



Australian Government

**Department of Defence
Intelligence & Security**

BlackBerry Hardening Guide

Defence Signals Directorate

Release Date: December 2007

Table of Contents

Table of Contents.....	2
Overview.....	3
Technical Guidance.....	4
Overview.....	4
Network Architecture.....	5
BES Installation.....	7
BES Configuration.....	10
Bluetooth Peripherals.....	11
S/MIME & PGP.....	13
APB Messages.....	14
Application Policy Settings.....	15
BES IT Policy Settings.....	16
Overview.....	16
Settings.....	17

Overview

Introduction This document provides technical guidance on how to harden the BlackBerry Enterprise Server (BES) produced by Research in Motion (RIM).

Versions This document relates to BES versions 3.6 to 4.1.4.

Settings and features listed in this document that are non-existent in the version of the BES being used may be disregarded.

Policy relating to the use of Portable Electronic Devices (PEDs) by Australian government agencies can be found in the Australian Government Information and Communications Technology Security Manual (ACSI33).

Contents This publication contains the following sections:

Section	See Page
Technical Guidance	4
BES IT Policy Settings	16

Technical Guidance

Overview

Introduction The information in this section is provided to give technical guidance to agencies installing a BlackBerry solution with an agency ICT environment.

Other software platforms This guidance is derived from the results of the DSD review in which the BlackBerry Enterprise Server (BES) was installed upon a Microsoft Windows 2000 Server and configured to function with Microsoft Exchange Server version 5.5.

Certain aspects of the following guidance are therefore limited to the software versions investigated. Where this occurs, agencies implementing BlackBerry solutions on other platforms are encouraged to apply comparable strategies to address the identified issues.

Currency Some of the information in this section, particularly with respect to current patches and URL locations, may become outdated. Although all such information is accurate at the time of publishing, agencies are advised to confirm that they have the latest information available when installing their BlackBerry systems.

Contents This chapter contains the following topics:

Topic	See Page
Network Architecture	5
BES Installation	7
BES Configuration	10
Bluetooth Peripherals	10
S/MIME	13

Network Architecture

General principles

Distributing services will help to mitigate the effects of any future exploits and to improve availability, as will hardening the system by keeping permitted services and open ports to the minimum required.

BlackBerry router

Placing the BlackBerry router behind the external agency firewall will afford it the same protection as the rest of the agency LAN.

Action: Install the BlackBerry router in a neutral subnetwork between the trusted agency LAN and the Internet.

Configuring the external firewall

The only traffic that should be passing through the firewall located between the Internet and the BlackBerry router is an agency-initiated connection to RIM's Network Operations Centre.

Action: Configure the external firewall to permit only a single, outbound-initiated but bi-directional connection on port 3101 between the router and RIM.

Attachment Service

The separation of the Attachment Service, which is known to have vulnerabilities, allows agencies to reduce the consequences of a successful attack against the Service by immediately isolating it from the network.

Action: Install the BlackBerry Attachment Service on a separate server to the BES.

Additional firewall

The installation of an additional firewall between the BES and the internal agency mail servers allows the BES to be isolated from the rest of the network if it is compromised.

Action: Install an internal firewall between the BES and agency mail servers.

Separation of devices

Installing services on different servers reduces the risk that vulnerabilities in one service could affect other services.

Action: Install the Attachment Service and the configuration database on separate servers.

