available to an external application or service. iOS and Android logs do exist, and can most often be obtained after a device syncs with a desktop and may need to be manually pulled from the device. Mobile apps may generate logs as well but this will be a design decision made by the developer and is not commonly available to the enterprise.

Mobile Deployment Considerations

Fully managed scenarios will provide additional access to mobile OS and application logs resident on-device. These logs are separate from EMM tools, which generate their own bodies of logs and can integrate with a SIEM. SIEMs can ingest and correlate events between all available data sources, such as apps, devices, EMM, MDM, MTD, and other mobile information sources.

Mobile Additional Discussion

Monitoring is irrelevant if there is not a process to identify events and respond to them. And this response must be matched with the potential impact of the event. This is the human aspect: determining which events or alerts can potentially damage the organization, and execute a response in a timely fashion based on that. Varying sources of mobile data can be monitored. MDMs use the more traditional network operations type of approach and try to answer the following questions: *Is the device live? What are the make, model, and version? Is it up to date? Which applications are installed? Has the device been rooted or jailbroken? How much traffic is it sending and receiving?* Many of these items can be set up via compliance policies.

Traditional security tools have more granular logging, such as installation of known bad or suspicious desktop applications, application-level changes to data, network routing changes, SSL certificates used, virtual private network (VPN) launching, and, in the case of cloud filtering, traditional perimeter gateway logs for web traffic, or other application traffic. There is also the practice of monitoring account connections to the network domain or a specific application.

Metrics should be actionable in lieu of providing solely the number of occurrences for an event. More effective things to track are: *Am I getting data from everything I should (How many devices are sending events)? Is the right data being collected (Are all data logs the correct ones)?* Another item to track is the turnover rate of mobile devices, which is much higher than laptops. You will find user accounts with multiple devices attributed to them.

CIS Control 6: Maintenance, Monitoring, and Analysis of Audit Logs			Applicability	
Sub-Control	Control Title	Control Descriptions	Included	Justification
6.1	Utilize Three Synchronized Time Sources	Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.		iOS and Android devices primarily utilize the cellular network (potentially via the Network Identity and Time Zone (NITZ) protocol) or the GPS network for their source of time. Within the mobile OS, they can generally only be synced to a single time source via the Network Time Protocol (NTP). Developers may be able to design individual applications to utilize additional time sources.
6.2	Activate Audit Logging	Ensure that local logging has been enabled on all systems and networking devices.	•	Audit logging can primarily be enabled via the EMM, MDM, MAM, or MTD management panel. This type of auditing would generally be for the EMM and not necessarily the device.
6.3	Enable Detailed Logging	Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.	•	Various levels of detail and types of audit logs can be enabled within the EMM.
6.4	Ensure Adequate Storage for Logs	Ensure that all systems that store logs have adequate storage space for the logs generated.	•	This is always a concern for any type of system.
6.5	Central Log Management	Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.	•	EMMs create extremely useful data about the state and health of the devices they manage. This information should be stored and processed via a single resource.

CIS Control 6: Maintenance, Monitoring, and Analysis of Audit Logs			Applicability	
Sub-Control	Control Title	Control Descriptions	Included	Justification
6.6	Deploy SIEM or Log Analytic Tools	Deploy Security Information and Event Management (SIEM) or log analytic tools for log correlation and analysis	•	Administrators can use a SIEM to correlate security events on mobile devices with other events occurring in the enterprise network.
6.7	Regularly Review Logs	On a regular basis, review logs to identify anomalies or abnormal events.	•	Logs provide very little value if they are never reviewed. At the very least, after an incident occurs they can provide some of the most valuable sources of information. SIEMs and other automated log analysis tools can also help to identify small issues before they become large problems.
6.8	Regularly Tune SIEM	On a regular basis, tune your SIEM system to better identify actionable events and decrease event noise.	•	Customizing rules and alerts to your enterprise's unique needs is important. Mobile devices will require modifying and creating new rules.

CIS Control 7: Email and Web Browser Protections

Minimize the attack surface and the opportunities for attackers to manipulate human behavior through their interaction with web browsers and email systems.

Mobile Applicability

Traditional email gateway security controls for reducing spam, phishing attacks, malware, and malicious URL links all apply to mobile. Mobile devices change the traditional enterprise architecture by not only extending it outside a traditional perimeter, but also bypassing the need to route much or all traffic through the enterprise network due to use of cloud services. However, web and email threats are still a concern with mobile devices. Additionally, MTD can apply host-based protection via an on-device VPN interface and review all links and pages visited.

Mobile Deployment Considerations

In situations where a full-device (or on-demand) VPN is not in use, a reverse proxy might be useful to act as a centralized, authenticated access point to corporate data and resources, with the added benefit that they can be controlled (turned on or off) based on device compliance policies. Organizations may wish to utilize additional agent-based tools with devices that are not provisioned into an EMM. This does assist with logical process isolation, and many of the MDM/MAM tools provide their email and web apps with a corresponding proxy service. This is not required, but many organizations choose to use it.

It is important to point out, however, that from a usability perspective and an update perspective, it is often preferable to utilize the native solutions that are available. There is often a period of time when a new version of a mobile OS is released and subsequently installed, and the third-party email and browser apps are not updated and do not function as intended. Several MTD solutions include phishing protection capabilities that can be implemented in different ways based on the MTD solution's design.

Mobile Additional Discussion

An on-device approach provides a better view into the threats affecting an employee's use of email and web browsers. This includes malicious applications, profiles, and network attacks (e.g., man-in-the-middle web proxy attacks). Some tools use on-device visibility to analyze sites that can be serving up malware or attempting to phish the user to collect credentials. There are also tools and approaches that funnel mobile traffic through filtering cloud infrastructures that perform web gateway filtering and security functions.

Mobile security providers often provide dedicated email clients and browsers for employees to use with their corporate email that the vendor and organization can have additional control over. These clients and browsers may be home-brewed, or utilize important libraries and kits from other on-device browsers. At the very least, these alternative applications will run under a different user and application ID, providing additional protections to isolate a user's personal and corporate email. Regardless, all email clients and browsers must be obtained from an authorized repository, written by a trustworthy developer, and kept up-to-date in order to remain effective.

CIS Control 7: Email and Web Browser Protections			Applicability	
Sub-Control	Control Title	Control Descriptions	Included	Justification
7.1	Ensure Use of Only Fully Supported Browsers and Email Clients	Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers and email clients provided by the vendor.	•	Browsers and email clients should be kept up-to-date. This is especially important if an organization is wrapping the app or using a custom app that cannot be updated via the normal mobile application store update process that a user would be familiar with.
7.2	Disable Unnecessary or Unauthorized Browser or Email Client Plugins	Uninstall or disable any unauthorized browser or email client plugins or add-on applications.		Email client and browser plugins generally do not exist for the mobile versions of these applications.
7.3	Limit Use of Scripting Languages in Web Browsers and Email Clients	Ensure that only authorized scripting languages are able to run in all web browsers and email clients.		Scripting languages for email client apps and mobile browsers generally do not exist on mobile platforms.
7.4	Maintain and Enforce Network-Based URL Filters	Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.	•	Network-based proxies, firewalls, and other proxies can be configured for mobile devices, or specifically support capabilities to filter mobile traffic. Content blockers can be developed for certain applications.
7.5	Subscribe to URL-Categorization Service	Subscribe to URL-categorization services to ensure that they are up-to-date with the most recent website category definitions available. Uncategorized sites shall be blocked by default.	•	Although network-based solutions exist for this CIS Sub-Control, some EMMs support a feature to whitelist and blacklist specific URLs, domains, or IP address blocks.
7.6	Log All URL Requests	Log all URL requests from each of the organization's systems, whether on-site or a mobile device, in order to identify potentially malicious activity and assist incident handlers with identifying potentially compromised systems.	•	VPN interfaces on mobile devices can siphon traffic to be logged and analyzed.

CIS Control 7: Email and Web Browser Protections			Applicability	
Sub-Control	Control Title	Control Descriptions	Included	Justification
7.7	Use of DNS Filtering Services	Use Domain Name System (DNS) filtering services to help block access to known malicious domains.	•	Mobile devices can be configured to support this within the mobile OS.
7.8	Implement DMARC and Enable Receiver-Side Verification	To lower the chance of spoofed or modified emails from valid domains, implement Domain-based Message Authentication, Reporting and Conformance (DMARC) policy and verification, starting by implementing the Sender Policy Framework (SPF) and the Domain Keys Identified Mail (DKIM) standards.		Although demarcation point (DMARC) is an important Sub-Control, there's little to be done specifically on the mobile device and management platforms to enable this mitigation.
7.9	Block Unnecessary File Types	Block all email attachments entering the organization's email gateway if the file types are unnecessary for the organization's business.	•	This can be performed via an EMM's email security policies.
7.10	Sandbox All Email Attachments	Use sandboxing to analyze and block inbound email attachments with malicious behavior.		On mobile devices, email attachments are downloaded and placed within each application's sandboxed directories. This is not the type of sandboxing envisioned by this CIS Sub-Control, and mechanisms do not exist to perform additional sandboxing.

CIS Control 8: Malware Defenses

Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.

