~~SENSITIVE BUT UNCLASSIFIED~~

United States Department of State
and the Broadcasting Board of Governors
Office of Inspector General

Report of Inspection

Review of Department Headquarters' Implementation of Cellular Telephone Security Policies

Report Number SIA-I-07-01, September 2007

~~IMPORTANT NOTICE~~

~~This report is intended solely for the official use of the Department of State or the Broadcasting Board of Governors, or any agency or organization receiving a copy directly from the Office of Inspector General. No secondary distribution may be made, in whole or in part, outside the Department of State or the Broadcasting Board of Governors, by them or by other agencies or organizations, without prior authorization by the Inspector General. Public availability of the document will be determined by the Inspector General under the U.S. Code, 5 U.S.C. 552. Improper disclosure of this report may result in criminal, civil, or administrative penalties.~~

~~SENSITIVE BUT UNCLASSIFIED~~

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This Office of Inspector General (OIG) review examined ten of the Department of State's (Department's) 50-plus bureaus and major offices for compliance with the Department's cellular telephone policies in areas where classified information is discussed and processed, exclusive of Sensitive Compartmented Information Facilities (SCIFs) and Secure Work Areas (SWAs). None were found to be fully compliant. Three of the nine bureaus and the one office that were reviewed were found to be partially compliant. The remainder were not in compliance.

The two principal reasons that interviewees gave for the lack of compliance were unawareness of the Department's policies in areas outside SCIFs and SWAs and the need for cellular telephone communication, both official and personal, in office areas, to include areas where classified information is discussed and processed. An additional factor contributing to the lack of awareness of the Department's policies are the policies themselves, which are inconsistent, misleading, and dispersed throughout the Department's Foreign Affairs Manual (FAM) and Foreign Affairs Handbook (FAH).

(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2) (b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2) (b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2) (b) (2)(b) (2) However, recognizing the proliferation of cellular telephones, including U.S. government-issued cellular telephones, such policies need to balance users' needs against known security vulnerabilities and threats.

This report recommends: 1) reevaluating the Department's cellular telephone policies to balance users' needs against known threats and vulnerabilities; 2) ensuring consistency between the security requirements for cellular telephones and other devices that have cellular telephone capability; 3) consolidating all cellular telephone security requirements at one location in 12 FAM, *Diplomatic Security;* 4) including cellular telephone security requirements in the Department's introductory security briefing and in the unit security officer guidebook; and 5) including Blackberry cellular telephone security requirements on the Blackberry Enterprise Server (BES) web site and in the user agreement for users of the Department's Blackberry Personal Digital Assistants (PDAs).

BACKGROUND

Since the introduction of cellular telephone service in the United States in 1983, cellular telephones have increased both in usage and in available features. According to Bureau of Labor Statistics,[1] the estimated percentage of U.S. households that reported having received a cellular telephone bill rose steadily from approximately two percent in the first quarter of 1994 to approximately 47 percent in the first quarter of 2003. Early cellular telephones had only telephonic capability. Current devices can have text messaging, Internet browsing, music recording and playback, voice recording, video and still picture recording, radio capability, and can employ Bluetooth,[2] Wi-Fi,[3] and infrared connectivity. Cellular telephones with still picture or video capturing capability were first produced in 1997. According to an industry source, two-thirds of the cellular telephones sold in the fourth quarter, 2006, had video capturing capability.[4] Personal digital assistants (PDAs), such as the PalmPilot that was introduced in 1996, were initially designed to function solely as a handheld computer for organizing personal information. However, since their introduction new features have continually been added. Among the features available with the current generation of PDAs, such as the Blackberry, is cellular telephone capability, as well as many of the added features found in current cellular telephones, such as still picture and video recording.

(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)

---

[1] *Household Telephone Service and Usage Patterns in the U.S. in 2004: A Demographic Profile.*

[2] An industrial specification for wireless personal area networks (PANs) that provides a way to connect and exchange information between devices such as cellular telephones, laptop computers, personal computers, and video game consoles.