Continued on next page

Network Architecture, Continued

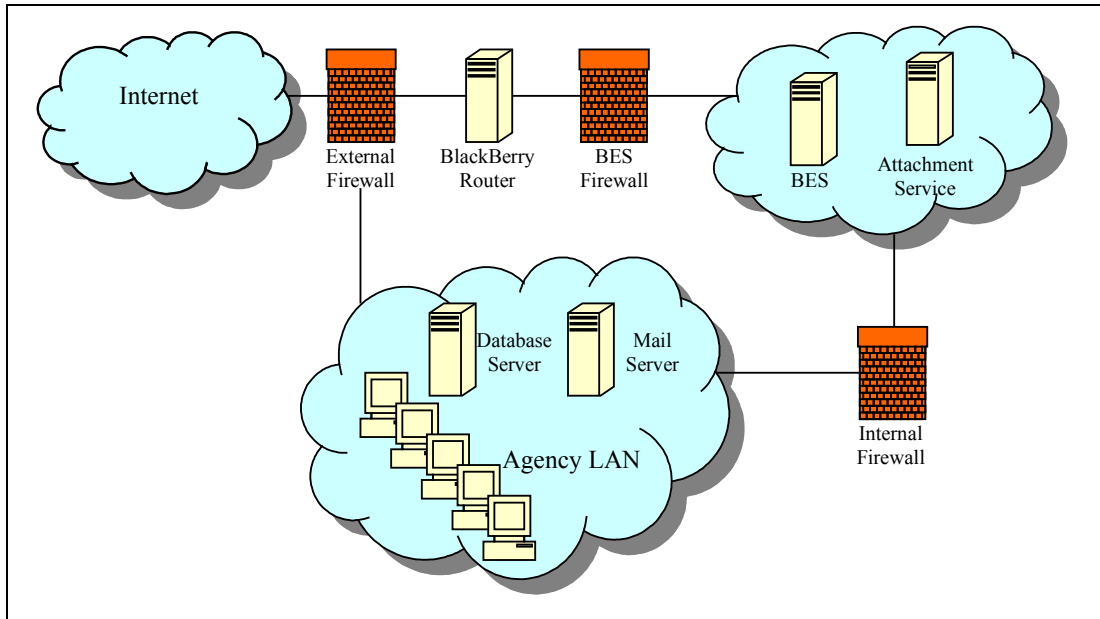
BES management

Managing the BES via a physical console removes the need for SNMP traffic to be permitted to the BES.

Action: Manage the BES via a physical console.

Network diagram

The diagram below shows a typical configuration for a BlackBerry installation designed to mitigate known risks.



BES Installation

Patching the host operating system

Although the RIM installation guides do not provide advice on the level of vendor security patching that should be applied to either the BES's underlying operating system or the Microsoft Exchange server, best practice dictates that production servers should be installed with the most current vendor cumulative patches and security hot fixes.

Information relating to patching levels is available from Microsoft's Technet.

Action: Apply relevant patches:

- Microsoft Windows 2000 Server – SP4,
 - Microsoft Windows 2003 Server – SP1, and
 - Any hot fixes released since these service packs.
-

Default Windows share

The default configuration for the BES, using a Microsoft Windows operating system, provides a Windows share of C:\ which is not required for BES functionality.

Action: Remove the C:\ share.

BES file share

Installing the BES automatically creates a common network directory share for holding BlackBerry handheld software configuration files. These files are used to configure handhelds with the agency's IT policy; unauthorised modification to the files could reduce the security of handhelds.

Action: Set the handheld configuration files to Read Only access.

Additional hardening

A complete hardening guide and assessment is beyond the scope of this review as there are a number of server configurations that could be utilised. However, to ensure that the BES is protected against known vulnerabilities, agencies should ensure at minimum the vendor best security practice guidelines are followed. These guides will assist administrators in identifying the required patching levels and help to determine the necessary functions, services and file shares.

Action: Harden the Microsoft Windows 2000 Server supporting the BES platform in accordance with the vendor security guides, prior to installing any BlackBerry system.

Guides such as Microsoft's Baseline Security Analyser (MSBSA) and Windows 2000 Server Baseline Security Checklist are available from:

URL: www.microsoft.com/technet/security/tools/mbsahome.mspx

URL: www.microsoft.com/technet/archive/security/chklist/w2ksvrcl.mspx

Continued on next page

BES Installation, Continued

Database Server

The BES relies on configuration information being held in a relational database. The databases supported by the BES include Microsoft SQL Server 2000 Desktop Engine (MSDE), Microsoft SQL Server 2000 SP3a, Microsoft SQL Server 2005 or DB2 for IBM Domino environments.

The full version of SQL Server is needed if administrators require management snap-ins for the local SQL database, as the functionality is not available with MSDE. Administrators will find SQL Server is useful if debugging is required during the installation process.