Mobile Applicability

Mobile malware primarily takes the form of malicious applications, updates to malicious applications, and browser-based malware. Another example threat vector for malware is via Android Debug Bridge (ADB) that can be exposed via Universal Serial Bus (USB) debugging capabilities and remotely accessible via port 5555. That is not to say that hardware and firmware vulnerabilities do not exist and are exploited, but the vast majority of mobile malware takes the form of malicious applications. Mobile malware utilizes track patterns that are different from traditional desktop-based malware, such as tricking a user into accepting a management profile, and differences even exist between the mobile operating systems. Google's Android Security 2017 Year In Review defines an entire system of classifying mobile malware, referred to as their Potentially Harmful Applications (PHA) categories.

Mobile Deployment Considerations

The proper configuration settings on mobile devices can help to mitigate a large percentage of mobile malware, such as ensuring the mobile sandbox is intact and being enforced. These configurations should be enforced to the degree possible before users are provided a device. The same goes for updating the mobile OS. This is much easier when considering fully managed scenarios and configurations can be mandated and enforced. From a BYOD perspective, personal phones are a greater risk, as users download a larger number of apps for personal use than business use. Users must be educated about their role preventing the installation of malware. One of the most important malware defenses possible on mobile is preventing employees from using an unofficial appstore. Google's Android Security 2017 Year In Review states that *"devices that installed apps from outside of Google Play were nine times more likely to be affected by PHAs."*

Mobile Additional Discussion

Traditional anti-malware techniques are not feasible on iOS, due to the platform not allowing access at a level where applications can have general knowledge about other applications running on the device. This does not apply to jailbroken and rooted devices, which are particularly susceptible to malware and general attacks. MTD host-based agents can provide anti-malware protection, especially if they are provided a privileged access via an EMM or profile / admin access. Another technique is to review mobile applications off-device and then match hashes of the apps installed on the device against that analysis. This type of application vetting process is detailed within NIST SP 800-163: Vetting the Security of Mobile Applications, and is further explored in CIS Control 18.

Another product category that is helpful is mobile threat intelligence. These services review apps and provide a risk rating or threat score based on app capabilities, behavior and other analysis, to mobile administrators. The information can be used to help make the installation decision easier for both admins and end users. Mobile app vetting tools can also serve a similar function by performing static and dynamic analysis to find vulnerabilities and identify Trojan apps. Many of

the tools described within this section may be able to integrate with EMMs so that one dashboard can be used.

Finally, mobile devices themselves are also risks to personal computers (PCs). Email attachments forwarded from mobile devices might have PC malware that does not affect the mobile device, but could infect the PC. Mobile devices connected via USB to a PC could also have malicious PC files as they can act as removable media. Traditional PC antivirus also cannot always scan mobile devices like a traditional USB drive. Traditional PC USB port monitoring can help with the threat of a mobile device connected to a PC.

CIS Control 8: Malware Defenses			Applicability	
Sub-Control	Control Title	Control Descriptions	Included	Justification
8.1	Utilize Centrally Managed Anti-Malware Software	Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.	•	This would often be the usage of an MTD product, although some EMMs and mobile threat intelligence server-side applications also contain this capability.
8.2	Ensure Anti-Malware Software and Signatures Are Updated	Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis.	•	MTD applications should be kept up-to-date with their subscriptions active.
8.3	Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies	Enable anti-exploitation features such as Data Execution Prevention (DEP) and Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		These are enabled by default on modern versions of mobile operating systems.
8.4	Configure Anti-Malware Scanning of Removable Media	Configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected.		Removable devices generally are not supported on mobile devices, and MTD apps would not have access to them.

CIS Control 8: Malware Defenses			Applicability	
Sub-Control	Control Title	Control Descriptions	Included	Justification
8.5	Configure Devices to Not Auto-Run Content	Configure devices to not auto-run content from removable media.		Mobile devices can be configured to prevent specific applications from running once a device is newly booted. Yet mobile apps generally do not auto-start when a peripheral is plugged into the device, although a notification may be presented to the user prompting the user to manually open the app.
8.6	Centralize Anti-Malware Logging	Send all malware detection events to enterprise anti-malware administration tools and event log servers for analysis and alerting.	•	Using an MTD product for all of the devices in an enterprise is essentially centralized anti-malware logging. The event information can be exported to a SIEM.
8.7	Enable DNS Query Logging	Enable Domain Name System (DNS) query logging to detect hostname lookups for known malicious domains.		If this capability exists within an enterprise's network, that capability should also work for mobile devices with no change necessary.
8.8	Enable Command-Line Audit Logging	Enable command-line audit logging for command shells, such as Microsoft® PowerShell and Bash.		Interacting with the device via a command-line interface is often not supported on mobile devices. In fact, Bash environments would have to be installed onto the device before they are able to be used.

CIS Control 9: Limitation and Control of Network Ports, Protocols, and Services

Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.

Mobile Applicability

Although mobile devices contain ports, protocols, and various network services, they do not always respond in a typical and expected manner to network scans. This is most often the case on iOS, as Android devices act in a manner closer to traditional systems. A related concept is the control and use of different wireless interfaces, such as WiFi, Bluetooth, or NFC. These should be managed, as WiFi, Bluetooth, and cellular beacons / advertisements may broadcast the presence of the mobile device to the surrounding area.

Mobile Deployment Considerations

This CIS Control is not affected by a mobile device deployment scenario. Managed scenarios allow for the control of network interfaces. Users can be made aware of the threats posed to enabling wireless interfaces, although turning them off may lead to untenable usability issues from an employee's perspective. For instance, turning off Bluetooth would not let an employee use Bluetooth headphones, which are potentially expensive and quite common nowadays. Some EMMs allow for enterprises to allow Bluetooth audio but block Bluetooth data, although this is an uncommon control.

Mobile Additional Discussion

Traditional guidance applies on limiting interfaces to only those required for purpose, and restricting viewing or connecting to these interfaces. Specific mobile apps may be directly correlated to an open port on Android. Accordingly, removing superfluous apps on any mobile OS is an attack surface reduction approach. Additional attack surface reduction activities can likely be done in high-risk scenarios, specifically for Android, but this is not a traditional approach.

The management platforms used for managing mobile devices should be treated as regular servers and scanned accordingly alongside other enterprise systems.

CIS Control 9: Limitation and Control of Network Ports, Protocols, and Services			Applicability	
Sub-Control	Control Title	Control Descriptions	Included	Justification
9.1	Associate Active Ports, Services, and Protocols to Asset Inventory	Associate active ports, services, and protocols to the hardware assets in the asset inventory.	•	Although the ports that are listed may not be directly associated with services running on a device, it is worthwhile to understand which ports are considered baseline for any enterprise devices and monitor for changes. Android Debug Bridge (ADB) is a service that may be necessary for certain user segments within the enterprise, but others will need it enabled. This includes those charged with security, testing, and development duties.
9.2	Ensure Only Approved Ports, Protocols, and Services Are Running	Ensure that only network ports, protocols, and services listening on a system with validated business needs are running on each system.		This is impractical on mobile devices. For instance, it is generally not considered possible to close transmission control protocol (TCP) port 62078 on Apple iOS.
9.3	Perform Regular Automated Port Scans	Perform automated port scans on a regular basis against all systems and alert if unauthorized ports are detected on a system.	•	Just as with traditional systems, automated port, and other types of network scans, should be performed.
9.4	Apply Host-Based Firewalls or Port-Filtering	Apply host-based firewalls or port-filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.		The privileges to do such a thing are generally not available on mobile operating systems.
9.5	Implement Application Firewalls	Place application firewalls in front of any critical servers to verify and validate the traffic going to the server. Any unauthorized traffic should be blocked and logged.		These are generally not available on mobile.

CIS Control 10: Data Recovery Capabilities

The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.

Mobile Applicability

Mobile devices are designed to make data available to users in a manner as easy as possible, and this includes backing data up. The two major mobile platforms have their own ecosystems to alleviate backup concerns that can often be used via a few configuration options. Many organizations find it more of a worry to have enterprise information unintentionally stored on unapproved servers and systems. The native backup utilities primarily attempt to back up a user's contacts, photos, text messages, and documents. These are stored in the mobile OS supporting platform(s), such as iCloud. Accordingly, only certain file formats and data storage locations can be backed up. Beyond this, certain applications have their own cloud storage methods and platforms to assist with data recovery, but they must be appropriately configured before they should be considered sufficiently reliable for enterprise usage.

Mobile Deployment Considerations

This CIS Control applies regardless of deployment scenario. Special considerations should be taken in BYOD and shared-device situations to prevent sensitive user data, such as photos, from being backed up and intermingled with enterprise data. This requires both the enterprise and user working together toward this common goal, necessitating additional user education. On the other side of the coin, when an enterprise needs to wipe a device for whatever reason, any enterprise information needs to have already been backed up onto an approved storage location.

Mobile Additional Discussion

Organizations should verify and review backup (e.g., iCloud, Google) settings to make sure the proper information is backed up, encrypted, and that improper information is not backed up. This might include corporate email, corporate contacts or calendar, or documents (e.g., xlsx, docx, pdf) to personal backup. The former would generally be stored on the corporate Exchange server already with mobile devices fetching that information as needed. Corporate policies should be specified for backing up enterprise data to a public cloud – especially if it is not a cloud platform or service provided and approved for corporate usage by the organization. Proper authentication mechanisms and other controls should be in place to protect any enterprise cloud backup.