[3] Derived from "wireless fidelity," a brand licensed by the Wi-Fi Alliance to describe the embedded technology of wireless local area networks (WLAN) based on the Institute of Electronic and Electrical Engineers (IEEE) 802.11 specifications.

[4] *The Online Reporter,* March 30, 2007.

The Department's domestic policy regarding the use of cellular telephones in Department facilities is described in Department Notice dated June 12, 2002 (2002-06-017), *Policy for Use of Cellular Telephones and Personal Digital Assistants (PDAs) Within Department Buildings,* and 5 FAM 526.2 *Restrictions for Cellular Telephones Usage.* The main security requirements set forth in these documents are that cellular telephones, both personal and U.S. government-issued, must be turned off in areas where classified information is discussed or processed, and they must not be placed within ten feet of classified processing equipment. Furthermore, according to 5 FAM 526.2 i, cellular telephones that have still picture or video capturing functions are not allowed in Department of State domestic facilities.

OBJECTIVE, SCOPE, AND METHODOLOGY

The objective of this review was to determine how well the Department is complying with security policies regarding cellular telephones, and devices having cellular telephone capabilities, in those areas of the Department where classified information is discussed and processed.

This review did not examine compliance with cellular telephone policies pertaining to SCIFs or SWAs, as set forth in Director of Central Intelligence Directive (DCID) 6/9, *Physical Security Standards for Sensitive Compartmented Information Facilities*, including Intelligence Community Policy Memorandum (ICPM) 2005-700-1, Attachment 1 (Annex D) and Attachment 2. This review also did not examine cellular telephone policies pertaining to overseas posts, as described in 12 FAH-6 H-531.1 *Cellular Telephone Standards.*

This review was conducted through interviews and reviews of the policies and procedures at a select number of bureaus and principal offices in the Department. For economy, nine bureaus and one principal office were selected from the 50-plus bureaus and principal offices in the Department. These were: the Office of the Coordinator for Counterterrorism (S/CT); the Bureau of Administration (A); the Bureau of Diplomatic Security (DS); the Bureau of Overseas Buildings Operations (OBO); the Bureau of International Narcotics and Law Enforcement Affairs (INL); the Bureau of European and Eurasian Affairs (EUR); the Bureau of Political-Military Affairs (PM); the Bureau of Economic, Energy, and Business Affairs (EEB); the Bureau of Public Affairs (PA); and the Bureau of Population, Refugees, and Migration (PRM). The personnel interviewed in the bureaus/office were principally the Unit Security Officer (USO) or Principal Unit Security Officer (PUSO). In addition, the responsible Bureau Security Officer (BSO)[5] was interviewed in those offices that had them.

[5]Bureau Security Officers are full-time, professional security officers, either Foreign Service or Civil Service, from the Bureau of Diplomatic Security, who are assigned to serve as a bureau's senior security advisor and to oversee and mentor the bureau's Unit Security Officers and Special Security Representatives.

Because direct examination for compliance with the Department's cellular telephone policy, i.e., monitoring cellular telephone usage in areas where classified information is discussed or processed, determining whether personnel have cellular telephones within ten feet of classified processing equipment, and determining whether personnel have cellular telephones with still picture or video capturing functions, was deemed to be impractical, this review attempted instead to assess each bureau/office's compliance indirectly by means of the following questions:

1) Does the bureau/office have written procedures or guidelines for cellular telephone usage in those areas where classified information is discussed or processed?

2) Are bureau/office personnel briefed or otherwise notified of the requirements of the Department's cellular telephone policies?

3) Does the bureau/office have and use lockable storage boxes or taken other reasonable measures for the storage of cellular telephones that cannot be brought into work areas?

4) In the opinion of the responsible USO, PUSO, or BSO are bureau/office personnel complying with the Department's cellular telephone policies?

