Homeland Security

U.S. Department of Homeland Security

DHS 4300A, "*Information Technology System Security Program, Sensitive Systems*"

Attachment I

Sensitive Mobile Devices

Version 1.0

January 22, 2022

Protecting the Information that Secures the Homeland

DOCUMENT CHANGE HISTORY

Version	Date	Description
1.0	January 22, 2022	Initial draft

CONTENTS

1.0 INTRODUCTION

This document provides techniques and procedures for the secure use of mobile devices within the Department of Homeland Security (DHS) Information Technology (IT) Program. It is an Attachment to the DHS Policy Directive 4300A, "*Information Technology System Security Program (ITSSP), Sensitive Systems*" (hereafter referred to as DHS 4300A) which is based on with DHS Management Directive 140-01, "*Information Technology Security Program*." The DHS 4300A Policy Directive contains wireless security requirements.

DHS Components should use the guidance in this Attachment as a foundation for developing and implementing wireless IT security programs. This Attachment incorporates many security techniques and procedures already in use by DHS Components and other Federal entities such as the National Institute of Standards and Technology (NIST), the National Security Agency (NSA), and the Department of Defense (DoD).

1.1 PURPOSE AND SCOPE

The guidance in this document is intended to amplify policy requirements and to provide a detailed explanation of the many countermeasures that can be applied to mobile devices. Because of the rapid evolution of mobile and wireless technology, all available countermeasures may not be described in this Attachment.

System Security Plans should address all currently effective security controls required to obtain Authority to Operate (ATO). The security checklist in Appendix A provides a summary of mobile device security guidelines.

Authorizing Officials (AO) should understand the risks associated with each particular mobile device, applying some or all of the countermeasures outlined in this Attachment. They should ensure that each risk is measured and mitigated to an acceptable level according to DHS policy. In approving mobile devices, AOs should pay particular attention to the potential risks presented by mobile devices that have technological barriers to countermeasure implementation.

1.2 MOBILE DEVICE BASELINE

The following characteristics are derived from the NIST Special Publication (SP) 800-124[1], and define the mobile device baseline:

- Small form factor
- At least one wireless network interface for network access (data communications). This interface uses Wi-Fi, cellular networking, or other

[1] "Guidelines for Managing the Security of Mobile Devices in the Enterprise," March 2020 https://csrc.nist.gov/publications/detail/sp/800-124/rev-2/draft

- technologies that connect the mobile device to network infrastructures with connectivity to the Internet or other data networks.
- Local built-in (non-removable) data storage
- An operating system that is not a full-fledged desktop or laptop operating system
- Applications available through multiple methods (provided with the mobile device, accessed through web browser, acquired and installed from third parties)

Many mobile devices include advanced features, such as:

- Network services:
  - One or more wireless personal area network interfaces, such as Bluetooth or near-field communications (NFC)
  - One or more wireless network interfaces for data and voice communications, such as cellular (e.g., LTE or 5G)
  - Global Positioning System (GPS), which enables location services
- One or more digital cameras
- Video recording devices
- Speaker and/or Microphone
- Sensors – data captured via sensors can be used to perform operations such as authentication and measurements. Examples include: gyroscope, accelerometer, magnetometer

1.3 USE OF APPENDED CHECKLIST

The checklist "Security Requirements Checklist for Mobile Devices," (Appendix A to this Attachment) can be used by DHS Components to verify compliance with Policy (items shown as "Required," and implementation of guidance and best practices (items shown as "Recommended.")

1.4 DHS 4300A POLICY REQUIREMENTS

Mobile devices include smart cellular telephones, two-way pagers, mobile radios, personal communications services (PCS) devices, multifunctional wireless devices, portable audio/video recording devices with wireless capability, scanning devices, messaging devices, and any other wireless clients capable of storing, processing, or transmitting sensitive information.

1.4.1 SECURITY INCIDENT RESPONSE

Security controls are designed to protect an organization against security threats; however, regardless of how effective those controls are, some security incidents are inevitable. Organizations need to have an effective response capability in place before the occurrence of such events. *DHS 4300A Attachment F, Incident Response* provides detailed implementation guidance

1.4.2 SECURITY AWARENESS TRAINING

The goal of security awareness training is to educate DHS users to protect the confidentiality, integrity, and availability of DHS IT assets and data.

1.4.3 MOBILE DEVICE SECURITY POLICIES

DHS mobile device security policy can be found in DHS Policy Directive 4300A, *Information Technology System Security Program, Sensitive Systems.* DHS 4300A provides policy implementation guidance, addressing technology, legal, security, privacy, procedure, and usage issues related to mobile devices.

2.0 THREAT OVERVIEW

Mobile devices have become common place within agencies infrastructures because they offer many benefits in communication and collaboration while remaining location independent. Mobile devices, however, require strict security controls and governance to combat the rising threat these devices pose to DHS IT infrastructure and resources.

2.1 WIRELESS THREATS AND VULNERABILITIES

Wireless communications employ an inherently insecure medium; the technology can provide no security from interception or jamming. Due to the ubiquitous use of mobile devices in support of DHS missions, unauthorized disclosure of mobile device data-at-rest or data-in-transit can reasonably be expected to cause significant damage.