Mobile devices may also intentionally or unintentionally back up information to any desktop environment they are physically or wirelessly connected to. The creation of these backups should be prevented unless specifically authorized by the enterprise. Desktop backups can also be protected via an authentication mechanism and cryptographic means.

CIS Control 10: Data Recovery Capabilities			Applicability	
Sub-Control	Control Title	Control Descriptions	Included	Justification
10.1	Ensure Regular Automated Backups	Ensure that all system data is automatically backed up on a regular basis.	•	Users should regularly back up enterprise data to approved backup locations. Enterprises should provide guidance for how to configure the mobile OS and applications to accomplish this goal.
10.2	Perform Complete System Backups	Ensure that all of the organization's key systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system.		Mobile devices generally lack the notion of a system image, and information oftentimes must be configured and backed up on a per-app basis.
10.3	Test Data on Backup Media	Test data integrity on backup media on a regular basis by performing a data restoration process to ensure that the backup is properly working.	•	Employees and administrators should regularly perform this action. An easy way of testing this is going through the motions of provisioning a new phone or application to a new device.
10.4	Protect Backups	Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.	•	Some cloud-based services will do this automatically, but users and enterprises need to check on the mitigations in place before electing to use a service, such as multifactor authentication. Any removable media for the device, alongside desktop backups, also need to be protected.
10.5	Ensure All Backups Have at Least One Offline Backup Destination	Ensure that all backups have at least one offline (i.e., not accessible via a network connection) backup destination.	•	Ransomware and its related offshoots (e.g., destructive malware) typically perform malicious activities on-device. In mobile scenarios, this type of malware typically prevents a user's access to the device. Similar to traditional scenarios, enterprise information should be backed up offline to prevent this type of attack from being successful.

CIS Control 11: Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches

Establish, implement, and actively manage (track/report on/correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

Mobile Applicability

This section has little direct effect on mobile security and more generally applies to the secure usage of network devices. Guidance on WiFi security is available and applicable in this situation, but that guidance applies to all computing devices utilizing WiFi.

Mobile Deployment Considerations

N/A

Mobile Additional Discussion

N/A

CIS Control 11: Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches			Applicability	
Sub-Control	Control Title	Control Descriptions	Included	Justification
11.1	Maintain Standard Security Configurations for Network Devices	Maintain documented security configuration standards for all authorized network devices.		See the *Applicability* statement above.
11.2	Document Traffic Configuration Rules	All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.		See the *Applicability* statement above.
11.3	Use Automated Tools to Verify Standard Device Configurations and Detect Changes	Compare all network device configurations against approved security configurations defined for each network device in use, and alert when any deviations are discovered.		See the *Applicability* statement above.

CIS Control 11: Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches			Applicability	
Sub-Control	Control Title	Control Descriptions	Included	Justification
11.4	Install the Latest Stable Version of Any Security-Related Updates on All Network Devices	Install the latest stable version of any security-related updates on all network devices.		See the *Applicability* statement above.
11.5	Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions	Manage all network devices using multi-factor authentication and encrypted sessions.		See the *Applicability* statement above.
11.6	Use Dedicated Workstations for All Network Administrative Tasks	Ensure network engineers use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be segmented from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading email, composing documents, or surfing the Internet.		See the *Applicability* statement above.
11.7	Manage Network Infrastructure Through a Dedicated Network	Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.		See the *Applicability* statement above.

CIS Control 12: Boundary Defense

Detect/prevent/correct the flow of information transferring across networks of different trust levels with a focus on security-damaging data.

Mobile Applicability

Mobile devices remove the concept of the traditional infrastructure boundary by allowing users to work completely locally, or frequently accessing cloud-based services directly, without routing through corporate infrastructure. With this in mind, traditional boundary defense concepts can still apply to mobile devices. Traditional network monitoring tools, email security, intrusion detection system (IDS) and intrusion prevention system (IPS) alerts, logging of events and alerts, and VPNs are all important. These can be implemented directly into the enterprise or some components may be hosted in the cloud. In one scenario, device traffic can be routed through the enterprise, while in the other scenario, traffic can be sent through cloud infrastructure. Many enterprises will use a combination of these two approaches, as some important services are only available via third-party cloud platforms.

Mobile Deployment Considerations

Enterprises should keep in mind that most mobile devices are explicitly outside of the network boundary, regardless of deployment scenario. A mobile device is a network endpoint when it is physically inside a corporate facility connecting via WiFi, as it is when a local or remote device is utilizing an always-on VPN. When a device is solely accessing information without a VPN, it is not considered a network endpoint. Even with an always-on VPN obtaining an internal IP address, certain types of traffic will not be sent through the enterprise VPN. Examples include diagnostic information about the device, OS traffic communication with an ecosystem provider, WiFi, Bluetooth, and cellular traffic. The device ultimately leaks information to any malicious actors passively sniffing this information and can help attackers fingerprint the device. In part because of this, BYOD scenarios should have additional security controls implemented on the device, and perhaps also on the home network of the user.

Mobile Additional Discussion

Organizations should choose to utilize a VPN for all BYOD or remote devices. Where it is terminated is a selection up to the enterprise, based on security concerns and policy/legal considerations. However, there are also tools and approaches that funnel mobile traffic through filtering cloud infrastructures that perform web gateway filtering and security functions.

Devices will automatically attempt to access WiFi networks they have previously been associated with and connected to. Blacklisting certain service set identifiers (SSIDs) on devices, such as those from major retailers and cafes, can help prevent a user's device from accessing a rogue version of that network and sending sensitive enterprise data over it.

CIS Control 12: Boundary Defense			Applicability	
Sub-Control	Control Title	Control Descriptions	Included	Justification
12.1	Maintain an Inventory of Network Boundaries	Maintain an up-to-date inventory of all of the organization's network boundaries.		In general, mobile devices should be considered to function outside of the network boundary
12.2	Scan for Unauthorized Connections Across Trusted Network Boundaries	Perform regular scans from outside each trusted network boundary to detect any unauthorized connections which are accessible across the boundary.		Enterprises would have to obtain specific permission to scan an employee's home network, and also would have to have an agent within the network to do the scanning. If the user was not on a network they own, then the enterprise could be scanning a network they do not own, which is potentially illegal in many countries.
12.3	Deny Communications With Known Malicious IP Addresses	Deny communications with known malicious or unused Internet IP addresses and limit access only to trusted and necessary IP address ranges at each of the organization's network boundaries.	•	Botnets and other malware distribution nodes that are specific to mobile should be included when an organization implements this Sub-Control. This Sub-Control is better and more easily enforced when devices are taking advantage of a VPN.
12.4	Deny Communication Over Unauthorized Ports	Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.		This is generally impractical on mobile devices. See information within the sections for CIS Controls 2, 3, and 9.
12.5	Configure Monitoring Systems to Record Network Packets	Configure monitoring systems to record network packets passing through the boundary at each of the organization's network boundaries.		Although this Sub-Control is quite useful, this is generally not a mobile-specific configuration, although some developer options support this.

CIS Control 12: Boundary Defense			Applicability	
Sub-Control	Control Title	Control Descriptions	Included	Justification
12.6	Deploy Network-Based IDS Sensors	Deploy network-based Intrusion Detection Systems (IDS) sensors to look for unusual attack mechanisms and detect compromise of these systems at each of the organization's network boundaries.	•	Enterprises can ensure that signatures and other information used by the IDS are mobile-specific, and that their IDS is "mobile aware." This Sub-Control is better and more easily enforced when devices are taking advantage of a VPN.
12.7	Deploy Network-Based Intrusion Prevention Systems	Deploy network-based Intrusion Prevention Systems (IPS) to block malicious network traffic at each of the organization's network boundaries.	•	Enterprises can ensure that any relevant IPS is "mobile aware." This Sub-Control is better and more easily enforced when devices are taking advantage of a VPN.
12.8	Deploy NetFlow Collection on Networking Boundary Devices	Enable the collection of NetFlow and logging data on all network boundary devices.		Although this Sub-Control is quite useful, there is nothing specific to mobile about it.
12.9	Deploy Application Layer Filtering Proxy Server	Ensure that all network traffic to or from the Internet passes through an authenticated application layer proxy that is configured to filter unauthorized connections.		Although this Sub-Control is quite useful, there is nothing specific to mobile about it.
12.10	Decrypt Network Traffic at Proxy	Decrypt all encrypted network traffic at the boundary proxy prior to analyzing the content. However, the organization may use whitelists of allowed sites that can be accessed through the proxy without decrypting the traffic.	•	This is most easily done using a VPN service that integrates within the mobile operating system.
12.11	Require All Remote Logins to Use Multi-Factor Authentication	Require all remote login access to the organization's network to encrypt data in transit and use multi-factor authentication.	•	VPN applications and their back-end components can integrate with external authentication services and identity providers. To the degree possible, enterprises should refrain from using a phone number as an identifier, as this can be used to enable personal attacks.
12.12	Manage All Devices Remotely Logging Into Internal Network	Scan all enterprise devices remotely logging into the organization's network prior to accessing the network to ensure that each of the organization's security policies has been enforced in the same manner as local network devices.	•	Administrators should have some degree of control over the security and configuration of any mobile devices accessing an internal network, if this is needed at all.