This review assessed each bureau/office's compliance with the Department's cellular telephone security policies based upon: a) an analysis of the bureau/office official's responses to the above questions; b) a review of associated documents; and c) a physical examination of the bureau/office area. An assessment of "being in compliance" did not require or necessarily result from affirmative answers to all of the above questions. For example, during this review it was found that a sub-office of one bureau/office had no written policy, but yet was assessed to be fully compliant because on the sub-office's access-controlled entrance door was a large sign stating that no cellular telephones were permitted in the office and that all cellular telephones must be stowed in the storage rack in the office entrance area. The reviewing officer found the rack full of cellular telephones, giving one reason to believe that the office is following the Department's cellular telephone policies. Another bureau/office had a well-written cellular telephone policy, storage boxes, and other measures for cellular telephone storage, and good cellular telephone procedures, yet was deemed not to be fully compliant because their written policy and their employee security briefings made no mention of the restrictions on cellular telephones with still picture or video capturing functions.

This review was conducted in Washington from January 8 to February 7, 2007, by Security and Intelligence Advisor Marilyn M. Wanner and Deputy Security and Intelligence Advisor Thomas C. Allsbury.

FINDINGS AND RECOMMENDATIONS

Overview

Using the above criteria for assessing compliance with the Department's cellular telephone policies, the bureaus/office that were reviewed could be categorized as being "fully compliant," i.e., fully complying with all aspects of the Department's cellular telephone security policies in all areas; "partially compliant," i.e., not meeting all aspects of the Department's cellular telephone security policies or not meeting them at all locations; or "noncompliant," i.e., not meeting any aspects of the Department's cellular telephone security policies in any office areas. This review found none of the reviewed bureaus/office to be "fully compliant." Three of the ten were found to be "partially compliant" and the remaining seven were found to be "noncompliant."

The most common reasons that were given for noncompliance to the Department's cellular telephone policies were lack of awareness of the applicable policies and the expressed need to use cellular telephones in the office area, including those areas where classified information is discussed and processed. Interviewees in four of the reviewed bureaus/office admitted to being unaware of the existence of any domestic cellular telephone security restrictions where classified information is discussed or processed in non-SCIF/SWA areas prior to this review. However, of those four, three were aware of the Department's cellular telephone restrictions concerning SCIFs and SWAs. Interviewees in five of the reviewed bureaus/office expressed the need for office personnel to have and use their cellular telephones in the office area. These needs were both personal and official. Examples of personal situations that were cited that required the use of the cellular telephone in the office were a seriously ill family member, a pregnant spouse, small children in daycare, and a restraining order against an ex-spouse. The most frequently given reason for the official use of cellular telephones in office areas was the communication needs of office principals. Other reasons that were given were that information management and general services personnel, who are on-call to provide service to their respective bureaus/office, need to stay in constant communication with their central office, and emergency response personnel who use their cellular telephones for emergency communication.

Awareness of Cellular Telephone Policies

The lack of awareness of the Department's domestic cellular telephone security restrictions stems from the lack of instruction. Prior to being issued a building pass and given access to classified information, all new Department employees are required to attend a half-day introductory security briefing. This briefing covers the processing, handling, and storage of classified information but does not cover cellular telephone restrictions in areas where classified information is discussed or processed.

A second opportunity exists for briefing new employees on the Department's domestic cellular telephone security restrictions through the USO or PUSO briefings. 12 FAM 563.1 requires the head of each domestic functional area to designate a PUSO to assist in carrying out the area's security responsibilities. PUSOs in larger functional areas may designate USOs to help carry out these responsibilities. The duties of PUSOs and USOs are described in *Principal Duties of a Unit Security Officer-A Guidebook*, dated October 2004. Among these duties is briefing new employees on the office's security practices. For that purpose the guidebook has a checklist (Appendix C – Security Orientation Checklist) that lists the topics to be covered and requires the employee's signature that they have been briefed on these topics. While this checklist includes the cellular telephone restrictions regarding SCIFs, neither the checklist nor the guidebook discusses cellular telephone restrictions where classified information is discussed or processed in non-SCIF/SWA areas. In addition, this review found that some offices/bureaus are not providing PUSO/USO briefings for new employees, but rather are depending solely on the introductory security briefing to make new employees aware of classified handling policies.