2.1.1 TAXONOMY OF WIRELESS ATTACK TYPES

Wireless systems are vulnerable to specifically engineered wireless attacks and to traditional wireline attacks. Attacks are categorized according to the following basic threat consequences: unauthorized disclosure, disruption, deception, and corruption. Generally, attacks fall into one of two categories: active or passive. Active attacks require actions on the part of the attacker to penetrate or disrupt the network, whereas passive attacks are used primarily for information gathering and surveillance. Figure 1 illustrates this taxonomy.

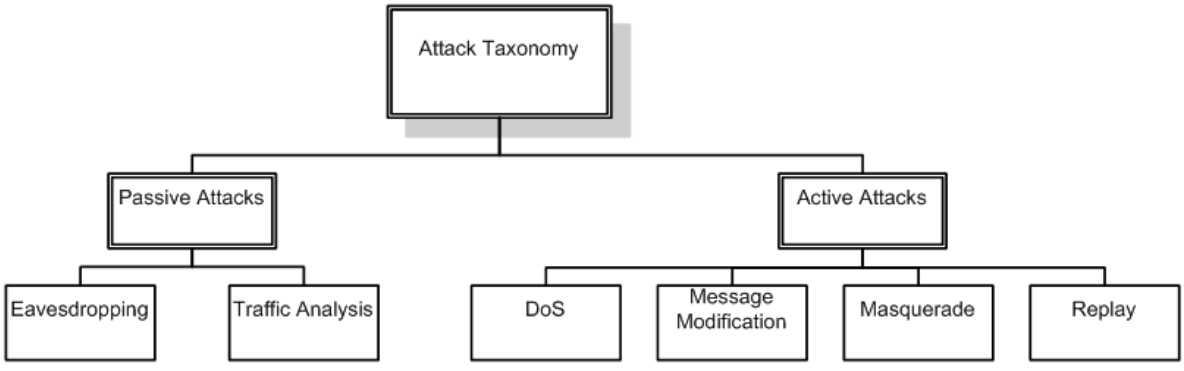

Figure 1: Taxonomy of Wireless Device Attack Types

2.1.1.1 Eavesdropping

Eavesdropping describes the threat whereby an attacker secretly captures wireless communication data. For instance, all wireless frames can be captured and inspected from a public wireless hotspot by any attacker using basic equipment and software.

Eavesdropping risk can be mitigated by using the federally-mandated Federal Information Processing Standard (FIPS) -140 validated data encryption for all sensitive data communications. Mobile device users are also required to use the DHS Virtual Private Network (VPN) service for remote access from locations not controlled by DHS.

2.1.2 TRAFFIC ANALYSIS

By secretly capturing and analyzing wireless communication data, an attacker could identify users and agencies, characterize the nature and pattern of the traffic, or identify the weakest link in security. Then the attacker can exploit networks based on their findings.

Implementation of this Attachment's guidance can provide safeguards against traffic analysis attacks. For instance, the wireless network footprint and power range should be carefully analyzed and controlled to minimize the wireless signal to outsiders. The use of strong FIPS-validated encryption also helps to counter this type of attack. Leveraging a layered security approach will further mitigate this threat.

2.1.2.1 Distributed Denial-of-Service (DDoS)

A Distributed Denial of Service (DDoS) attack on the wireless network occurs when an attacker floods the system with data packets, preventing or inhibiting legitimate users from accessing the network. Some physical layer DDoS attacks disrupt transmission by introducing interference with radio waves that prevent wireless hardware from properly receiving traffic. Disruptions can also be caused by other small appliances such as microwave ovens, cordless telephones, and other devices that use the same radio frequency bands as the attacked wireless network.

In a broad sense, a DDoS attack can happen at any of the seven Open Systems Interconnection (OSI) layers. In addition to the attacks that are unique to the wireless networks described above, well-known DDoS attacks include flooding networks with Ping packets, Transmission Control Protocol (TCP) messages, Web site access, and other seemingly legitimate types of wireless traffic. To counter DDoS attacks, DHS Components must implement a comprehensive defense-in-depth security strategy.

Data encryption mitigates DDoS attacks because most wireless hardware ignores traffic that is not properly encrypted. For a DDoS attack unique to the wireless environment, a wireless Intrusion Detection System (IDS), as described in *NIST SP 800-94 "Guide to Intrusion Detection and Prevention Systems (IDPS)*[2], can be used to detect and log

[2] NIST SP 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS) - https://csrc.nist.gov/publications/detail/sp/800-94/final

abnormal signals, and physically geolocate the suspicious devices via direction finding and triangulation algorithms. Wireless network monitoring and centralized management systems are also crucial to detecting and countering DDoS attacks. Furthermore, the wireless network and its associated systems must be integrated with firewalls, IDS, and wired network monitoring and management systems during the design and implementation phases.

2.1.2.2 Message Manipulations

Outside attackers can intercept and manipulate legitimate wireless messages with inclusions, deletions, additions, changes, and by reordering, or replaying legitimate messages.

Enabling appropriate FIPS 140 validated encryption can mitigate message manipulation threats, as the encryption algorithms are designed to protect the confidentiality and integrity of the data in wireless traffic. Wireless technology standards provide enhanced protection of data confidentiality and integrity using encryption, frame modification checking, frame discard and retransmission, and other security features. Data protection at higher layer protocols, such as dependable TCP using enhanced federally-mandated encryption and authentication, will also help to maintain the confidentiality and integrity of data.