CIS Control 13: Data Protection

The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.

Mobile Applicability

Detecting and preventing the flow of data on mobile devices is a difficult task, as is protecting that information from unauthorized disclosure. The fact that mobile devices have such a diverse supply chain and utilize numerous cloud services by default makes Data Protection an even more difficult task. Yet steps can be taken to protect enterprise data, and a variety of data protection mitigations can be put into place for mobile.

Mobile Deployment Considerations

Organizations with BYOD programs will need to consider end-user privacy implications within policies and security monitoring and operations procedures. Additionally, agents on the device must not prevent users from accessing their own data. Within unmanaged scenarios, access can be allowed for contractors and employees to log in to enterprise systems with their own devices, leaving the enterprise without visibility into the device itself. Simple device posture assessment techniques could be minimal, such as just checking that the phone is up-to-date and not jailbroken or rooted. Within the traditional BYOD use case employees will want to use their own device, and stronger levels of control and device posture assessment will need to be maintained. Within the COPE scenario a much greater degree of data protection can be attained, alongside a significantly lessened expectation of privacy from the user.

Mobile Additional Discussion

Mobile devices can use traditional VPNs or require the use of an enterprise-approved VPN for accessing the enterprise network, and gaining an internal IP address if necessary. A large majority of mobile apps will attempt to store data in the cloud by default. This makes data protection difficult, as enterprises may not have visibility into how individual apps are configured and, depending on their access rights, may not even know which apps are installed on a device. Therefore, data storage locations should be analyzed for multiple devices' deployment scenarios. Important questions to consider are: *Is this data flowing to a back-end system? Is data stored in multiple places? Is this data in an external cloud platform? Can this data ever be purged? In which country is this data stored (for privacy and other regulatory considerations)?*

Traditional guidance on encrypting data on the devices, and using a VPN with good encryption for protecting sensitive data in transit, still applies to mobile. There are VPNs that allow mobile devices to connect to corporate networks to access applications or data shares, as well as application-specific VPNs that encrypt the data in transit for that application. Some of these technologies include a hardware component, such as a microSD chip, for encryption key management. Traditional enterprise Data Loss Prevention (DLP) can be helpful for email and network stored data. But cloud applications and data may be more difficult to get visibility from mobile device and user access. There are tools that leverage cloud service APIs to gain this visibility, or filtering clouds that proxy mobile users to these external services, which can provide a source for data access controls.

CIS Control 13: Data Protection			Applicability	
Sub-Control	Control Title	Control Descriptions	Included	Justification
13.1	Maintain an Inventory of Sensitive Information	Maintain an inventory of all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located on-site or at a remote service provider.	•	Sensitive information on mobile devices should be recorded.
13.2	Remove Sensitive Data or Systems Not Regularly Accessed by Organization	Remove sensitive data or systems not regularly accessed by the organization from the network. These systems shall only be used as stand-alone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed.	•	These could include unused mobile devices, third-party cloud services, or un-needed management systems. The implementation of this Sub-Control could depend on the deployment model.
13.3	Monitor and Block Unauthorized Network Traffic	Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.		Although an important capability, this typically is controlled from a network appliance, not a device or EMM.
13.4	Only Allow Access to Authorized Cloud Storage or Email Providers	Only allow access to authorized cloud storage or email providers.	•	Managed devices can prevent access to certain services. This can also be partially accomplished via policy.
13.5	Monitor and Detect Any Unauthorized Use of Encryption	Monitor all traffic leaving the organization and detect any unauthorized use of encryption.		This can be extremely difficult on mobile devices, with many applications, and even the mobile OS itself, encrypting information by default with cryptographic keys that are not controlled by the enterprise.
13.6	Encrypt Mobile Device Data	Utilize approved cryptographic mechanisms to protect enterprise data stored on all mobile devices.	•	The NAND flash storage of mobile devices is typically encrypted by default.
13.7	Manage USB Devices	If USB storage devices are required, enterprise software should be used that can configure systems to allow the use of specific devices. An inventory of such devices should be maintained.		This generally does not affect mobile devices as USB storage devices are still not widely utilized, but this can be managed via EMM.

CIS Control 13: Data Protection			Applicability	
Sub-Control	Control Title	Control Descriptions	Included	Justification
13.8	Manage System's External Removable Media's Read/Write Configurations	Configure systems not to write data to external removable media, if there is no business need for supporting such devices.	•	This can be managed via an EMM.
13.9	Encrypt Data on USB Storage Devices	If USB storage devices are required, all data stored on such devices must be encrypted while at rest.		This generally does not affect mobile devices as USB storage devices are still not widely utilized, but this may change in the near future. Removable SD cards within phones were popular in the past but this is no longer the case.

CIS Control 14: Controlled Access Based on the Need to Know

The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.

Mobile Applicability

Email, contacts, and calendar are often considered the most important enterprise data on a mobile device. Yet some enterprises will have their own applications and unique data stored on the device as well. Determinations on enterprise data access should be specifically made for all users, apps, devices, mobile apps, and mobility management infrastructure. Regardless of access control, additional defensive measures can be taken to protect data on the device and data leaving the device. For instance, the storage and usage of cryptographic keys should be taken into consideration on mobile devices, as should the use of approved cryptographic algorithms and hardware cryptographic engines. Traditional guidance on encrypting on-device data and using a VPN or transport layer security (TLS) tunnel with sufficiently strong encryption for protecting sensitive data in-transit still apply within the mobile arena.

Mobile Deployment Considerations

The ability to remotely wipe devices is critical for controlling access based on the need to know. Unmanaged scenarios provide the enterprise no ability to remotely wipe information. Personally owned and corporate enabled devices (i.e., typical BYOD) can be configured for a full device wipe, but in many situations an "enterprise wipe" of just enterprise information and not the entire device is sufficient. Employees will often feel uncomfortable with an enterprise having administrative control over their device and worry that their pictures, texts, and browsing habits are being accessed and viewed by their enterprise. Additionally, providing enterprises the ability to wipe a personally owned device can be untenable. It is a reasonable strategy to provide fully managed and secured mobile devices additional access (based on need to know), and prevent access to sensitive enterprise information for devices for which the security cannot be verified.

Mobile Additional Discussion

Mobile devices can use traditional VPNs accessing the enterprise network, and gain an internal IP address if necessary. TLS or Internet Protocol Security (IPSec) VPNs can be installed. VPN applications can take advantage of cryptographic engines and hardware acceleration, and can utilize specific DNS servers to prevent leakage. VPN apps can be “always-on” and may not overly consume power. In regards to cryptographic protection of data at rest, most modern devices encrypt user data by default. There are VPNs that allow mobile devices to connect to the corporate network to access applications or data shares, as well as application-specific VPNs that encrypt the data in transit for that application. Some of these technologies include a hardware component, such as a microSD chip, for encryption key management.

Although traditional network security mitigations apply, holistic approaches to mobile security must also include the security of messaging platforms and audio. By default, phone calls made over both the public switched telephone network (PSTN) and the cellular networks should not be considered encrypted. The same can be said for text messages. Since the security of these networks is difficult to independently validate, enterprises can elect to use alternative messaging and voice communication services. As an alternative to traditional short message service (SMS) /

texting, third-party messaging apps such as Signal and iMessage can be used. Signal also can make encrypted voice calls, as can FaceTime Audio.

CIS Control 14: Controlled Access Based on the Need to Know			Applicability	
Sub-Control	Control Title	Control Descriptions	Included	Justification
14.1	Segment the Network Based on Sensitivity	Segment the network based on the label or classification level of the information stored on the servers, locate all sensitive information on separated Virtual Local Area Networks (VLANs).	•	Decisions will be need to be made for mobile devices accessing sensitive networks.
14.2	Enable Firewall Filtering Between VLANs	Enable firewall filtering between VLANs to ensure that only authorized systems are able to communicate with other systems necessary to fulfill their specific responsibilities.		This is generally outside the scope of the device itself.
14.3	Disable Workstation-to-Workstation Communication	Disable all workstation-to-workstation communication to limit an attacker's ability to move laterally and compromise neighboring systems, through technologies such as private VLANs or micro segmentation.	•	Although peer-to-peer (P2P) clients and Personal Area Networks (PANs) are possible, this is generally not a common capability. An exception would be Apple's AirDrop protocol, which should be disabled unless needed.
14.4	Encrypt All Sensitive Information in Transit	Encrypt all sensitive information in transit.	•	The use of mobile VPNs, and even per-app VPNs, can help to protect sensitive information in transit. This Sub-Control can also apply to the security of messaging platforms and voice traffic.
14.5	Utilize an Active Discovery Tool to Identify Sensitive Data	Utilize an active discovery tool to identify all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located on-site or at a remote service provider, and update the organization's sensitive information inventory.		This is not specific to mobile devices or their management platforms.

