DoD Wireless Mobile Device Security Requirements Matrix
Version 4.1
21 November 2011

Requirement Number	Requirement	Source of Requirement

This matrix was developed by Defense Information Systems Agency Field Security Operations (DISA FSO) and is an unofficial compilation of Department of Defense (DoD) security requirements for wireless mobile device systems. The purpose of the matrix is to provide a tool for DISA FSO when evaluating commercial mobile device systems. The requirements listed in this document are subject to change as new security vulnerabilities are identified or DoD security polices are updated.

For the purpose of this matrix, wireless mobile devices are defined as smartphones and tablets used to store and process up to sensitive/FOUO data/information and can be connected directly or indirectly to DoD information systems and networks. One of the primary uses for these devices is accessing DoD email via an indirect wireless connection to a DoD email system. Operating systems covered in this matrix are Blackberry OS, BlackBerry QNX, Android, iOS, and Windows 7. Requirements for laptop computers and wireless barcode or RFID scanners are not included in the matrix.

A DoD wireless smartphone email system usually consists of the following components:

- Mobile device operating system
- Productivity management application (provides connectivity to productivity services such as email, calendar, and contacts located on the management server)
- Smart Card Reader (SCR) and Drivers
- Other applications (e.g., Internet browser, productivity applications, etc.)
- Wireless email client and management server
- Common Access Card (CAC) middleware
- Mobile Device Management (MDM) server that manages security and other policies on the mobile device
- Device integrity validation tool

Note: Bluetooth SCR security requirements are listed in a separate document (**DoD Bluetooth Requirements Specification**, 16 July 2010, located on the web site: http://iase.disa.mil/stigs/content_pages/wireless_security.html.

Changes from previous version:

- Previous version was 3.5, dated 21 January 2011.

- Changed the focus of the matrix to cover mobile device (smartphones and tablets).

- Minor edits to most requirement statements.

- Added new requirements: 10.2.4, 11.13 to 11.18, and 17 to 19.

Requirement Number	Requirement	Source of Requirement
1. Email System Requirements		
1.1	Email redirection from the email server (e.g., Exchange Server) to the mobile device must be controlled via centrally managed server. Desktop or Internet controlled email redirection is not authorized.	Wireless STIG, USCYBERCOM Technical Bulletins 05-018 and 05-019
1.2	Mobile/wireless email management server must be capable of being configured to require PKI digital certificate authentication or shared secret authentication between the mobile device and the server.	DoDD 8500.1, CTO 07-15Rev1
1.3	Mobile/wireless email management server must be capable of being configured to disable connections from the mobile device to back office server unless Common Access Card (CAC) (i.e., DoD smart card) authentication is enforced at the server.	DoDD 8500.1, CTO 07-15Rev1
1.4	Mobile/wireless email server must be configured to disable connections from the mobile device to a network share drive unless PKI authentication is enforced at the share drive.	DoDD 8500.1, CTO 07-15Rev1
2. Data Protection (Requirements in either 2.1 or 2.2 must be met.)		
2.1	Data Wipe (hard reset) requirements	
2.1.1	The system must have the capability to perform a "Data Wipe" function whereby all data stored in user addressable memory on the mobile device and the removable memory card must be erased.	Wireless STIG, USCYBERCOM Technical Bulletins 05-018 and 05-019
2.1.2	The system "Data Wipe" function must sanitize all addressable memory locations on the mobile device according to the procedures in the NSA/CSS Policy Manual 9-12 (FOUO). Note: This is a highly desired capability, not a requirement. The goal is to sanitize the device after a data spill (Classified Message Incident (CMI)).	Wireless STIG
2.1.3	The system must automatically perform a Data Wipe after a set number of incorrect passwords have been entered by the user.	USCYBERCOM Technical Bulletins 05-018 and 05-019
2.1.3.1	The number of incorrect password attempts is configurable (minimum requirement is 3-10).	USCYBERCOM Technical Bulletins 05-018 and 05-019
2.2	Data Obfuscation	
2.2.1	When the Data Obfuscation procedure is implemented, the AES encryption key must be deleted, scrambled, or hidden such that it is no longer available to decrypt the device data.	USCYBERCOM Technical Bulletins 05-018 and 05-019
2.2.2	The system must automatically perform a Data Obfuscation after a set number of incorrect passwords have been entered by the user.	USCYBERCOM Technical Bulletins 05-018 and 05-019
2.2.2.1	The number of incorrect password attempts is configurable (minimum requirement is 3-10).	USCYBERCOM Technical Bulletins 05-018 and 05-019