2.1.2.3 Masquerading

Masquerading attackers disguise themselves as legitimate users, and try to access enterprise networks and resources. Wireless networks make this type of attack easier because attackers do not need to be physically connected to the wired network. In some cases, the attacker may be located outside of the agency's physical facility or campus.

Enabling FIPS 140 validated encryption can mitigate masquerading threats, as an adversary will be unable to masquerade data unless the attacker can validly encrypt the traffic. It will still be possible for an adversary to spoof Media Access Control (MAC) addresses, as these are unencrypted, but such activity is of limited use to the attacker.

Strong authentication requirements such as the use of two-factor authentication will mitigate the risks of a masquerading attack. DHS Components should implement strong digital identity management and user security training, and should follow the recommendations outlined in the NIST SP 800-63, "*Digital Identity Guidelines*" and the DHS 4300A, "*Information Technology System Security Program, Sensitive Systems*."

3.0 SECURING THE PHYSICAL DEVICE

A mobile device should be considered to be a critical component of the DHS wireless network and an extension of the DHS network infrastructure. Critical risks associated with securing the device include authentication of the user and the device, data protection, central management, monitoring of the device and application, malware protection, and physical security.

3.1 AUTHENTICATION

Identification and authentication will be implemented to access the device and the data on the device.

3.2 MOBILE THREAT DEFENSE

A MTD system has the ability to protect organizations from mobile threats. These systems often run an agent on the device—typically a mobile app—and may also initiate analysis and learning on external cloud-based platforms[3]. MTD systems provide real time, continuous monitoring protections at the device, network, and application level. For example, MTD can detect malicious apps and mobile OS vulnerabilities, man-in-the-middle (MitM) attacks, improper device configurations (e.g., rooted/jail broken). For further information, review the *NIST SP 800-124 "Guidelines for Managing the Security of Mobile Devices in the Enterprise."*

3.3 DISABLING UNDESIRABLE MOBILE DEVICE CAPABILITIES

Mobile device capabilities left in default unprotected configuration can be attack vectors to the mobile device or trusted network. Wireless capabilities that may not be required include infrared, Bluetooth, Wi-Fi, games, and other built-in tools and applications.

3.4 MOBILE DEVICE AND APPLICATION MANAGEMENT

IT security managers should limit mobile device deployment to DHS-sanctioned devices, technologies, and applications by using Mobile Device Management (MDM) systems. An MDM allows DHS to centrally manage mobile devices and enforce security policies on the devices by supporting the following key capabilities: malware detection, Over-the-Air (OTA) software distribution, configuration change detection, remote data-wipe, remote configuration, and asset/property management.

Mobile applications should also be centrally managed by DHS enterprise Mobile Application Management (MAM), which functions to evaluate and select mobile applications, and acts as an authorized enterprise application store for DHS users. It also provides DHS the ability to monitor installed applications and remotely upgrade or uninstall applications as necessary.

3.5 DATA PROTECTION

The AO ensures all information stored on mobile devices is encrypted using FIPS 140 validated encryption schemes consistent with the sensitivity (e.g., FIPS 199) of the stored information. Implementing countermeasures such as file and data encryption helps to ensure the confidentiality of information residing on the device.

[3] NIST SP 800-124 "Guidelines for Managing the Security of Mobile Devices in the Enterprise"

3.6 MONITORING OF SYSTEM FILES

Information Systems Security Officers (ISSO) should implement mechanisms that periodically scan for unauthorized changes to system files and other critical files on all mobile devices.

3.7 DEVICE SYNCHRONIZATION AND BACKUP

Mobile devices, when wirelessly synchronizing, must use products or modules with FIPS 140 validated encryption.

3.8 DEVICE DATA SANITIZATION

Data on a mobile device will be sanitized or zeroized when the device are retired. It is important to understand that a soft or hard reset will not permanently erase the data on a mobile device, nor will a file management utility will also not permanently remove files.

3.9 RECOMMENDED SAFEGUARDS FOR TRAVEL

Travelers need to be especially vigilant and wary to mitigate loss, theft, eavesdropping, and other increased vulnerabilities and heightened risks to mobile device security. All employees and contractors, regardless of security clearance level, are not authorized to take government-issued equipment, including cell phones, computers, or tablets such as iPads, outside of the United States for any personal or official foreign travel, unless such use is pre-authorized by their supervisor.[4] Section 3.9 of the Appendix A checklist focuses on guidance for DHS travelers. *DHS Policy Directive 4300A, Attachment Q International Travel with Mobile Devices* also provides specific DHS guidance on traveling internationally with DHS issued mobile devices. Additional guidance from the Federal Mobility Group on international traveling with Government Furnished Equipment (GFE) can be found on the CIO.gov website.[5]

4.0 SECURING THE WIRELESS LINK

The wireless interface (the link between a mobile device and a network endpoint or between two mobile devices) is a critical component of DHS network infrastructure, and is vulnerable to wireless attacks.

4.1 AUTHENTICATION

Access to mobile devices and to the data on the devices requires mutual network identification and two-factor authentication.