CIS Control 14: Controlled Access Based on the Need to Know			Applicability	
Sub-Control	Control Title	Control Descriptions	Included	Justification
14.6	Protect Information Through Access Control Lists	Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.		This is not specific to mobile devices or their management platforms.
14.7	Enforce Access Control to Data Through Automated Tools	Use an automated tool, such as host-based Data Loss Prevention, to enforce access controls to data even when the data is copied off a system.	•	Automated compliance rules can be set and utilized by EMM technology to enforce policies, and notify users and administrators of access violations.
14.8	Encrypt Sensitive Information at Rest	Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.	•	Modern mobile devices encrypt data at rest by default, but MDM APIs and policies can be set to ensure this occurs.
14.9	Enforce Detail Logging for Access or Changes to Sensitive Data	Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).	•	EMMs can log device access and adherence to compliance policies. Developers can also log changes to sensitive data access within their applications.

CIS Control 15: Wireless Access Control

The processes and tools used to track/control/prevent/correct the secure use of wireless local area networks (WLANs), access points, and wireless client systems.

Mobile Applicability

WiFi is one of the primary methods of network access for mobile devices, and an array of mitigations can be applied to protect both devices and networks. As an example, wireless access can be restricted to a subset of authorized devices and WiFi networks can be properly encrypted. The definition of wireless for mobile also includes cellular, Bluetooth, NFC, and other medium- to short-range wireless protocols.

Mobile Deployment Considerations

Disabling wireless interfaces will be difficult in personally enabled scenarios, and potentially infeasible with unmanaged devices. An administrator will need some form of presence on the device in order to monitor and recommend these device configuration settings. Fully managed devices can also be made to prevent the installation of P2P applications.

Mobile Additional Discussion

Unlike traditional systems, connections via Telnet or Secure Shell (SSH) to the mobile device are not a large concern, unless the device in question is jailbroken or rooted. Mobile devices are still susceptible to network level man-in-the-middle attacks, such as TLS stripping and address resolution protocol (ARP) poisoning. These attacks can allow an attacker to sniff unencrypted traffic, or reroute traffic to insecure web sites, leading to credential theft. Some MTD on-device agents can detect these attacks and notify a user / administrator. Developers can implement certificate pinning to help stop these types of network-based attacks as well.

Traditional guidance on WiFi security applies, such as using strong credentials and restricting unauthorized device connectivity. If WiFi Protected Access-Pre-Shared Key (WPA2-PSK) is used, a strong password is necessary, although 802.1x is preferred.

CIS Control 15: Wireless Access Control			Applicability	
Sub-Control	Control Title	Control Descriptions	Included	Justification
15.1	Maintain an Inventory of Authorized Wireless Access Points	Maintain an inventory of authorized wireless access points connected to the wired network.		Although important, there is nothing mobile-specific within this Sub-Control.
15.2	Detect Wireless Access Points Connected to the Wired Network	Configure network vulnerability scanning tools to detect and alert on unauthorized wireless access points connected to the wired network.		Although important, there is nothing mobile-specific within this Sub-Control.
15.3	Use a Wireless Intrusion Detection System	Use a wireless intrusion detection system (WIDS) to detect and alert on unauthorized wireless access points connected to the network.	•	IDS systems that work for traditional networks generally have mobile-specific capabilities in today's products. Expanding on the initial intent of this Control, devices exist that search for rogue wireless clients. This includes WiFi, Bluetooth, and potentially cellular identities as well.
15.4	Disable Wireless Access on Devices if Not Required	Disable wireless access on devices that do not have a business purpose for wireless access.	•	Although this can create usability issues for the users, it is a legitimate threat surface reduction tactic. This is not advocating the use of airplane mode, but instead turn off WiFi and switch to cellular in certain high-security situations.
15.5	Limit Wireless Access on Client Devices	Configure wireless access on client machines that do have an essential wireless business purpose, to allow access only to authorized wireless networks and to restrict access to other wireless networks.		Employee devices with enterprise access will need wireless networking to function.
15.6	Disable Peer-to-Peer Wireless Network Capabilities on Wireless Clients	Disable peer-to-peer (ad hoc) wireless network capabilities on wireless clients.		This is less of a concern on mobile, but rooted / jailbroken devices can utilize P2P applications.

CIS Control 15: Wireless Access Control			Applicability	
Sub-Control	Control Title	Control Descriptions	Included	Justification
15.7	Leverage the Advanced Encryption Standard (AES) to Encrypt Wireless Data	Leverage the Advanced Encryption Standard (AES) to encrypt wireless data in transit.	•	Users can be trained to avoid open wired equivalent policy (WEP) and WiFi Protected Access (WPA) networks and prefer those using WPA2 with counter mode with cipher block chaining message authentication code protocol, or CCMP.
15.8	Use Wireless Authentication Protocols That Require Mutual, Multi-Factor Authentication	Ensure that wireless networks use authentication protocols such as Extensible Authentication Protocol-Transport Layer Security (EAP/TLS) that requires mutual, multi-factor authentication.	•	Enterprises can leverage 802.1x in order to meet this Sub-Control, although this generally doesn't apply to unmanaged scenarios.
15.9	Disable Wireless Peripheral Access to Devices	Disable wireless peripheral access of devices [such as Bluetooth and Near Field Communication (NFC)], unless such access is required for a business purpose.	•	Although this can create usability issues for the users, it is a legitimate threat surface reduction tactic. This is not advocating the use of airplane mode, but instead turn off Bluetooth and other short range protocols in certain situations.
15.10	Create Separate Wireless Network for Personal and Untrusted Devices	Create a separate wireless network for personal or untrusted devices. Enterprise access from this network should be treated as untrusted and filtered and audited accordingly.	•	This Sub-Control has important implications for device usage models, as personal devices, even if managed, would not be allowed on an enterprise network.

CIS Control 16: Account Monitoring and Control

Actively manage the life cycle of system and application accounts - their creation, use, dormancy, deletion - in order to minimize opportunities for attackers to leverage them.

Mobile Applicability

Account management is applicable to mobile devices and their management platforms. This CIS Control is primarily enforced at the back-end management systems, and not within the device. Yet the mobile OS and applications must also be managed.

Mobile Deployment Considerations

It is more difficult, or sometimes not possible, for enterprises to monitor accounts on unmanaged devices. On-device EMM agents can give enterprises access to the list of applications on the device, which can make it easier to monitor which third-party applications are being utilized.

Mobile Additional Discussion

Administrators should regularly review user accounts on all systems utilized by the enterprise. Privileges should be adjusted accordingly on a regular basis with over-privileged users losing access and unneeded accounts deactivated when necessary.

Cloud-based applications supported by the enterprise must be monitored and have their credentials disabled during employee separation. Enterprise apps should be analyzed and reviewed for proper authentication techniques. Special attention should be focused on areas where integration occurs between third-party services and when identities are federated. Logging should be enabled within back-end management services to monitor activity, with the logs regularly reviewed.

CIS Control 16: Account Monitoring and Control			Applicability	
Sub-Control	Control Title	Control Descriptions	Included	Justification
16.1	Maintain an Inventory of Authentication Systems	Maintain an inventory of each of the organization's authentication systems, including those located on-site or at a remote service provider.		Although an important Sub-Control, mobile-specific authentication systems are not commonplace.
16.2	Configure Centralized Point of Authentication	Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.		This is difficult to accomplish when Google and Apple accounts are necessary to enable even basic mobile device functionality.
16.3	Require Multi-Factor Authentication	Require multi-factor authentication for all user accounts, on all systems, whether managed on-site or by a third-party provider.	•	Although not all applications support this, where possible it should be performed. 2FA for the lock screen is out of scope for this Control.

CIS Control 16: Account Monitoring and Control			Applicability	
Sub-Control	Control Title	Control Descriptions	Included	Justification
16.4	Encrypt or Hash All Authentication Credentials	Encrypt or hash with a salt all authentication credentials when stored.		The authentication methods used by apps are often difficult to understand as a third-party, even with documentation available. Authentication protocols like those supported by the file integrated design and operations (FIDO) alliance often do not simply encrypt or hash credentials and can be significantly more complicated.
16.5	Encrypt Transmittal of Username and Authentication Credentials	Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.	•	This is an important Sub-Control for mobile systems, and authentication data should be cryptographically protected using modern means.
16.6	Maintain an Inventory of Accounts	Maintain an inventory of all accounts organized by authentication system.	•	This is an important Sub-Control, and must be accomplished via technical and procedural means. To accomplish it, enterprises must be aware of the different apps and platforms that their employees are utilizing. This is sometimes difficult as shadow IT can be difficult to detect and remediate.
16.7	Establish Process for Revoking Access	Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor. Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.	•	In addition to typical workstations and servers, administrators should define this process specifically for mobile devices and their management platforms.
16.8	Disable Any Unassociated Accounts	Disable any account that cannot be associated with a business process or business owner.	•	Just as with traditional systems, accounts that are not linked to an approved user should be disabled.
16.9	Disable Dormant Accounts	Automatically disable dormant accounts after a set period of inactivity.	•	In a manner similar to traditional systems, dormant accounts should be disabled after a pre-defined period of inactivity.