Requirement Number	Requirement	Source of Requirement
2.3	Remote Data Protection	Wireless STIG, USCYBERCOM Technical Bulletins 05-018 and 05-019
2.3.1	The system administrator must have the capability to transmit a remote Data Protection (e.g., "Data Wipe" or "Data Obfuscation") command to the handheld device.	USCYBERCOM Technical Bulletins 05-018 and 05-019
2.3.2	The system must automatically perform a "Data Protection" procedure ("Data Wipe" or "Data Obfuscation") after a set period of time the device has not contacted the management server. (Optional requirement)	USCYBERCOM Technical Bulletins 05-018 and 05-019
2.4	Data-at-Rest (DAR) encryption	
2.4.1	All data stored on the mobile device must be encrypted using AES encryption. AES 128 bit encryption key length is the minimum requirement; AES 256 desired.	CTO 08-001
2.4.2	The data cryptographic module must be FIPS 140-2 validated.	OMB Circular A-130
2.4.3	A password must be successfully entered before the mobile device data is unencrypted.	CTO 08-001
2.4.4	When a screen lock occurs (user initiated or due to an inactivity timeout) all data must be re-encrypted.	DoDI 8500.2
2.5	Removable storage	
2.5.1	Data stored on removable media cards must be encrypted using the same standards used for embedded memory.	CTO 08-001
2.5.2	Removable storage media cards must be bound to the mobile device so that data stored on them can only be read by that mobile device.	Wireless STIG and CTO 08-001
3. Encryption of Transmitted Data/Email		
3.1	All data (including email attachments) sent over the wireless link from the mobile device to the wireless email server located on the DoD network must be encrypted using AES. AES 128 bit encryption key length is the minimum requirement; AES 256 desired.	DoDD 8100.2
3.2	Data encrypted by a FIPS 140-2 validated encryption algorithm.	OMB Circular A-130
3.3	The mobile device must support SSL v3 and TLS v1 (or later versions) encryption.	DoDD 8100.2
3.4	VPN Client	
3.4.1	VPN client must support DoD PKI certificate based authentication to the DoD VPN gateway.	Secure Remote Computing STIG
3.4.2	VPN client must disable split tunneling.	Secure Remote Computing STIG
3.4.3	The VPN must support either IPSec or SSL.	Secure Remote Computing STIG

Requirement Number	Requirement	Source of Requirement
3.4.4	The VPN must use a FIPS 140-2 validated encryption algorithm.	Secure Remote Computing STIG
4. S/MIME Requirements		
4.1	The system must be capable of providing S/MIME v3 (or later version) encryption of email.	DoDD 8500.1, DoDD 8100.2, CTO 07-15Rev1
4.2	S/MIME must be fully interoperable with DoD PKI and CAC/PIV. CAC/PIV (hard token) and PKCS#12 (soft token) certificate stores must be supported.	DoDI 8520.2
4.2.1	The S/MIME encryption algorithm must be 3DES or AES. When AES is used, AES 128 bit encryption key length is the minimum requirement; AES 256 desired.	DRAFT DoD PKI Public Key Enabled Application Requirements
4.2.2	The S/MIME cryptographic module must be FIPS 140-2 validated.	OMB Circular A-130
4.2.3	Path Processing: System must verify all digital certificates in the path (user certs, intermediate certs, and root certs).	DRAFT DoD PKI Public Key Enabled Application Requirements
4.2.3.1	It is required that DoD root and intermediate certs be stored on the handheld device.	DRAFT DoD PKI Public Key Enabled Application Requirements
4.2.4	A user should have the ability to save public certs of contacts in the contact object by one or both of the following methods. 1. By saving public certs to the contacts object that were attached to a received email message 2. By saving public certs to the contacts object downloaded via an external partner PKIs lookup from the handheld device This is an optional requirement.	DRAFT DoD PKI Public Key Enabled Application Requirements
4.2.5	A user should be able to check the status of the cert on a received or outgoing message without having to be connected to the email management server (desired, but optional requirement).	DRAFT DoD PKI Public Key Enabled Application Requirements
4.2.5.1	It is recommended (but not required) that the certificate status be cached on the handheld device for a period not extending beyond the expiration period of the revocation data.	DRAFT DoD PKI Public Key Enabled Application Requirements
4.2.6	If Smart Card or Certificate Store Password caching is available, the timeout period should be able to be set from at least 15 to 120 minutes.	DRAFT DoD PKI Public Key Enabled Application Requirements
4.2.7	Digital signing/encrypting/decrypting messages	