---

[4] Joint Office of the Chief Security Officer and Office of the Chief Information Officer Guidance on Foreign Travel (August 18, 2021): https://dhsconnect.dhs.gov/org/comp/mgmt/ocio/ciso/CISO%20ALL%20Documents/Joint%20OCSO%20OCIO%20Guidance%20on%20Foreign%20Travel.pdf#search=joint%20ocio%20ocso

[5] CIO.gov – "International Travel Guidance for Government Mobile Devices" - https://www.cio.gov/assets/files/FMG%20International%20Travel%20Guidance%20-Final.pdf

Identity Access Management is further detailed in the DHS IT Security Program Handbook for Sensitive Wireless Systems and DHS IT Security Architecture Guidance Application Infrastructure Design, Volume III.

4.2 END-TO-END SECURE COMMUNICATIONS

End-to-end security means that the entire message is encrypted from sending device to receiving device. Both devices must use appropriate FIPS 140 validated encryption. The use of certificates is also essential to implementation of strong end-to-end encryption. Users need to be conscious of security warnings indicating certificate error warnings. These precepts should be included in mobile security awareness training. See NIST SP 800-63 "*Digital Identity Guidelines*" and NIST SP 800-77 "*Guide to IPsec VPNs*" for additional requirements details.

4.3 PERSONAL FIREWALLS

Personal firewalls are software-based solutions that reside on client machine and are either client-managed or centrally managed. A firewall helps to secure the mobile device from unauthorized access by blocking specific types of inbound and outbound network traffic. Client-managed versions are not recommended because users can easily circumvent security settings. Managed IT solutions standardize Department-wide mobile device protection because IT departments can centrally configure and remotely manage client devices. Although personal firewalls offer some measure of protection, they do not protect against all advanced forms of attack.

4.4 VIRTUAL PRIVATE NETWORK (VPN)

Because they are not controlled by DHS, networks that are maintained by third parties may introduce security risks when used by DHS personnel. For example, cellular infrastructure facilities are often not owned by the cellular carrier, and are accessible to other carriers and to maintenance subcontractors; therefore, DHS personnel who use public wireless networks such as those in airports, conference centers, and other public places, should use the DHS VPN service to access DHS resources.

4.5 INTRUSION PROTECTION SYSTEMS

Intrusion systems are host- or network-based technologies used to protect information assets from exploitation. An Intrusion Prevention System (IPS) is proactive prevention technology that makes automated access control decisions based on application content. An Intrusion Detection System (IDS) is a more reactive technology that is used to detect attacks as or after they occur. Systems Security Plans shall adopt appropriate network protection mechanisms such as IDS. Refer to DHS Policy Directive 4300A, "*Information Technology System Security Program, Sensitive Systems*" and *NIST SP 800-94 "Guide to Intrusion Detection and Prevention Systems (IDPS)* for additional information.

4.6 SECURING THE NETWORK INTERFACE

When referring to the network interface or endpoint, two basic components are usually considered: network base stations (e.g., an access point for Wireless Local Area Network (WLAN) access) and client stations.

Typical mobile device wireless interfaces are illustrated in Figure 2, such as Bluetooth, WLAN, and cellular technology.