CIS Control 16: Account Monitoring and Control			Applicability	
Sub-Control	Control Title	Control Descriptions	Included	Justification
16.10	Ensure All Accounts Have An Expiration Date	Ensure that all accounts have an expiration date that is monitored and enforced.	•	To the extent possible on mobile devices and within applications, accounts should not be created to be used in perpetuity.
16.11	Lock Workstation Sessions After Inactivity	Automatically lock workstation sessions after a standard period of inactivity.	•	All devices should be configured to have their lock screens automatically lock after a defined period of time.
16.12	Monitor Attempts to Access Deactivated Accounts	Monitor attempts to access deactivated accounts through audit logging.	•	Attempts to access disabled or deactivated accounts are logged.
16.13	Alert on Account Login Behavior Deviation	Alert when users deviate from normal login behavior, such as time-of-day, workstation location, and duration.	•	When abnormal behavior for an account occurs, the necessary parties are properly notified.

CIS Control 17: Implement a Security Awareness and Training Program

For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.

Mobile Applicability

Users and administrators should be trained on risks and threats specific to mobile platforms. Security awareness training can be tailored to remote employees, contractors, and all employees accessing corporate email using mobile devices.

Mobile Deployment Considerations

Remote employees, and those using devices in a BYOD mobile deployment scenario, should be provided security awareness training dedicated to the threats most affecting BYOD. This includes device loss and theft, data loss via malicious applications, application data (AD) credential theft via phishing, and the mixing of personal / enterprise information. More traditional mobile deployment scenarios are also at risk, but BYOD should be given additional time and consideration, with the importance of these issues impressed upon the employee.

Mobile Additional Discussion

Many of the risks and threats affecting mobile users require direct user interaction in order to be mitigated - even if there is an MDM or enterprise administrator managing the device. The large majority of CIS Sub-Controls applicable to mobile that are not technically implementable are candidates for security awareness training. Candidates include CIS Controls 5.1 (Establish Secure Configurations), 7.1 (Ensure Use of Only Fully Supported Browsers and Email Clients), 15.7 [Leverage the Advanced Encryption Standard (AES) to Encrypt Wireless Data], and 15.10 (Create Separate Wireless Network for Personal and Untrusted Devices). Many of these Controls are not necessarily for mobile devices, but are infrastructure components that enable secure usage. Additional items include enterprise policies surrounding trustworthy replaceable components (e.g., digitizer, screen, battery). For instance, devices accessing enterprise information should not be replaced by an untrustworthy technician as they will have unsupervised physical access with the device and may install malicious components / software.

Security awareness training for mobile should at first focus on lock screen security and the prevention or mitigation of device loss / theft. Additionally, serious focus should be provided for SMS phishing and various ways that users can be tricked into clicking on dangerous links or installing Trojan mobile apps that will steal passwords. Subscriber Identity Module (SIM) swapping can also be a dangerous social engineering technique that can affect an enterprise that users should be aware of. Employees should be trained against these types of attacks via regularly scheduled white hat phishing campaigns that are specific to mobile.

CIS Control 17: Implementation a Security Awareness and Training Program			Applicability	
Sub-Control	Control Title	Control Descriptions	Included	Justification
17.1	Perform a Skills Gap Analysis	Perform a skills gap analysis to understand the skills and behaviors workforce members are not adhering to, using this information to build a baseline education roadmap.	•	Employees use mobile devices differently than laptops or traditional workstations. Understanding the habits of users can help focus future cybersecurity awareness training. For instance, are employees using a personal identification number (PIN) or passcode to protect their lock screen?
17.2	Deliver Training to Fill the Skills Gap	Deliver training to address the skills gap identified to positively impact workforce members' security behavior.	•	Once a gap analysis has been performed, specific training should be provided to heavy users of mobile and those involved in BYOD scenarios.
17.3	Implement a Security Awareness Program	Create a security awareness program for all workforce members to complete on a regular basis to ensure they understand and exhibit the necessary behaviors and skills to help ensure the security of the organization. The organization's security awareness program should be communicated in a continuous and engaging manner.	•	A holistic, long-term approach should be developed to address user education concerns surrounding the use of mobile.
17.4	Update Awareness Content Frequently	Ensure that the organization's security awareness program is updated frequently (at least annually) to address new technologies, threats, standards, and business requirements.	•	Consistent updates to user awareness training can help ensure employees know the latest threats.
17.5	Train Workforce on Secure Authentication	Train workforce members on the importance of enabling and utilizing secure authentication.	•	Secure authentication is different on mobile platforms and employees should know the security risks and implications of using SMS as a second factor. This method of authentication is no longer supported by NIST for U.S. agencies.

CIS Control 17: Implementation a Security Awareness and Training Program			Applicability	
Sub-Control	Control Title	Control Descriptions	Included	Justification
17.6	Train Workforce on Identifying Social Engineering Attacks	Train the workforce on how to identify different forms of social engineering attacks, such as phishing, phone scams, and impersonation calls.	•	Pre-texting by phone is common and can be used to obtain information about the mobile devices and applications used by the enterprise.
17.7	Train Workforce on Sensitive Data Handling	Train workforce members on how to identify and properly store, transfer, archive, and destroy sensitive information.	•	Users should understand what data is sensitive on their mobile devices and how to prevent commingling alongside personal information.
17.8	Train Workforce on Causes of Unintentional Data Exposure	Train workforce members to be aware of causes for unintentional data exposures, such as losing their mobile devices or emailing the wrong person due to *autocomplete* in email.	•	This can be tailored to mobile-specific causes such as installing insecure apps on corporate devices or forgoing multifactor authentication.
17.9	Train Workforce Members on Identifying and Reporting Incidents	Train workforce members to be able to identify the most common indicators of an incident and be able to report such an incident.	•	Employees can be trained on what successful attacks on mobile devices look like, and to whom they should be reported.

CIS Control 18: Application Software Security

Manage the security life cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.

Mobile Applicability

The security of individual mobile applications is important, as millions of apps are freely available for personal and business use. These apps may reside within official public appstores (i.e., Apple's App Store, Google's Play Store), unofficial public stores (e.g., Amazon Appstore, Cydia), or private appstores / repos hosted by enterprises. Appstores hosted by an organization are often referred to as *private appstores* or *enterprise appstores*. These private appstores are often used to host apps that are developed in-house and are not available to the general public. Secure software development is a complex process that has unique considerations for mobile. Once apps are developed, they typically go through a process known as "mobile app vetting" to analyze the security of an app. The tools, procedures, and testing processes for engaging in application security for mobile apps is generally different.

Mobile Deployment Considerations

It is more difficult to ensure that properly vetted apps are running on unmanaged devices. Fully managed devices can whitelist apps and prevent the installation of unwanted ones. Managed devices can have profiles that sign privately developed apps, allowing them to bypass the restrictions of the primary appstores. This potentially provides additional functionality and usage of private or sensitive APIs.

Mobile Additional Discussion

Mobile apps may leverage web technologies in whole or part or may solely leverage the mobile frameworks provided by the OS. Web technologies are not the only external technologies that may be utilized to develop mobile apps. Third-party mobile libraries, software development kits (SDKs), and libraries created for more traditional server and enterprise use cases may be embedded into mobile apps. Mobile application vetting can help to identify if there are discrete software vulnerabilities that can be exploited within any of the technologies used within the application. Additionally unintentional dangerous behavior and malware embedded into the application can be found. Examples of mobile application risks include accessing sensitive personal information (e.g., text messages, photos, contacts), sensitive enterprise information, or directly attacking the underlying operating system and firmware. Malicious native apps have also been seen to be turning on the camera or microphone, logging geolocation, capturing credentials, initiating toll calls or texts, or creating nuisance issues like resource saturation that drains the battery.

- The Open Web Application Security Project (OWASP) Mobile Top 10 is a great resource to begin to understand the mistakes that developers can make when writing apps.
- OWASP also provides a Mobile Application Security Testing Guide.
- NIST provides guidance on testing and vetting mobile applications via NIST SP 800-163 Revision 1: Vetting the Security of Mobile Applications.
- The National Information Assurance Partnership (NIAP) provides guidelines for vetting mobile apps based on the requirements found in the Protection Profile for Application Software.

- NowSecure provides Secure Mobile Development Best Practices Guides https://info.nowsecure.com/rs/201-XEW-873/images/secure-mobile-development.pdf
- NowSecure provides a Mobile Application Security Testing Checklist https://info.nowsecure.com/rs/201-XEW-873/images/mobile-appsec-testing-checklist.pdf

It is extremely important to ensure that users are installing legitimate versions of an app; and that those apps are up-to-date. Trojan and repackaged apps are some of the most pernicious and successful types of malware in the Google Play store, per Google's Android Security 2017 Report.