The configuration database may also be hosted on a separate SQL Server. This server may reside within the corporate network with the appropriate firewall opened to allow traffic on port 1433 between the BES and the database server. This reduces the risks associated with hosting this information in the DMZ.

Action: The SQL Server component of the BES should also be maintained to appropriate service pack levels and patched regardless of whether it is MSDE or the full SQL Server product. More information is available from:

URL:<http://www.microsoft.com/sqlserver>

Host-based firewall

Installing a host-based firewall on the BES will reduce likelihood of a successful attack against the BES.

Action: Install a host-based firewall on the BES, configured to limit traffic to the minimum necessary to allow the BES to perform its authorised tasks.

Browser

The BES requires Internet Explorer (IE) to be installed to allow viewing and navigation of locally stored RIM help files. However, the BES has no functional requirement for this IE installation to be aware of any external gateway allowing it to establish connections to the Internet, and to do so would greatly increase the risk to the system.

Note: The BES configuration manager, not the IE installation, is the service that allows the BES to conduct Internet requests made from BlackBerry handhelds.

Action: Ensure that all relevant IE Service Packs and hot fixes have been applied to IE.

Action: Ensure that the server is not able to make connections to the Internet via the agency's default gateway.

Action: Configure any personal firewalls on the BES server with rules that allow the BES applications to communicate whilst explicitly denying IE.

Continued on next page

BES Installation, Continued

Exchange environment

The BES can be used with MS Exchange 5.5, MS Exchange 2000 and MS Exchange 2003 servers in the Microsoft Windows environment.

Action: Apply Microsoft cumulative Service Packs and hot fixes for the version of Microsoft Exchange used prior to connection to the BES. At the time of publication the current service packs for Microsoft Exchange were:

- a. MS Exchange 5.5 - Service Pack SP4, and security fixes MS05-029, MS05-012, MS04-026, MS03-047, MS03-046, MS01-047 and MS01-041,
- b. MS Exchange Server 2000 - SP3 and post SP3 update rollup and hot fixes, and
- c. MS Exchange Server 2003 - SP2.

Note: Microsoft has announced that Microsoft Exchange 5.5 will no longer be supported after 31 December 2005, so an upgrade strategy for moving to a supported application will be required.

Additional information

RIM provides a comprehensive guide on preparing and installing the system to operate in a functioning environment.

Action: Review the guide designed for the version of software that you intend to install, available from:

URL: <http://www.blackberry.com/knowledgecenterpublic>

RIM also provides a current series of hot fixes to address application efficiency and to mitigate against BES security issues. Australian service providers may provide local websites with this information and/or provide an update alert feature. A generic entry to this information is also available at:

URL: [https://www.blackberry.com/Downloads\\$entry.do?](https://www.blackberry.com/Downloads$entry.do?)

Action: Periodically check for and apply Service Packs and hot fixes to the BES Server as they become available.

BES Configuration

Default settings When initially installed, the BES provides a default IT policy. To avoid inadvertently activating insufficiently secure handhelds, these settings need to be reconfigured.

Action: Reconfigure the BlackBerry default IT policy settings to reflect agency policies prior to providing handhelds to users for activation.

Determining permitted functionality In order to minimise the potential attack surface against BlackBerry components non essential functionality should be disabled unless there is a legitimate business requirement for its use.

Action: Disable all functionality that is not required for operational purposes.

Peer-to-peer messaging Peer-to-peer (also known as PIN-to-PIN) messaging allows users to send unencrypted messages directly to other handhelds.

Action: Prevent users from using peer-to-peer communications to transmit classified information.

Using the MDS The “Mobile Data Service” (MDS) allows the BES software to act as a proxy between the agency’s Internet connection and the BlackBerry handhelds.

Action: Configure the MDS to use the agency proxy server.

Patching Keeping patches for BlackBerry components and supporting servers up to date reduces the risk that attackers could exploit known vulnerabilities in the system.

Action: Apply patches for BlackBerry components and supporting servers inline with policy on the patching and hardening of servers in *ACSI 33*.

Reviews Technical reviews can assist in revealing any previously undetected compromises or other failures of security.