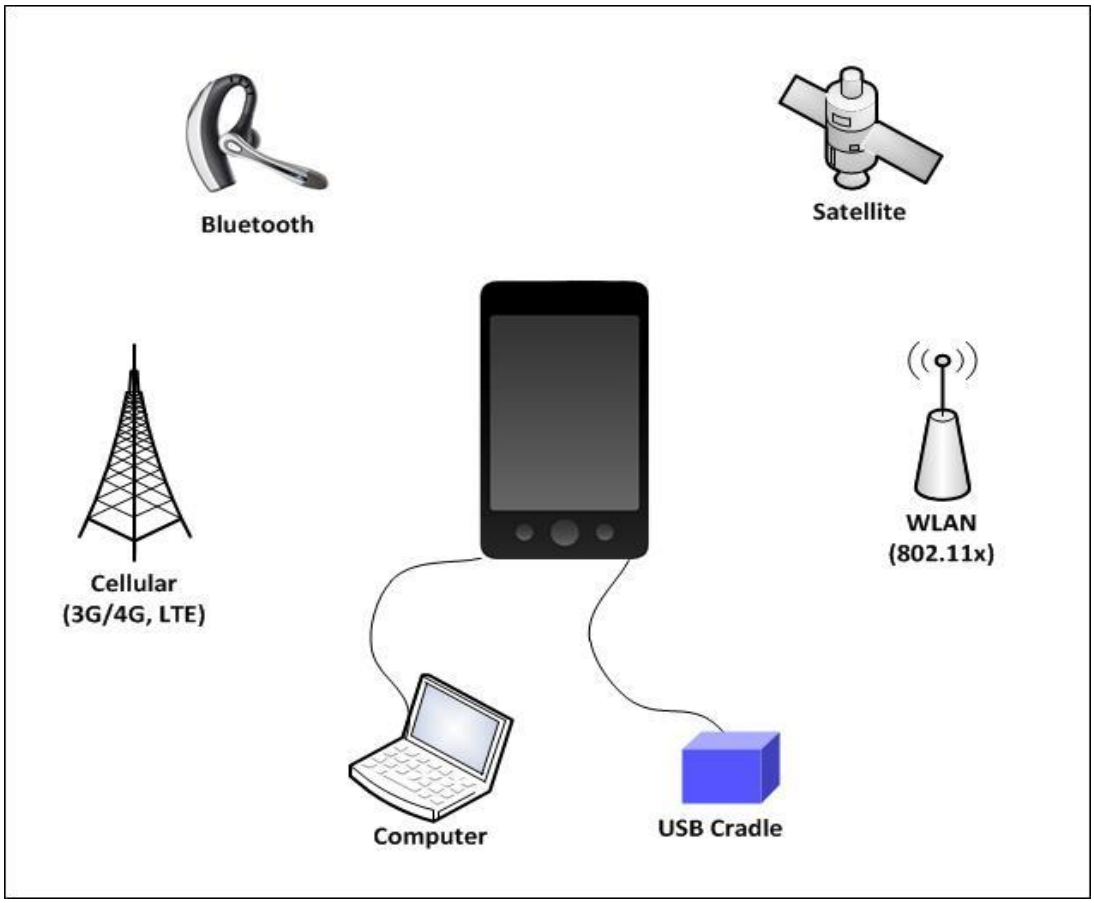

Figure 2: Typical Mobile Device Wireless Interfaces

4.6.1 BLUETOOTH

Bluetooth is a Wireless Personal Area Network (WPAN) technology that is commonly used for close-proximity wireless communications for devices such as headphones, keyboards, and other peripheral devices. Bluetooth technology, standardized by Institute of Electrical and Electronics Engineers (IEEE) 802.15.1, provides pre-shared key authentication and encryption capabilities to enable devices to authenticate each other and encrypt data traffic, but its security protocol is not FIPS-validated, and the technology has known inherent vulnerabilities. Several Bluetooth versions are currently available, including high speed 3.0 +HS and Low Energy (LE) 4.0, and they support different levels of security modes. For example, for Bluetooth 3.0, Security Mode 3 is the strongest mode because it requires establishment of authentication and encryption

before the Bluetooth physical link is completely established. For Bluetooth LE 4.0, Security Mode 1 Level 3 is considered the strongest mode because it requires authenticated pairing and encryption. NIST SP 800-121, "Guide to Bluetooth Security,"[6] provides detailed security recommendations as well as information on vulnerabilities.

4.6.2 WIRELESS LOCAL AREA NETWORKS (WLAN)

A WLAN can communicate with mobile devices equipped with IEEE 802.11 wireless network adaptors. Although a WLAN typically covers only a limited area, an adversary wanting to intercept data can greatly extend WLAN range by using special directional equipment.

4.6.3 CELLULAR TECHNOLOGY

A cellular Wireless Wide Area Network (WWAN) is a network composed of many small radio cells. Each cell covers a limited geographic area (with a radius of 3 to 5 kilometers), and is equipped with a fixed transmitter that connects the mobile device via its air interface to the cellular carrier's network. The security offered by commercial cellular providers does not meet DHS policy requirements; therefore, it is critical for AOs and system owners to ensure that mobile device system administrators and users are properly trained and that security controls are properly implemented.

5.0 EMERGING TECHNOLOGIES

This section examines emerging security technologies that may impact security guidance for mobile devices.

5.1 BIOMETRICS AND SMART CARDS

Biometrics has been introduced as an added layer of security, providing the ability to identify and authenticate users by means of their unique personal characteristics. Some laptops are now available with built-in fingerprint biometrics and smart cards, which can allow the user immediate access to sensitive information, eliminating the necessity of having the information stored on a host computer. Although less desirable, Universal Serial Bus (USB) fingerprint biometric readers are also commercially available, and can provide authentication to the device, protection of user profiles in the operating system, and encryption services for files and folders. Unlike passwords or public key infrastructure, which require exactly matching credentials for successful authentication, biometrics incorporates a sliding scale of assurance, based on a certain degree of matching, to balance false acceptance with false rejection rates.

[6] NIST SP 800-121 Rev 2, "Guide to Bluetooth Security" May 2017.
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-121r2-upd1.pdf

5.2 ENVIRONMENTALLY ADAPTABLE SECURITY POLICIES

Mobile devices should be configured to adapt to changing network environments by automatically switching between authorized network security policies and applying adaptive controls.

5.3 NEAR FIELD COMMUNICATION SECURITY POLICES

Near Field Communication (NFC) is a wireless technology designed to enable communications between two devices over very close distances (only a few centimeters). In NFC, range is limited by operating frequency, power consumption, and hardware and software design. NFC allows two devices to establish a communication channel that complies with ISO/IEC Standards 18092 and 21481. For instance, two NFC-capable smartphone users can share photos by placing their phones close together and clicking the photos.

NFC standards require few security features. Because the two devices must be in very close proximity, NFC is less vulnerable to threats such as eavesdropping, data modification, and MitM attacks. Nevertheless, a secure channel at a higher OSI layer, such as a Transport Layer Security (TLS) at the application layer, should be used for sensitive data exchange. In addition, unless required by operations or business considerations, the NFC feature on devices should be disabled by default and enabled manually by users to minimize potential data leakage. See NIST SP 800-52, "*Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations"* for additional details on encryption requirements.