CIS Control 18: Application Software Security			Applicability	
Sub-Control	Control Title	Control Descriptions	Included	Justification
18.1	Establish Secure Coding Practices	Establish secure coding practices appropriate to the programming language and development environment being used.	•	Apple's developer portal provides An Introduction to Secure Coding page for Swift. Google provides safe coding practices and other resources for Kotlin.
18.2	Ensure That Explicit Error Checking Is Performed for All In-House Developed Software	For in-house developed software, ensure that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats.	•	Error checking is an important software assurance concept and is still necessary in the languages used to develop mobile applications.
18.3	Verify That Acquired Software Is Still Supported	Verify that the version of all software acquired from outside your organization is still supported by the developer or appropriately hardened based on developer security recommendations.	•	Using apps that are no longer supported for mobile tasks exposes sensitive enterprise data via application-level vulnerabilities and misconfigurations.
18.4	Only Use Up-to-Date and Trusted Third-Party Components	Only use up-to-date and trusted third-party components for the software developed by the organization.	•	All of the libraries and development kits compiled or injected into an app must be supported.
18.5	Use only Standardized and Extensively Reviewed Encryption Algorithms	Use only standardized, currently accepted, and extensively reviewed encryption algorithms.	•	Most mobile devices come with standardized cryptographic algorithms with sufficient key sizes built into the mobile OS. These are available through well-documented and exposed APIs.

CIS Control 18: Application Software Security			Applicability	
Sub-Control	Control Title	Control Descriptions	Included	Justification
18.6	Ensure Software Development Personnel Are Trained in Secure Coding	Ensure that all software development personnel receive training in writing secure code for their specific development environment and responsibilities.	•	Classes and training materials are easily available online and in-person to educate developers on the common pitfalls of secure software development for mobile platforms.
18.7	Apply Static and Dynamic Code Analysis Tools	Apply static and dynamic analysis tools to verify that secure coding practices are being adhered to for internally developed software.	•	Many companies offer these types of services for mobile applications. These systems can be deployed on-premises or apps can be uploaded, reviewed, and a report returned. Although Apple and Google vet apps in some way before granting access to the store, it is unclear exactly what is performed and developers should not count on these processes for security.
18.8	Establish a Process to Accept and Address Reports of Software Vulnerabilities	Establish a process to accept and address reports of software vulnerabilities, including providing a means for external entities to contact your security group.	•	Enterprises should be set up for vulnerability disclosure associated with mobile software.
18.9	Separate Production and Non-Production Systems	Maintain separate environments for production and non-production systems. Developers should not have unmonitored access to production environments.	•	Non-production systems should not be exposed to untrusted parties, as they commonly store sensitive data, but are often not hardened or running up-to-date software.

CIS Control 18: Application Software Security			Applicability	
Sub-Control	Control Title	Control Descriptions	Included	Justification
18.10	Deploy Web Application Firewalls	Protect web applications by deploying web application firewalls (WAFs) that inspect all traffic flowing to the web application for common web application attacks. For applications that are not web-based, specific application firewalls should be deployed if such tools are available for the given application type. If the traffic is encrypted, the device should either sit behind the encryption or be capable of decrypting the traffic prior to analysis. If neither option is appropriate, a host-based web application firewall should be deployed.		This are typically not available on mobile platforms.
18.11	Use Standard Hardening Configuration Templates for Databases	For applications that rely on a database, use standard hardening configuration templates. All systems that are part of critical business processes should also be tested.		These templates are typically unavailable for mobile.

CIS Control 19: Incident Response and Management

Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.

Mobile Applicability

Traditional incident response (IR) guidance applies, most of which can be tailored to mobile. This includes the need for planning, defining roles and responsibilities, and identifying escalation paths. Now that many users access company data and services with mobile devices in a manner similar to PCs, the need to identify, investigate, respond, and recover from incidents involving mobile devices is important. A mobile incident response plan is sometimes separate from the normal plan, but many times it is folded into an organization's overall strategy.

Mobile Deployment Considerations

Significant challenges exist for incident response activities associated with BYOD devices. Incident response activities can severely affect an employee's or contractor's personal privacy. An individual's mobile phone can be considered an intimate part of their life, as the personal data stored within is quite sensitive. Individuals often have their entire digital life on their phones, from texts, calendar, contacts, and photos. Reverse-engineering the path someone's taken in the world is possible via the geolocation metadata from pictures, social networking check-ins, and applications that store a person's "last active location." It is also possible to reveal someone's personal contact network via phone logs, text messages, email, and private social network accounts.

Mobile Additional Discussion

Operations personnel and incident responders need to be trained on what to look for with unusual behavior on the mobile devices. For example, if a user receives hundreds of messages around the same time from an account or application on the device, it is often a sign that a service or device has been compromised. A major challenge in mobile response and recovery activities is the vast quantity of different types of mobile device hardware, even among generations of products. When considering data forensics for mobile devices, a wealth of different types of data is available to support the objective of the acquisition; be it eDiscovery, misuse, or evidence collection to support a criminal case.

NowSecure offers a free guide to mobile incident response activities. The guide contains a number of real-world case studies to assist individuals charged with IR activities for mobile. For more information on mobile forensics procedures, you can refer to NIST SP 800-101: Guidelines on Mobile Device Forensics.

CIS Control 19: Incident Response and Management			Applicability	
Sub-Control	Control Title	Control Descriptions	Included	Justification
19.1	Document Incident Response Procedures	Ensure that there are written incident response plans that define roles of personnel as well as phases of incident handling/management.	•	Written plans for EMM and mobile device breaches are key to mobile incident response.
19.2	Assign Job Titles and Duties for Incident Response	Assign job titles and duties for handling computer and network incidents to specific individuals, and ensure tracking and documentation throughout the incident through resolution.	•	Especially if an enterprise is supporting a mobile application, personnel should be dedicated to mobile IR and understand the fundamentals of EMM, iOS, and Android.
19.3	Designate Management Personnel to Support Incident Handling	Designate management personnel, as well as backups, who will support the incident handling process by acting in key decision-making roles.	•	Management and backup personnel should be specifically appointed for mobile incident response.
19.4	Devise Organization-wide Standards For Reporting Incidents	Devise organization-wide standards for the time required for system administrators and other workforce members to report anomalous events to the incident handling team, the mechanisms for such reporting, and the kind of information that should be included in the incident notification.	•	Standards for reporting mobile incidents should be put in place that are mandated across the enterprise. This should include the time to report, types of anomalous events, and the details of any relevant mobile incident.
19.5	Maintain Contact Information For Reporting Security Incidents	Assemble and maintain information on third-party contact information to be used to report a security incident, such as Law Enforcement, relevant government departments, vendors, and Information Sharing and Analysis Center (ISAC) partners.	•	Information for specific individuals and external organizations should be maintained for whom should be contacted regarding mobile security incidents.
19.6	Publish Information Regarding Reporting Computer Anomalies and Incidents	Publish information for all workforce members, regarding reporting computer anomalies and incidents, to the incident handling team. Such information should be included in routine employee awareness activities.	•	Information regarding mobile breaches and other incidents should be made available to internal employees. This information can be fed back into awareness training.

CIS Control 19: Incident Response and Management			Applicability	
Sub-Control	Control Title	Control Descriptions	Included	Justification
19.7	Conduct Periodic Incident Scenario Sessions for Personnel	Plan and conduct routine incident response exercises and scenarios for the workforce involved in the incident response to maintain awareness and comfort in responding to real-world threats. Exercises should test communication channels, decision making, and incident responder's technical capabilities using tools and data available to them.	•	Breaches of mobile apps and management systems can be periodically assessed in order to test mobile incident response procedures. This also helps to keep the necessary individuals aware of the mobile IR procedures.
19.8	Create Incident Scoring and Prioritization Schema	Create incident scoring and prioritization schema based on known or potential impact to your organization. Utilize score to define frequency of status updates and escalation procedures.	•	Depending on their criticality to the organization, a security incident affecting mobile systems may be more or less important to the enterprise.

CIS Control 20: Penetration Tests and Red Team Exercises

Test the overall strength of an organization's defense (the technology, the processes, and the people) by simulating the objectives and actions of an attacker.

Mobile Applicability

Traditional penetration testing and Red Team activities, such as running scans to see which ports are open, and what vulnerable services they are supporting, does not apply. However, penetration testing of mobile deployments is an important and worthwhile activity. The use of mobile generally expands the attack surface of an organization, making additional methods available to attackers for social engineering and technical attacks on devices and apps. For instance, SIM swapping is applicable to mobile devices but not most other types of systems.

Mobile Deployment Considerations

Penetration testers and Red Team members should pay extra care in securing authorization to perform vulnerability assessment and penetration testing activities on BYOD devices. Specific user approval may be necessary in addition to any authorization to what is typically provided by the enterprise. Accidentally deleting a user's personal data or bricking their mobile device could cause contractual and legal difficulties.

Mobile Additional Discussion

Many of the attack techniques discussed throughout this document, such as sniffing mobile traffic over the air and man-in-the-middle attacks, are possible. As discussed in CIS Control 18, potentially the most vulnerable portions of your mobile deployment may be the mobile apps themselves. The traditional approach for mobile app testing has been code review tools, but standard web proxy tools and web application penetration testing techniques are possible and should be explored. Use of an experimental lab and test devices for more thorough hardware examination is also relevant to mobile. NowSecure offers guidance for performing penetration testing activities on mobile devices.