Recommendation 1: The Bureau of Diplomatic Security should include domestic cellular telephone security requirements in the introductory security briefing given to all new Department employees and in the unit security officer guidebook. (Action: DS)

Cellular Telephone Policies

Aggravating the lack of awareness of the Department's cellular telephone security policies are the policies themselves, which are dispersed throughout the FAMs/FAHs, lack consistency, and are misleading.

The primary Department policy concerning cellular telephone restrictions is 5 FAM 526.2 *Restrictions for Cellular Telephones Usage*. As discussed above, it states that domestically, where classified information is discussed or processed, U.S. government and personally-owned cellular telephones are permitted provided they are turned off and not placed within ten feet of classified processing equipment. Furthermore, cellular telephones that have still picture or video capturing functions are not allowed in Department domestic facilities. Not discussed in this portion of the FAM are Bluetooth devices which provide connectivity between the earpiece and the cellular telephone, thereby providing hands-free operation of the cellular telephone. Bluetooth devices are prohibited in Department facilities, as stated 5 FAM 584.3 *Ancillary Telephone Accessories*.

At present there is no FAM or FAH on PDAs (most common is the Blackberry); although at the time of this review a FAM on PDAs, including PDAs with cellular telephone capability, had been drafted and was in the final stages of review. However, that policy is tentatively proposed for release as 12 FAM 683 *Personal Digital Assistant (PDA)*. Furthermore, there are some inconsistencies between that draft policy and 5 FAM 526.2. For example, the draft PDA policy does not have the ten-foot requirement of 5 FAM 526.2. During this review, a senior Department technical security official said that this requirement is excessively stringent and is not justifiable in the present-day technological environment. The draft PDA policy requires visitors to turn off their PDAs in areas where classified information is discussed or processed, but only requires Department employees to turn them off when not in use. Furthermore, instead of the prohibition against cellular telephones with still picture or video capturing capability found in 5 FAM 526.2, the draft PDA policy only requires that the lenses of such devices be covered.

As discussed above, a common misperception of personnel who were interviewed as part of this review is that domestic cellular telephone restrictions only apply to SCIFs and SWAs. A possible contributor to this misunderstanding is the first paragraph of 5 FAM 526.2 *Restrictions for Cellular Telephones* Usage, which reads:

> *"a. There are two different directives regarding the use of cellular telephones. Domestic usage is derived from Director of Central Intelligence Directive (DCID) 1/21.[6] Usage abroad is derived from Overseas Security Policy Board (OSPB) Security Standards and Policy Handbook 12 FAH-6 H-531.1. Both directives apply to all persons, whether employees or visitors."*

As DCID 1/21 and 6/9 pertain only to SCIFs and SWAs, this paragraph implies that domestically, cellular telephone restrictions only pertain to SCIFs and SWAs. However, this is not correct. Paragraph b. of 5 FAM 526.2, after a description of the cellular telephone restrictions for SCIFs and SWAs, states:

> *"In other domestic areas where classified information is discussed or processed, U.S. Government and personally owned cellular telephones are permitted providing the cellular telephone: (1) remains off; and (2) is never placed within 10 feet from equipment processing classified information."*

(b) (2)

Recommendation 2: The Bureau of Diplomatic Security, in coordination with the Bureau of Information Resource Management, should consolidate all the security requirements for cellular telephones, cellular telephone accessories, and devices with cellular telephone capabilities, such as Personal Digital Assistants, into one location in 12 FAM, *Diplomatic Security*. These requirements should be revised as needed to: a) ensure consistency between the requirements for cellular telephones and other devices with cellular telephone capabilities, b) clarify the applicability of security requirements in non-SCIF/SWA areas, and c) balance users' needs against known security vulnerabilities and threats. (Action: DS, in coordination with IRM)

[6] DCID 1/21 was replaced by DCID 6/9 on November 18, 2002.