APPENDIX A—CHECKLIST FOR SECURING MOBILE DEVICES

SECURITY REQUIREMENTS CHECKLIST FOR MOBILE DEVICES			
✓	**Section 1.4: Policy Requirements**	**Required**	**Recommended**
	Personally owned equipment and software is not used to process, access, or store sensitive information without the written prior approval of the AO.	X	
	ONLY government furnished equipment (GFE) that has been properly configured by DHS-managed services is used on DHS wireless systems.	X	
	Personally-owned contractor mobile devices are not used on DHS wireless systems. Personally owned mobile devices used to communicate directly with DHS systems are specifically approved by the AO.	X	
✓	**Section 1.4.1: Security Incident Response**	**Required**	**Recommended**
	Security incident response Standard Operating Procedures (SOP) specify methods for mobile device users and other personnel to report security incidents, including a lost or stolen mobile device, in accordance with *DHS 4300A, "Information Technology System Security Program, Sensitive Systems,"* Attachment F - Incident Response.	X	
	One of the methods used to report security incidents SHALL be telephone communications to a security operations center or to on-call security operations personnel.	X	
	Security incident response capability is available on a continuous basis (i.e., 24 hours a day, 365 days a year).	X	
✓	**Section 1.4.2: Security Awareness Training**	**Required**	**Recommended**
	Appropriate security awareness training is provided in accordance with DHS 4300A, "Information Technology System Security Program. Sensitive Systems."	X	
	Wireless security awareness training is included in annual training at the Component level.		X
	All employees who use or administer mobile devices have completed IT security awareness training prior to use of the system. (The security awareness training may be combined with similar training for other systems and may be provided during an employee's orientation program.)	X	
	IT security awareness training recurs annually, and evidence of completion is submitted to the Information System Security Manager (ISSM) of the program or to the appropriate responsible security authority.	X	

SECTION 3: SECURING THE PHYSICAL DEVICE			
✓	**Section 3.1: Authentication**	**Required**	**Recommended**
	Mobile devices implement password protection for device and data access.	X	

SECURITY REQUIREMENTS CHECKLIST FOR MOBILE DEVICES			
	Passwords follow access control guidance given in *DHS 4300A, "Information Technology System Security Program. Sensitive Systems."*	X	
	Passwords to access data on mobile devices are combined with the use of a smart card or a biometrics authentication method.		X
	Numerical passwords used for mobile device access contain a minimum of six digits, or the maximum allowed by the device is used if the device's maximum is less than six.	X	
	Mobile device authentication mechanisms are not configured for automatic access, and mobile devices require device re-authentication after a 10-minute timeout.	X	
✓	**Section 3.2: Mobile Threat Defense**	**Required**	**Recom-mended**
	Mobile Threat Defense software is centrally managed and continuously updated to protect mobile devices and organization data\employee data from mobile threats (e.g., malicious apps, network-based attacks)		X
	Companion devices that provide personal information management (PIM) synchronization have MTD installed so that malicious mobile code is not transferred between the mobile device and the companion device.		X
	If no suitable MTD solution exists for a particular mobile device, then the AO should take this into consideration when approving or disapproving the adoption of the mobile device.		X
✓	**Section 3.3: Disabling Undesirable Mobile Device Capabilities**	**Required**	**Recom-mended**
	Unapproved or unnecessary mobile device capabilities and applications are disabled or removed whenever possible.	X	
	Device-integrated capabilities such as cameras and recording mechanisms are subject to the approval of the AO, recognizing that these capabilities have varying degrees of risk and should be disabled unless specifically required, in order to mitigate the risk of exposing sensitive information.		X
	Short Message Service (SMS) and Multimedia Messaging Service (MMS) are not used to process, store, or transmit sensitive information, unless they are protected by appropriate FIPS 140-2 validated encryption mechanisms and approved by the appropriate AO.	X	
	Mobile devices issued by Components are distributed and restricted to an approved baseline configuration.	X	
	Personal mobile devices are not used to connect to DHS resources by data exchange functions such as email and file shares.	X	
✓	**Section 3.4: Mobile Device and Application Management**	**Required**	**Recom-mended**
	Changes to physical mobile device components adhere to DHS policies and security protocols.	X	
	An MDM system is used to centrally manage mobile devices.	X	
	Mobile device configuration is maintained and monitored by an MDM system.	X	

SECURITY REQUIREMENTS CHECKLIST FOR MOBILE DEVICES			
	Mobile device configuration management includes secure updates to security policies and user profiles where possible.	X	
	An MAM system is used to centrally manage approved mobile applications.	X	
✓	**Section 3.5: Data Protection**	**Required**	**Recom-mended**
	Applications such as file sharing are disabled on mobile devices, and all file sharing ports are blocked in both directions, especially when processing sensitive information.		X
	Where possible, data protection is extended to include PIM databases, telephone contact lists, text messages, and temporary browser files.		X
	Mobile devices encrypt all data-at-rest by securing either the individual files or the file system (operating system, storage partition and removable media).	X	
✓	**Section 3.6: Monitoring of System Files**	**Required**	**Recom-mended**
	Integrity verification mechanisms are deployed to perform system file integrity checks automatically, by means such as routinely comparing a cryptographic hash of the current system files on the mobile device to a "known good" previously recorded hash.		X
✓	**Section 3.7: Device Synchronization and Backup**	**Required**	**Recom-mended**
	Mobile devices are periodically synchronize and back up all stored information. Recommended intervals are daily for incremental data backups and weekly for full data backups.		X
	A replacement device supports full restoration functionality of the archived file(s) to limit the downtime and loss of productivity possible after an attack or loss has taken place.		X
	Wireless capabilities are disabled during hot-synchronization with companion devices.		X
	To prevent unauthorized connections between multiple networks, only a single wired or wireless network connection is active at any one time.		X
✓	**Section 3.8: Device Data Sanitization**	**Required**	**Recom-mended**
	Data on mobile devices is properly sanitized by degaussing, overwriting, or destroying the hardware.	X	
✓	**Section 3.9: Recommended Safeguards for Travel**	**Required**	**Recom-mended**
	Update the mobile Operating System (mOS) of the mobile device to the latest DHS authorized OS.	X	
	Obtain supervisor approval prior to traveling internationally with DHS issued mobile devices.	X	
	Adhere to DHS 4300A Attachment Q for international travel with mobile devices	X	