Requirement Number	Requirement	Source of Requirement
4.2.7.1	The user must have the capability to digitally sign and/or encrypt outgoing email messages using software or hardware based digital certificates.	CTO 07-15Rev1
4.2.7.2	The user must have the capability to decrypt incoming email messages using software or hardware based digital certificates.	CTO 07-15Rev1
4.2.7.3	The system must provide a mechanism to provide certificate validation through a trusted OCSP, CRL, or SCVP.	CTO 07-15Rev1
4.2.7.4	The system must provide a noticeable warning to the user if the CRL, SCVP, or OCSP server cannot be contacted or the revocation data provided cannot be verified (highly desired, but optional).	DRAFT DoD PKI Public Key Enabled Application Requirements
4.2.7.5	The system must support retrieving encryption certificates not stored in the local trust anchor store for S/MIME purposes.	DRAFT DoD PKI Public Key Enabled Application Requirements
4.2.7.6	The system must support SHA1 signing operations until December 31st, 2010, and the system must support SHA2 signing operations after December 31st, 2010.	NIST SP 800-78-2 and Draft NIST SP 800-131
4.2.7.7	The system must support SHA1 signature verification after December 31st, 2010, and the system must support SHA2 signature verification after December 31st, 2010.	NIST SP 800-78-2 and Draft NIST SP 800-131
5.0 PKI Requirements		
5.1	Mobile device Certificate Store Requirements	
5.1.1	The mobile device certificate store must be FIPS validated.	OMB Circular A-130 DRAFT DoD PKI Public Key Enabled Application Requirements
5.1.2	The certificate store must encrypt contents using AES. AES 128 bit encryption key length is the minimum requirement; AES 256 desired.	DRAFT DoD PKI Public Key Enabled Application Requirements
5.1.3	The certificate store encryption algorithm must be FIPS 140-2 validated.	OMB Circular A-130 DRAFT DoD PKI Public Key Enabled Application Requirements
5.1.4	The certificate store must require a password to access contents of the store.	DRAFT DoD PKI Public Key Enabled Application Requirements

Requirement Number	Requirement	Source of Requirement
5.2	The system must validate the following PKI certificate characteristics. Note: The desire is to have the certificate policy on the mobile device (e.g., accept/not accept certificates with specific characteristics) mirror the practice used on DoD workstations.	
5.2.1	- Revoked certificate use	DRAFT DoD PKI Public Key Enabled Application Requirements
5.2.2	- Unverified certificate use	DRAFT DoD PKI Public Key Enabled Application Requirements
5.2.3	- Untrusted certificate use	DRAFT DoD PKI Public Key Enabled Application Requirements
5.2.4	- Non-FIPS approved algorithm used in certificate	DRAFT DoD PKI Public Key Enabled Application Requirements
5.2.5	- Invalid certificate use	DRAFT DoD PKI Public Key Enabled Application Requirements
5.2.6	- Unverified CRL use	DRAFT DoD PKI Public Key Enabled Application Requirements
5.3	Digital credential migration	
5.3.1	The handheld device must support credential migration in a secure manner by credential owner if device is to be re-provisioned (e.g., system/application software reloaded).	DRAFT DoD PKI Public Key Enabled Application Requirements
5.3.2	The handheld device must support credential migration in a secure manner by credential owner when user gets a new CAC or is new software certificates.	DRAFT DoD PKI Public Key Enabled Application Requirements
5.4	Support provided for both software certificates and hardware certificates (CAC/PIV).	DoDI 8520.2
5.5	Only DoD PKI issued or approved device authentication certificates must be installed on DoD mobile devices.	DoDI 8520.2
6. Mobile Device Provisioning		
6.1	The system administrator must have the capability to disable OTA provisioning.	DoD D 8100.2
6.2	A trusted loading process must be the foundation for device provisioning (whether tethered or over-the-air).	DoD D 8100.2