CIS Control 20: Penetration Tests and Red Team Exercises			Applicability	
Sub-Control	Control Title	Control Descriptions	Included	Justification
20.1	Establish a Penetration Testing Program	Establish a program for penetration tests that includes a full scope of blended attacks, such as wireless, client-based, and web application attacks.	•	A penetration testing program focused on mobile systems will include any relevant mobile applications, mobile devices, and management infrastructure.
20.2	Conduct Regular External and Internal Penetration Tests	Conduct regular external and internal penetration tests to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems successfully.	•	The frequency of testing can be difficult to determine, especially when multiple versions of an app can be pushed in a single day. This will be a decision decided by the organization in question.
20.3	Perform Periodic Red Team Exercises	Perform periodic Red Team exercises to test organizational readiness to identify and stop attacks or to respond quickly and effectively.	•	Red Team exercises focused on mobile systems will include any relevant mobile applications, mobile devices, and management infrastructure.
20.4	Include Tests for Presence of Unprotected System Information and Artifacts	Include tests for the presence of unprotected system information and artifacts that would be useful to attackers, including network diagrams, configuration files, older penetration test reports, emails or documents containing passwords or other information critical to system operation.	•	Red Team tests should look for passwords, digital certificates, and other artifacts that will allow them to access mobile devices and EMMs.
20.5	Create a Test Bed for Elements Not Typically Tested in Production	Create a test bed that mimics a production environment for specific penetration tests and Red Team attacks against elements that are not typically tested in production, such as attacks against supervisory control and data acquisition and other control systems.	•	EMMs may be prime examples of elements not typically tested in Red Team exercises.
20.6	Use Vulnerability Scanning and Penetration Testing Tools in Concert	Use vulnerability scanning and penetration testing tools in concert. The results of vulnerability scanning assessments should be used as a starting point to guide and focus penetration testing efforts.	•	Although this can be done in a manner similar to normal desktop systems, it may not be as effective for mobile devices.

CIS Control 20: Penetration Tests and Red Team Exercises			Applicability	
Sub-Control	Control Title	Control Descriptions	Included	Justification
20.7	Ensure Results From Penetration Test Are Documented Using Open, Machine-Readable Standards	Wherever possible, ensure that Red Team results are documented using open, machine-readable standards (e.g., SCAP). Devise a scoring method for determining the results of Red Team exercises so that results can be compared over time.	•	Mobile results can be documented in a similar manner as traditional systems. The Mobile version of ATT&CK can also provide value in helping to explain test results to outside parties.
20.8	Control and Monitor Accounts Associated With Penetration Testing	Any user or system accounts used to perform penetration testing should be controlled and monitored to make sure they are only being used for legitimate purposes, and are removed or restored to normal function after testing is over.	•	Any tools designed to penetrate mobile devices should be monitored and routinely audited.

Acronyms and Abbreviations

2F2	Two-Factor Authentication
AD	Application Datat
ADB	Android Debug Bridge
AES	Advanced Encryption Standard
API	Application Programming Interface
ARP	Address Resolution Protocol
ASLR	Address Space Layout Randomization
B2B	Business-to-Business
BYOD	Bring Your Own Device
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMVP	Cryptographic Module Validation Program
COPE	Corporate Owned, Personally Enabled
CVSS	Common Vulnerability Scoring System
DMARC	Domain-based Message Authentication Reporting and Conformance
DEP	Data Execution Prevention
DHCP	Dynamic Host Configuration Protocol
DKIM	Domain Key Identifier Mail
DLP	Data Loss Prevention
DNS	Domain Name System
DRM	Digital Rights Management
EAP/TLS	Extensible Authentication Protocol-Transport Layer Security
EMM	Enterprise Mobility Management
FIDO	File Integrated Design and Operations
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act
GLONASS	Global Navigation Satellite System
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure
IDS	Intrusion Detection Systems
IMEI	International Mobile Equipment Identifier
IMSI	International Mobile Subscriber Identity
iOS	Internet Operating System
IoT	Internet of Things
IPS	Intrusion Prevention Systems
IPSec	Internet Protocol Security
IR	Incident Response

ISAC	Information Sharing and Analysis Center
IT	Information Technology
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Control
MAM	Mobile Application Management
MAV	Mobile Application Vetting
MCDF	Mobile Computing Decision Framework
MDM	Mobile Device Management
MitM	Man-in-the-Middle
MTD	Mobile Threat Defense
MTP	Mobile Threat Protection
NFC	Near Field Communication
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NITZ	Network Identify and Time Zone
Nmap	Network Mapper
NTP	Network Time Protocol
OEM	Original Equipment Manufacturer
OS	Operating System
OWASP	Open Web Application Security Project
P2P	Peer to Peer
PAN	Personal Area Network
PC	Personal Computer
PDF	Portable Document Format
PHA	Potentially Harmful Applications
PII	Personally Identifiable Information
PIN	Personal Identification Number
PSTN	Public Switched Telephone Network
QR	Quick Response
RADIUS	Remote Authentication Dial-In User Service
RFID	Radio Frequency Identification
RTOS	Real Time Operating System
SCAP	Security Control Automation Protocol
SDK	Software Development Kit
SIEM	Security Information and Event Management
SIM	Subscriber Identity Module
SMS	Short Message Service
SoC	System on a Chip
SP	Special Publication
SPF	Sender Policy Framework
SSH	Secure Shell

SSID	Service Set Identifier
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TPM	Trusted Platform Module
UEM	Unified Endpoint Management
UICC	Universal Integrated Circuit Card
URL	Uniform Resource Locator
USB	Universal Serial Bus
VMI	Virtual Mobile Infrastructure
VPN	Virtual Private Network
WAF	Web Application Firewalls
WEP	Wired Equivalent Policy
WIDS	Wireless Intrusion Detection System
WiFi	Wireless Fidelity
WLAN	Wireless LAN
WPA	WiFi Protected Access
WPA2/PSK	WiFi Protected Access-Pre-Shared Key
WPAN	Wireless Personal Area Network

Links and Resources

- CIS Controls
  https://www.cisecurity.org/controls/
- SANS Institute
  https://www.sans.org/findtraining/
- ICS ISAC
  http://ics-isac.org/blog/
- ICS Cert
  https://ics-cert.us-cert.gov/
- ICS Security Resources and Tools
  http://www.chemicalcybersecurity.org/RESOURCES-And-TOOLS
- Special Publication (SP) 800-53 Revision 4
  https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final
- Managing Devices & Corporate Data on iOS
  https://www.apple.com/business/resources/docs/Managing_Devices_and_Corporate_Data_on_iOS.pdf
- Android mobility best practice advisory
  https://static.googleusercontent.com/media/www.google.com/en/US/work/android/files/best-practice-advisory.pdf
- Cloud Security Alliance Mobile Working Group
  https://downloads.cloudsecurityalliance.org/initiatives/mobile/Mobile_Guidance_v1.pdf
- Android Developer Page on Application Signing
  https://source.android.com/security/apksigning
- Apple's iOS Security Guide
  https://www.apple.com/ca/business-docs/iOS_Security_Guide.pdf
- Overview of Android Management
  https://androidenterprisepartners.withgoogle.com/
- Overview of iOS management
  https://help.apple.com/configurator/mac/2.8/#/cade8b212c76
- Apple DEP Program
  https://support.apple.com/en-us/HT204142
- NIAP Approved Product List
  https://www.niap-ccevs.org/Product/index.cfm
- Mobile version of ATT&CK
  https://attack.mitre.org/tactics/mobile/
- Now Secure mobile incident response
  https://books.nowsecure.com/mobile-incident-response/en/overview/ir-process.html
- Open Web Application Security Project (OWASP) Mobile Top 10
  https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10
- Mobile Application Security Testing Guide
  https://www.owasp.org/index.php/OWASP_Mobile_Security_Testing_Guide
- NIST SP 800-163 Revision 1: Vetting the Security of Mobile Applications
  https://csrc.nist.gov/publications/detail/sp/800-163/final
- NIAP Protection Profile for Application Software
  https://niap-ccevs.org/MMO/PP/394.R/pp_app_v1.2_table-reqs.htm
- NIST SP 800-101: Guidelines on Mobile Device Forensics
  https://csrc.nist.gov/publications/detail/sp/800-101/rev-1/final
- Apple Introduction to Secure Coding
  https://developer.apple.com/library/archive/documentation/Security/Conceptual/SecureCodingGuide/Introduction.html
- Google Kotlin Safe Coding Practices
  https://kotlinlang.org/docs/reference/coding-conventions.html
- Google's Android Security 2017 Year In Review
  https://source.android.com/security/reports/Google_Android_Security_2017_Report_Final.pdf

Closing Notes

In this document, we provide guidance on how to apply the security best practices found in CIS Controls Version 7 to cloud environments. The newest version of the CIS Controls and other complementary documents may be found at www.cisecurity.org.

As a nonprofit organization driven by its volunteers, we are always in the process of looking for new topics and assistance in creating cybersecurity guidance. If you are interested in volunteering and/or have questions, comments, or have identified ways to improve this guide, please write us at: controlsinfo@cisecurity.org.

All references to tools or other products in this document are provided for informational purposes only, and do not represent the endorsement by CIS of any particular company, product, or technology.

Contact Information

CIS
31 Tech Valley Drive
East Greenbush, NY 12061
518.266.3460
controlsinfo@cisecurity.org