Blackberry Enterprise Server (BES) Program

The establishment of the Department's Blackberry Wireless PDA program brought a new dimension to the issue of cellular telephones in areas where classified information is discussed and processed. The program was introduced in July 2005.[7] As of October 2006, according to IRM documents, there were nearly 800 Department users enrolled in the Blackberry Enterprise Server (BES) Program. Blackberry PDAs provide users with the ability to access Outlook through the exchange server, including its e-mail, calendar, and contacts applications. In addition, these Blackberries also have cellular telephone capability. The BES web site (http://bes.irm.state.gov/index.cfm) has information about acquiring, activating, and using the Blackberry, but no information about the restrictions of the cellular telephone component of the Blackberry, and no reference to 5 FAM 526.

Recommendation 3: The Bureau of Diplomatic Security, in coordination with the Bureau of Information Resource Management, should provide detailed cellular telephone security requirements, applicable to the Department's Blackberry Wireless Personal Digital Assistant, on the Blackberry Enterprise Server Program web site and in the user's acknowledgement statement required for all Department Blackberry users. (Action: DS, in coordination with IRM)

[7]Department Announcement number 2005_07_018, dated July 7, 2005, *Blackberry Wireless PDA Use in the Department of State.*

RECOMMENDATIONS

Recommendation 1: The Bureau of Diplomatic Security should include domestic cellular telephone security requirements in the introductory security briefing given to all new Department employees and in the unit security officer guidebook. (Action: DS)

Recommendation 2: The Bureau of Diplomatic Security, in coordination with the Bureau of Information Resource Management, should consolidate all the security requirements for cellular telephones, cellular telephone accessories, and devices with cellular telephone capabilities, such as Personal Digital Assistants, into one location in 12 FAM, Diplomatic Security. These requirements should be revised as needed to: a) ensure consistency between the requirements for cellular telephones and other devices with cellular telephone capabilities, b) clarify the applicability of security requirements in non-SCIF/SWA areas, and c) balance users' needs against known security vulnerabilities and threats. (Action: DS, in coordination with IRM)

Recommendation 3: The Bureau of Diplomatic Security, in coordination with the Bureau of Information Resource Management, should provide detailed cellular telephone security requirements, applicable to the Department's Blackberry Wireless Personal Digital Assistant, on the Blackberry Enterprise Server Program web site and in the user's acknowledgement statement required for all Department Blackberry users. (Action: DS, in coordination with IRM)

ABBREVIATIONS

A	Bureau of Administration
BES	Blackberry Enterprise Server
BSO	Bureau security officer
DCID	Director of Central Intelligence Directive
DS	Bureau of Diplomatic Security
EEB	Bureau of Economic, Energy, and Business Affairs
EUR	Bureau of European and Eurasian Affairs
FAH	Foreign Affairs Handbook
FAM	Foreign Affairs Manual
ICPM	Intelligence Community Policy Memorandum
INL	Bureau of International Narcotics and Law Enforcement Affairs
IRM	Bureau of Information Resource Management
ITCCB	Information Technology Change Control Board
OBO	Bureau of Overseas Buildings Operations
OSPB	Overseas Security Policy Board
PA	Bureau of Public Affairs
PDA	Personal Digital Assistant
PM	Bureau of Political-Military Affairs
PRM	Bureau of Population, Refugees, and Migration
PUSO	Principal unit security officer
RIM	Research In Motion, Limited

SCIF	Sensitive compartmented information facilities
S/CT	Office of the Coordinator for Counterterrorism
SWA	Secure work area
USO	Unit security officer