Requirement Number	Requirement	Source of Requirement
6.2.1	The trusted OTA provisioning process must provide mutual authentication between the provisioning server and the provisioned device.	DoD D 8100.2
6.2.2	The trusted OTA provisioning process must provide data integrity and confidentiality of the provisioning data downloaded from the server to the handheld device.	DoD D 8100.2
7. Internet Connections		
7.1	The system administrator must have the capability to configure the mobile device browser to connect only to a specific URL (e.g., DoD network, VPN gateway, or DoD web proxy) during provisioning of the handheld device. The user must not be able to override this setting.	DoDD 8500.1
7.2	The mobile device and browser must support certificate based authentication for access to web sites.	DoDD 8500.1
8. Mobile Device Unlock Password Requirements		
8.1	The mobile device must support the capability to enable a device unlock password.	DoDI 8500.2
8.2	Maximum password age (e.g., 30 days, 90 days, 180 days)	DoDI 8500.2
8.3	Minimum password length of eight or more	DoDI 8500.2
8.4	Maximum password attempts	
8.4.1	Device must perform a Data Wipe function after a set number of incorrect passwords are entered.	DoDI 8500.2
8.4.2	The system must allow the system administrator to specify exact number of incorrect passwords before the device must perform a Data Wipe (a range of at least 3-10 is the minimum requirement).	DoDI 8500.2
8.5	Maximum password history. The system must allow the system administrator to specify exact number of previous passwords that cannot be used (1-5 is the minimum requirement).	DoDI 8500.2
8.6	Several different password compositions (i.e., pattern checks) should be available, to include upper and lower case letters, numbers, and special characters, to allow administrators to tailor the password policies to fit unique organizational requirements.	DoDI 8500.2
8.7	The handheld device has an inactivity timeout whereby the user must reenter their user password or Smart Card PIN to unlock the device. The inactivity timeout must be configurable. The following settings must be available, at a minimum: Disable (no timeout), 15 minutes, and 60 minutes.	DoDD 8500.1
8.8	User (or hacker) cannot bypass device unlock password requirement.	DoDI 8500.2
9. Application Controls		
9.1	The system must control the capability of the user to install or remove applications on the mobile device.	
9.1.1	Only approved applications can be installed by the user.	DoDI 8500.2
9.1.2	Required applications cannot be removed by the user.	DoDI 8500.2

Requirement Number	Requirement	Source of Requirement
9.2	OTA application download must be from a DoD controlled source (e.g., DoD operated mobile device application store or MDM server).	DoDI 8500.2
9.3	Only digital signed applications must run on the mobile device.	DoDI 8500.2
10. Bluetooth Requirements		
10.1	The system administrator must have the capability to disable or remove the mobile device Bluetooth stack.	DoDD 8100.02
10.2	The following controls must be available for the Bluetooth stack.	
10.2.1	The system administrator must have the capability to enable or disable any available Bluetooth profile.	DoDD 8100.02
10.2.2	The system administrator must have the capability to disable the following if not already permanently disabled. Note: The Bluetooth features listed below must be enabled by the system/system administrator only when an approved Bluetooth device (smart card reader, secure headset) is used.	
10.2.2.1	- Bluetooth radio and/or Bluetooth connectable mode	DoDD 8100.02
10.2.2.2	- Discoverable mode	DoDD 8100.02
10.2.3	The system must have the following Bluetooth capabilities.	DoDD 8100.02
10.2.3.1	Bluetooth pairing using a randomly generated passkey size of at least 8 digits.	DoDD 8100.02
10.2.3.2	Bluetooth mutual authentication immediately after the initial establishment of any Bluetooth connection between the handheld and the smart card reader or handsfree headset.	DoDD 8100.02
10.2.3.3	128 bit Bluetooth encryption	DoDD 8100.02
10.2.3.4	FIPS 140-2 validated cryptography of data-in-transit over the Bluetooth link. Note: FIPS 140-2 encryption not required for voice. See the DoD Bluetooth Requirements Specification for specific requirements.	DoDD 8100.02 OMB Circular A-130
10.2.3.5	Bluetooth devices must use only Class 2 or 3 standard radios. Class 1 radios are not permitted. Radio modifications (e.g., signal amplification, antenna modification) are not permitted.	NSA IAD Report I732-016R-07
10.2.4	The system administrator must have the capability to set up a white list of Bluetooth devices that are authorized to pair to the mobile device. (White list filters based on device Friendly Name.)	DoD Bluetooth Requirements Specification
11. Security Policy Enforcement The system must centrally enforce security policies on the handheld device via a Mobile Device Manager (MDM). The following policies must be available:		
11.1	All mobile device unlock password requirements	DoDD 8500.1
11.2	All Data-at-Rest protection requirements	CTO 08-001