Action: Conduct a technical review at least annually.

Bluetooth Peripherals

Available peripherals

BlackBerry handhelds may incorporate Bluetooth functionality allowing pairing with headsets and hands-free car sets.

These peripherals are designed to allow hands-free voice communications only.

If agencies require a less risky hands-free option, the use of an earpiece and jack is recommended.

Recommended process

The risks of using Bluetooth within the context of BlackBerry handheld voice communications can be partially mitigated by using the process detailed below.

Step	Action
1	Ensure that, as a minimum, BES Version 4 Service Pack 3 is installed. This will provide the Bluetooth IT Policy group with the option to disallow Bluetooth Discovery mode on the handheld.
2	Create a separate Bluetooth IT Policy Group on the BES for users that will be using Bluetooth. This policy should reflect all other agency IT policy settings with the exception of: <ul style="list-style-type: none"> • Bluetooth Policy Group: Disable Bluetooth = FALSE, • Bluetooth Policy Group: Disable Headset profile = FALSE, • Bluetooth Policy Group: Disable Pairing = TRUE, and • Bluetooth Policy Group: Disable Discovery Mode = TRUE.
3	Create a separate IT Policy for users that will not be using the Bluetooth peripherals: <ul style="list-style-type: none"> • Bluetooth Policy Group: Disable Bluetooth = TRUE.
4	Create a Bluetooth configuration IT Policy that represents the agency IT policy with the exception that: <ul style="list-style-type: none"> • Bluetooth Policy Group: Disable Bluetooth = FALSE, • Bluetooth Policy Group: Disable Headset profile = FALSE, • Bluetooth Policy Group: Disable Pairing = FALSE, and • Bluetooth Policy Group: Disable Discovery Mode = FALSE.
5	Within the confines of a controlled environment, set the handheld Bluetooth setting to Discoverable mode under the Bluetooth options menu. This will allow the device to be paired with a BlackBerry headset.

Continued on next page

Bluetooth Peripherals, Continued

Recommended process (continued)

Step	Action
6	Follow the RIM guide for pairing to the BlackBerry headset and ensure that: <ul style="list-style-type: none">• encryption with the paired device is used,• the device is set to non-discoverable mode, and• the handheld's Bluetooth device name is set.
7	Apply the Bluetooth IT Policy Group to the Handheld which disallows pairing to other devices.
8	Create a set of standard operating procedures for Bluetooth enabled users that is designed to educate them on the exploitability of Bluetooth and the manner in which they are to operate this function. Content may include: <ul style="list-style-type: none">• attempts to pair additional devices to the handheld are forbidden,• if prompted to pair with another Bluetooth device the user is to deny all requests and report such information to system administrators, and• the functionality is to be used only when a hands-free environment is required, and the functionality should be turned off whenever this is not the case.

S/MIME & PGP

Using S/MIME or PGP

The introduction of Secure Multipurpose Internet Mail Extension (S/MIME) or PGP, using the OpenPGP message Format, would ensure that end-to-end encryption using a DSD Approved Cryptographic Protocol (DACP) is applied to emails between all users, including the BlackBerry handheld. The use of S/MIME or PGP on an enterprise email system would therefore mitigate some of the risks introduced by a BlackBerry system.

BlackBerry networks are able to handle S/MIME or PGP and its introduction would decrease the attractiveness of all sources of email content information, including the BES.

Considerations

If S/MIME or PGP is used, the network owner has to allow the traversal of encrypted information through their firewall to the mail server. Methods of dealing with the agency's email filtering and anti-virus protection requirements at the workstation, rather than just the gateway environment, would then need to be implemented.

Action: Consider the introduction of S/MIME or PGP to the enterprise wide mail network.

APB Messages

**All Points
Bulletin
message
functionality**

The BlackBerry Enterprise Server management console allows the ability for an administrator to send general alerts to all handsets, a group or an individual. This can be useful to notify users of outages or other general information.

Action: Consider sending only UNCLASSIFIED information with little or no identifying information of the organisation or operations when using this feature.