SECURITY REQUIREMENTS CHECKLIST FOR MOBILE DEVICES			
SECTION 4.0: SECURING THE WIRELESS LINK			
✓	**Section 4.0: Securing the Wireless Link**	**Required**	**Recommended**
	Because communication cannot be protected from interception, controls are implemented to prevent the unauthorized disclosure of information.	X	
	Because all receivers of the transmitted signal will not be authorized users, security mechanisms are put in place to protect wireless resources and data.	X	
	Users SHALL adhere to DHS policy and refrain from peer-to-peer associations unless approved by the appropriate AO.	X	
	AOs ensure that proper authentication and encryption mechanisms are implemented, so as to ensure data integrity, confidentiality, and availability.	X	
✓	**Section 4.1: Authentication**	**Required**	**Recommended**
	Authentication is required after power-up, reset, restart, or five minutes of user inactivity.	X	
	Components configure systems to lock a user's account for 20 minutes after ten consecutive failed logon attempts.	X	
	Implement access control guidance described in DHS 4300A, "Information Technology System Security Program, Sensitive Systems."	X	
	Passwords for access to data on mobile devices are combined with the use of a smart card or biometric authentication.		X
	Numerical passwords used for mobile device access contain a minimum of six digits, or the maximum allowed by the device is used if the device's maximum is less than six.	X	
	Administrators are aware that the access control mechanisms supported by many wireless systems identify client stations and not users, and that unauthorized users may gain access through lost or stolen devices or by a combination of the types of attacks described in Section 2.0.		X
	Authentication mechanisms are put into place to require smart cards, certificates, or security tokens to verify user identity.	X	
	Identity management systems authenticate wireless users and mobile devices, and take full advantage of any existing public key infrastructure when accessing DHS resources		X

SECURITY REQUIREMENTS CHECKLIST FOR MOBILE DEVICES			
✓	**Section 4.2: End-to-End Secure Communication**	**Required**	**Recom-mended**
	Users are trained not to ignore warning messages and to report suspicious activity. For more information regarding incident response, see DHS 4300A Attachment F – Incident Response.		X
	Encryption keys stored on client stations are protected from unauthorized disclosure.	X	
	The use of dynamic keys includes Extensible Authentication Protocol (EAP). (Using dynamic keys mitigates the risks associated with shared static keys and is highly recommended.)		X
	Symmetric encryption keys (AES-256-bit) are used to protect all transmitted information. Technologies such as IPSec VPN incorporate the use of public key cryptography and inherently use dynamic key exchange to set up the encrypted VPN tunnel.		X
	Key distribution occurs over a secure channel to minimize risk of compromise.		
✓	**Section 4.3: Personal Firewalls**	**Required**	**Recom-mended**
	Personal firewalls block access to high-risk ports.		X
	Personal firewalls enable audit logging.		X
✓	**Section 4.4: Virtual Private Network (VPN)**	**Required**	**Recom-mended**
	Mobile device communications between third-party networks and the DHS network are prohibited, being considered inherently untrustworthy given the lack of network control and the public nature of these networks.		X
	Implemented VPNs have NIST FIPS 140-2 validated encryption and appropriate key management mechanisms. [A list of FIPS 140-2 validated products may be found in the DHS Technical Reference Model (TRM)].		X
	Remote access of Personally Identifiable Information (PII) complies with all DHS requirements for sensitive systems, including strong authentication.	X	
	Strong authentication is accomplished via VPN or by an equivalent approved method.	X	
✓	**Section 4.5: Intrusion Systems**	**Required**	**Recom-mended**
	Components routinely scan wireline and wireless networks to determine whether unauthorized mobile devices are connected to DHS networks.		X

✓	**Section 4.6: Securing the Network Interface**	**Required**	**Recom-mended**
	Other components are included in the architecture to provide additional security services, such as authentication servers, firewalls, and VPN concentrators.		X

SECURITY REQUIREMENTS CHECKLIST FOR MOBILE DEVICES			
	As wireless convergence continues to increase, capabilities or functions are restricted to specific wireless interfaces whenever possible.		X
✓	**Section 4.6.1: Bluetooth**	**Required**	**Recommended**
	The strongest security mode is used for Bluetooth communications. Details can be found in the NIST SP 800-121 Rev. 1 for various Bluetooth versions.	X	
✓	**Section 4.6.2: Wireless Local Area Networks (WLAN)**	**Required**	**Recommended**
	Mobile devices use authentication and encryption mechanisms as required by applicable policies.[7]	X	
✓	**Section 4.6.3: Cellular Technology**	**Required**	**Recommended**
	Mobile devices implement strong identification and authentication controls to access DHS resources and SHALL encrypt all data-in-transit.	X	
	SECTION 5.0: EMERGING TECHNOLOGIES		
✓	**Section 5.1: Biometrics and Smartcards**	**Required**	**Recommended**
	Smart cards and biological recognition systems (e.g., retina scanner, handprint, voice recognition), are cost-justified through the risk assessment process.	X	
✓	**Section 5.2: Environmentally Adaptable Security Policies**	**Required**	**Recommended**
	Whenever a mobile device is outside the corporate network or communicating from an insecure location, capabilities such as VPNs and firewalls self-configure to the changing operational environment.		X