Requirement Number	Requirement	Source of Requirement
11.3	All Bluetooth security requirements	DoDD 8100.02 DoD Bluetooth Requirements Specification
11.4	Disable MMS messaging	DoDD 8100.02
11.5	Disable/Enable the following services. (Note: There is no requirement that the services remain disabled after a hard reset (device wipe) of the mobile device, but after a wipe, the device must not be able to connect to a DoD network until the security policy is reapplied.)	
11.5.1	- IR port	DoDD 8100.02
11.5.2	- Wi-Fi radio	DoDD 8100.02
11.5.3	- Bluetooth radio	DoDD 8100.02
11.5.4	- Voice recorder	DoDI 8500.2
11.5.5	- Microphone	DoDI 8500.2
11.5.6	- Camera	DoDI 8500.2
11.5.7	- Memory card port	DoDI 8500.2
11.6	Enable/Disable user's ability to switch devices	DoDI 8500.2
11.7	Access to an application store or repository	DoDI 8500.2
11.8	Installation of third-party applications	DoDI 8500.2
11.9	Block access to specific web sites	DoDI 8500.2
11.10	User modification of the security configuration file, policy, or profile. One of the following features must be available.	DoDI 8500.2
11.10.1	User cannot disable or bypass the mobile device security policy.	DoDI 8500.2
11.10.2	System detects if the security policy has been disabled or bypassed and disables the capability for the mobile device to connect to the DoD network.	DoDI 8500.2
11.11	Set security policy refresh interval.	DoDI 8500.2
11.12	Location services (OPSEC control)	DoDI 8500.2
11.13	Video recorder	DoDI 8500.2
11.14	USB Port mass storage mode	DoDI 8500.2

Requirement Number	Requirement	Source of Requirement
11.15	Wi-Fi tethering	DoDI 8500.2
11.16	Cellular tethering	DoDI 8500.2
11.17	Contact List	DoDI 8500.2
11.17.1	Enable or disable the capability for contact list data elements to be available to the phone application when the device is locked.	DoDI 8500.2
11.17.2	When access to the contacts list by the phone application is enabled, the administrator can select which data fields can be accessed (e.g., only name and phone numbers).	DoDI 8500.2
11.18	The MDM must not conflict with the device integrity validation tool. See requirement 17.	DSAWG Guidance
12. Wi-Fi Requirements		
12.1	WPA2 supported (enterprise and personal)	DoDI 8420.01
12.1.1	EAP-TLS supported	DoDI 8420.01
12.1.2	AES-CCMP supported	DoDI 8420.01
12.2	FIPS 140-2 validated cryptographic module used	OMB Circular A-130 DoDI 8420.01
12.3	When Wi-Fi radio is on, cellular radio data is disabled.	Wireless STIG
12.4	Mobile device Wi-Fi can be configured to disable automatic connections to saved Wi-Fi networks.	Wireless STIG
13. Malware Controls		
13.1	One of the following antivirus methods below must be used.	
13.1.1	Installation of a DoD approved antivirus application	DoDD 8100.02
13.1.2	Mobile device prevents a malware application from installing and executing.	DoDD 8100.02
13.2	DoD approved personal firewall application must be installed. The firewall must be able to filter both inbound and outbound traffic based on ports, protocols, and IP address.	DoDD 8100.02
14. Active Content in Email		
14.1	All active content in email (HTML, RTF, etc.) will either be blocked or converted to text.	DoDD 8100.02
15. Remote Access to DoD Network		
15.1	If the mobile device is used to remotely access a DoD network via a connection other than provided by the mobile device management system (e.g., via a VPN), the requirements listed in the Wireless STIG for PDA remote access apply.	Wireless STIG

Requirement Number	Requirement	Source of Requirement
16. Miscellaneous Requirements		
16.1	The mobile device will display the DoD warning banner before or immediately after device unlock: "I've read & consent to terms in IS user agreem't." (Wording must be exactly as specified.)	DoD CIO 9 May 2008 memo: Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement
17. Device Integrity Validation Tool		
17.1	The mobile device system will include either the DoD developed AutoBerry tool, the commercial version of the tool (Fixmo Sentinel), or other commercially available tool with similar capabilities.	DSAWG Guidance
18. Jailbreak/Rooting Detection		
18.1	The mobile device system must have the capability to detect jailbreaking or rooting of the device.	DSAWG Guidance
18.2	The mobile device system must have the capability to alert the MDM and disable the device when it has detected that the device has been jailbroken or rooted in an unauthorized manner.	DSAWG Guidance
19. Dual Environment Devices If a mobile device has the capability to physically or logically separate the device operating environment into a business use environment and personal use environment, the following requirements must be met:		
19.1	The appropriate smartphone/tablet STIG is applicable to the business use environment of the device.	DoDI 8500.2
19.2	The General Mobile device (Non-Enterprise Activated) STIG is applicable to the personal use environment of the device.	DoDI 8500.2
19.3	Personal environment data and applications and work environment data and applications must be separated on the device.	DoDI 8500.2
19.4	When the business use environment is open, the user and applications cannot access data or applications in the personal use area.	DoDI 8500.2
19.5	When the personal use environment is open, the user and applications cannot access data or applications in the business use area.	DoDI 8500.2