Application Policy Settings

Third Party application control

Agencies have the ability to control what applications are installed on BlackBerry handsets through the use of IT Policy Settings, which will control use of all third party applications, and Application Control Policies which will allow more granular control of permissions for each application or group of applications.

Action: If no third party applications are required a default policy with all options to Not Permitted should be used. Furthermore, control policies should be created for required applications to enforce the minimum features required.

BES IT Policy Settings

Overview

Introduction

The BlackBerry solution provides users with a broad range of options, approximately 300 IT policy settings, aimed at delivering end user functionality and flexibility.

To ensure that security is also addressed by these settings, DSD has reviewed the available settings and determined appropriate values.

Other settings

This section does not contain the full list of settings. Those setting not included here were not considered by DSD to have a direct impact on security and therefore are left up to the discretion of each agency.

Settings

BlackBerry Messenger policy group

The following settings control the BlackBerry Messenger application:

Name	Value	Notes
Disable BlackBerry Messenger	True	

Bluetooth policy group

The following group of settings controls the use of Bluetooth:

Name	Value	Notes
Allow Outgoing Calls	1	
Disable Address Book Transfer	True	
Disable Bluetooth	True	See Bluetooth Peripherals configuration guidance
Disable Desktop Connectivity	True	
Disable Dial-Up Networking	True	
Disable Discoverable Mode	True	See Bluetooth Peripherals configuration guidance
Disable File Transfer	True	
Disable Handsfree Profile	True	See Bluetooth Peripherals configuration guidance
Disable Headset Profile	True	See Bluetooth Peripherals configuration guidance
Disable pairing	True	If an agency has decided to implement Bluetooth, then this setting must be changed to "True" immediately after the approved peripherals have been paired, to prevent any additional, non-approved devices to be added later. See Bluetooth Peripherals configuration guidance
Disable serial port profile	True	

Continued on next page

Settings, Continued

Disable Wireless Bypass	True	
Require Encryption	True	This may cause compatibility issues with some Bluetooth peripherals. It is recommended that any peripherals used support encryption
Require LED Connection Indicator	True	
Require Password for Enabling Bluetooth Support	True	
Require Password for Discoverable Mode	True	

Browser policy group

The following group of settings controls the use of the browser:

Name	Value	Notes
Disable execution of Java script in the handheld browser	True	
Allow IBS Browser	False	
Disable Auto Synchronization in Browser	True	
MDS Browser JavaScript Enabled	False	

Camera policy group

The following setting controls the use of a camera if present in the device:

Name	Value	Notes
Disable Camera	[Agency decision]	No device with a camera should be brought into an area used to process classified information. If the functionality does not serve a business purpose then it should be disabled. If photography is needed for business reasons a dedicated device should be used for this purpose.

Continued on next page

Settings, Continued

**CMIME
application
policy group**

The following settings are BlackBerry Messenger items:

Name	Value	Notes
Allow Auto Attachment Download	False	

**Common policy
group**

The following group of settings controls some BlackBerry policies that apply to multiple groups:

Name	Value	Notes
BlackBerry Server Version	Null	Providing the version number may allow attackers to determine vulnerabilities more easily.
Disable Kodiak PTT	True	
Disable MMS	True	The Multimedia Message Service does not go via the BES.
Disable Voice-Activated Dialing	True	
IT policy notification	True	Advising users when policy settings have changed will allow them to better judge whether a handheld is not behaving as expected.
Lock owner info	3	Lock down the fields with as little identifying information as necessary.
Set owner info	[see Notes]	Include sufficient information to enable a lost handheld to be returned, with no further identifying information. Example: If found, please return to BlackBerry PO Box XXX etc.
Set owner name	[see Notes]	Include as little identifying information as necessary: Example: Government Device [Asset number if necessary]

Continued on next page

Settings, Continued

Desktop policy group The following group of settings controls the Desktop Policy:

Name	Value	Notes
Desktop password cache timeout	10 min	
Desktop allow desktop add-ins	False	Desktop software to be managed by the agency in accordance with the risk assessment.
Desktop allow device switch	False	Use to prevent users from switching to other devices.