[7] https://dhsconnect.dhs.gov/org/comp/mgmt/ocio/ciso/CISO%20ALL%20Documents/Forms/knowledge%20View.aspx

APPENDIX B—REFERENCED PUBLICATIONS

DHS Publications

ISSM Guide to the DHS Information Security Program, Version 2.0, July 19, 2004, https://dhsconnect.dhs.gov/org/comp/mgmt/ocio/ciso/CISO%20ALL%20Documents/ISSM_Guide.pdf#search=ISSM%20Guide

ISSO Guide to the DHS Information Security Program, Version 10, September, 2013, https://dhsconnect.dhs.gov/org/comp/mgmt/ocio/ciso/_layouts/15/WopiFrame.aspx?sourcedoc={551871BA-3F7D-4DFF-A773-6AFE75E390B9}&file=ISSO%20Guide%20v10.doc&action=default&DefaultItemOpen=1

DHS Management Directive 140-01, "*Information Technology Security Program*," Revision 2, May 5, 2017.

DHS Policy Directive 4300A and Attachments – (DHS Connect – CISO)

DHS Policy Directive 4300A, "*Information Technology System Security Program. Sensitive Systems*," Version 1.0 (Draft Revision in Progress)

DHS 4300A, Attachment F "*Incident Response"* Version 1.0 (Draft Revision in Progress)

DHS 4300A, Attachment Q "*International Travel with Mobile Devices"* Version 1.0 (Draft Revision in Progress)

Defense Information Systems Agency (DISA) Publications

Wireless Security Technical Implementation Guide (STIG), and Addendums
Current versions at: Security Technical Implementation Guides (STIGs) – DoD Cyber Exchange (https://public.cyber.mil/stigs/)

National Institute of Standards and Technology (NIST) Publications

National Vulnerability Database - https://nvd.nist.gov/

NIST SP 800-53, Rev 5, "Security and Privacy Controls for Info Systems and Organizations". https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

NIST SP 800-121, Rev. 2, "Guide to Bluetooth Security" https://csrc.nist.gov/publications/detail/sp/800-121/rev-2/final

NIST SP 800-124, Rev 1, "Managing the Security of Mobile Devices in the Enterprise" https://csrc.nist.gov/publications/detail/sp/800-124/rev-1/final

NIST SP 800-63 "Digital Identity Guidelines". https://doi.org/10.6028/NIST.SP.800-63-3

NIST SP 800-77 "Guide to IPsec VPNs". https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-77r1.pdf

National Security Agency (NSA) Publications

National Security Agency / Central Security Service Web Site, http://www.nsa.gov

Committee on National Security Systems (CNSS) Instructions

CNSS Instruction No. 4009 (Revised), CNSS Instructions - https://www.cnss.gov/CNSS/issuances/Instructions.cfm (Requires a DoD Root Certificate to Access)

National Information Assurance Partnership (NIAP) Publications

Wireless Protection Profiles - NIAP: Protection Profiles (https://www.niap-ccevs.org)

Other Publications

FAQS.org, Network Working Group, "Request for Comments (RFC) 2828, Internet Security Glossary" http://www.faqs.org/rfcs/rfc2828.html

APPENDIX C—ACRONYMS AND DEFINITIONS

Acronym	Definition
AES	Advanced Encryption Standard
AO	Authorizing Official
ATO	Authority to Operate
CISO	Chief Information Security Officer
DHS	Department of Homeland Security
DDoS	Distributed Denial of Service
DoD	Department of Defense
EAP	Extensible Authentication Protocol
FIPS	Federal Information Processing Standard
GFE	Government Furnished Equipment
GPS	Global Positioning System
IDS	Intrusion Detection System
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IEEE	Institute of Electrical and Electronics Engineers
IPS	Intrusion Prevention System
IPsec	Internet Protocol Security
ISSO	Information System Security Officer
IMT	International Mobile Telecommunications
IT	Information Technology
ITU	International Telecommunications Union
J2ME	Java 2 Platform Micro Edition
LE	Low Energy
LTE	Low Term Evolution
MAC	Media Access Control
MAM	Mobile Application Management
MDM	Mobile Device Management
MMS	Multimedia Messaging Service
NFC	Near Field Communication
NIST	National Institute of Standards and Technology
NSA	National Security Agency

Acronym	Definition
OSI	Open Systems Interconnection
OTA	Over-the-Air
PCS	Personal Communications Services
PII	Personally Identifiable Information
PIM	Personal Information Management
SMS	Short Message Service
SOP	Standard Operating Procedure
SP	Special Publication
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TRM	Technical Reference Model
USB	Universal Serial Bus
VPN	Virtual Private Network
WLAN	Wireless Local Area Network
WWAN	Wireless Wide Area Network