Desktop-Only items The following settings are desktop-only items:

Name	Value	Notes
Auto backup enabled	True	
Auto backup include all	True	
Do not save sent messages	False	Ensure that a copy of all sent emails is saved.
Message Conflict Mailbox Wins	True	
Force load count	0	
Show application loader	False	
Show web link	False	

Device IOT Application policy group The following group of settings controls the diagnostics application for the handset:

Name	Value	Notes
Device Diagnostic App Disable	True	Device Diagnostics should only be run by support personnel

Continued on next page

Settings, Continued

Device-Only items

The following settings are non-grouped device-only items:

Name	Value	Notes
Allow Peer-to-Peer messages	False	
Allow SMS	[Agency decision]	Messages sent via SMS cannot be logged by the BES. Only UNCLASSIFIED messages may be sent.
Default browser config UID	Null	This will ensure that the default RIM browser is used.
Enable long term timeout	True	
Enable WAP configuration	False	Maintain accountability by forcing all Internet browsing to go through the BES.
Maximum password age	90 days	
Maximum security timeout	5 min	
Minimum password length	[see Notes]	Set to 7 or greater if pattern checks = 3. Set to 12 or greater if pattern checks = 0.
Password pattern checks	[see Notes]	Set to 3 if password length is less than 12. Set to 0 if password length is 12 or greater.
Password required	True	
User can change timeout	False	
User can disable passwords	False	

Continued on next page

Settings, Continued

Global Items The following group of settings controls global functions of the handset:

Name	Value	Notes
Allow Browser	[Agency decision]	It is recommended that if Internet access is required by BlackBerry users that this setting be set to TRUE and the default BlackBerry Browser should be used as it has been tested and certified by RIM. This will also ensure all internet access can be controlled by the MDS service of the BES. Periodic checks against user activity should be conducted to ensure inappropriate sites have not been accessed.
Allow Phone	[Agency decision]	Refer to the ACSI 33 for handling of the phone component of the device.
Auto signature	[Agency decision]	Ensure that no information identifying version numbers or that the email originated from a BlackBerry handheld is included.

Location Based Services The following settings control Location Based Services that use GPS data:

Name	Value	Notes
Disable BlackBerry Maps	True	If users are travelling outside Australia it is recommended that use of BlackBerry maps or any other mapping application is disabled.
Enable Enterprise Location Tracking	False	

Continued on next page

Settings, Continued

MDS policy group

The following group of settings controls the Mobile Data System services:

Name	Value	Notes
Disable activation with public MDSS	True	Users should not be able to configure their MDS settings
Disable user-initiated activation with MDSS	True	
Verify MDSS certificate	True	

Password policy group

The following group of settings controls the use of passwords:

Name	Value	Notes
Forbidden passwords	[Agency decision]	Refer to ACSI 33 for password usage
Maximum password history	8	No re-use within two years, based on a 90 day cycle.
Periodic challenge time	60 min	
Set maximum password attempts	5	
Set password timeout	5 min	
Suppress password echo	True	

PGP Application policy group

If used, the following group of settings defines how to configure PGP in accordance with *ACSI 33*:

Name	Value	Notes
PGP allowed content ciphers	0,1,2,5	Allows DACAs: AES (128), AES (192), AES (256) and 3DES.
PGP blind copy address	[Agency decision]	If used, seek legal advice on appropriate warnings to users.
PGP minimum strong DH key length	1024	
PGP minimum strong DSA key length	1024	
PGP minimum strong RSA key length	1024	

Continued on next page

Settings, Continued

UNCLASSIFIED

S/MIME Application policy group

If used, the following group of settings defines how to configure S/MIME in accordance with *ACSI 33*:

Name	Value	Notes
S/MIME allowed content ciphers	0,1,2,5	Allows DACAs: AES (128), AES (192), AES (256) and 3DES.
S/MIME blind copy address	[Agency decision]	If used, seek legal advice on appropriate warnings to users.
S/MIME minimum strong DH key length	1024	
S/MIME minimum strong DSA key length	1024	
S/MIME minimum strong ECC key length	163	
S/MIME minimum strong RSA key length	1024	

Security policy group

The following group of settings controls various aspects of security:

Name	Value	Notes
Allow external connections	False	Prevent the handheld from opening connections to the Internet
Allow internal connections	False	
Allow Outgoing Call When Locked	False	This does not affect the ability to make Emergency Calls
Allow smart card password caching	False	RIM recommendation.
Allow split pipe connections	False	Such connections can pass through the firewall without creating an audit trail.
Allow Third Party Apps to Use Persistent Store	[see Notes]	If no third party applications are installed or need this setting then this should be set to False.
Allow third party applications to use serial port	False	No third party applications are approved to use the serial port functionality
Application download control	[see Notes]	Limit the permitted downloads to certified applications only.
Certificate status cache timeout	1 day	

Continued on next page

Settings, Continued

Certificate status maximum expiry time	4 hours	
Disable 3DES transport crypto	True	Use AES encryption
Disable External Memory	True	
Disable email normal send	[see Notes]	If agencies have not implemented S/MIME or PGP, then set to False.
Disable forwarding between services	True	
Disable invalid certificate use	True	
Disable IP modem	True	Disable the modem capability where present.
Disable key store backup	True	
Disable key store low security	True	
Disable Media Manager	True	
Disable Message Normal Send	[see Notes]	If S/MIME or PGP has been implemented set this option to True to ensure usage.
Disable peer-to-peer normal send	True	
Disable persisted plaintext	True	Ensure that data stored in non-volatile memory is encrypted.
Disable radio when cradled	1	Do not allow the handheld to transmit RF when connected to workstations.
Disable revoked certificate use	True	
Disable Stale Certificate Status Checks	False	
Disable stale status use	True	
Disallow third-party applications download	True	
Disable untrusted certificate use	True	
Disable unverified certificate use	True	
Disable unverified CRLs	True	
Disable USB Mass Storage	True	
Disable weak certificate use	True	
FIPS level	2	

Continued on next page

Settings, Continued

Firewall Block Incoming Messages	MMS, PIN Messages (Public), PIN Messages (Corporate)	Agency to determine the use of SMS
Force Content Protection of Master Keys	True	
Force Include Address Book In Content Protection	True	
Force LED Blinking When Microphone Is On	True	
Forced lock when holstered	True	
Minimal encryption keystore security level	2	“2” = “high security”
Minimal signing keystore security level	2	“2” = “high security”
Secure Wipe Delay After IT Policy Received	[Agency decision]	The BES periodically sends policy updates to handsets. This setting can wipe the handset if a new policy has not been received within a certain time frame.

Service Exclusivity policy group

The following group of settings controls the service exclusivity:

Name	Value	Notes
Allow other browser services	False	Force all web browsing to go through the BES
Allow other message services	False	Force all email to go through the BES.
Allow Public AIM Services	False	
Allow Public Google Talk Services	False	
Allow Public ICQ Services	False	
Allow Public IM Services	False	
Allow public Yahoo! Messenger service	False	

Continued on next page

Settings, Continued

UNCLASSIFIED

TLS policy group

The following group of settings controls the use of Transport Layer Security (TLS):

Name	Value	Notes
TLS device side	False	
TLS disable invalid connection	0	0 = true & 1 = false
TLS disable untrusted connection	0	0 = true & 1 = false
TLS disable weak ciphers	0	0 = true & 1 = false
TLS minimum strong DH key length	1024 bits	
TLS minimum strong DSA key length	1024 bits	
TLS minimum strong ECC key length	163 bits	
TLS minimum strong RSA key length	1024 bits	
TLS Restrict FIPS Ciphers	True	

WTLS policy group

The following group of settings controls the use of Wireless Transport Layer Security (WTLS):

Note: WTLS mode allows users to bypass the agency's gateway infrastructure.

Name	Value	Notes
WTLS disable invalid connection	0	Disabled
WTLS disable untrusted connection	0	Disabled
WTLS disable weak ciphers	0	Disabled
WTLS minimum strong DH key length	1024 bits	
WTLS minimum strong ECC key length	163 bits	
WTLS minimum strong RSA key length	1024 bits	
WTLS Restrict FIPS Ciphers	True	
