MANAGEMENT OF WIRELESS COMMUNCIATION DEVICES

EXECUTIVE SUMMARY

We found that the Commission can improve its management of wireless communication devices (such as Personal Digital Assistants or PDAs, cell phones, and pagers). The Office of Information Technology (OIT) needs to remind office heads of the requirements of the PDA regulation (SECR 24-5.2) to improve compliance with the regulation and enhance controls. Also, the regulation needs to be revised to clarify the role of OIT and the IT Specialists, and to cover cell phones and pagers, in addition to PDAs. All wireless users should be required to sign written agreements and the Offices of Information Technology and Administrative Services should improve property management for wireless devices and eliminate any excess devices.

SCOPE AND OBJECTIVES

Our objective was to determine if the management of wireless communication devices needs to be improved. We also evaluated the adequacy of the Commission regulation on PDAs (SECR 24-5.2), and the extent of compliance with certain parts of this regulation. We did not evaluate whether Commission staff were appropriately protecting sensitive information on wireless devices.

Our audit steps included interviews with staff from the Office of Information Technology (OIT), the Office of Administrative Services (OAS), and other Commission offices. We also reviewed applicable guidance, vendor and user agreements, invoices, and the list of users.

Our audit was performed in accordance with generally accepted government auditing standards between October 2004 and December 2004.

BACKGROUND

Commission Regulation SECR 24-5.2, issued November 4, 2002, governs the use of Personal Digital Assistants (PDAs) and similar technologies by Commission staff and contractors. The regulation covers both Commission-issued and employee owned PDAs.

Under the regulation, PDA users must comply with applicable regulations and laws (e.g., the Government Information Security Reform Act) and SECR 24-4.3, Use of SEC Office Equipment). Users must sign a service agreement, and protect agency data on their devices.

Office heads are responsible for authorizing PDA use within their offices; maintaining user agreements within their office; ensuring that office employees use secure information practices; and authorizing unannounced audits of PDAs when appropriate. OIT technical staff and contractors are required to provide full support to Commission-owned PDAs, and limited support to employee-owned PDAs.

The Commission issues a Blackberry (a type of PDA) to authorized users. The Blackberry provides access to Commission e-mail and the Internet, links to users' workstations, and interfaces with agency systems. It also serves as a cell phone and walkie-talkie.

OIT began deployment of Blackberries during December 2003. To date, OIT has issued approximately 800 of these devices, and plans to purchase and distribute 200 more. Generally, the IT Specialist within each office coordinates requests for Blackberries and distributes them to employees.

Under a government-wide contract, each Blackberry costs about $200. The Commission as of September 2004 paid over $53,000 per month for use of its Blackberries (about $66 for each device). This fee includes the monthly access fee ($49.99), data features, and additional charges (such as for roaming and taxes).

Besides PDAs, the Commission issues cell phones and pagers to authorized employees who do not need a link with their desk top computer. OIT manages the acquisition of cell phones from several providers (Nextel, Verizon, and AT&T).

A total of 124 cell phones have been issued to employees. During September 2004, the Commission paid approximately $6000 for the cell phones, or an average of about $49 per phone.

Until recently, the Office of Administrative Services (OAS) managed pagers. OAS leased 146 pagers for about $1900 per month, an average of $13 each. The monthly usage rate varies depending upon the features and level of service offered by the pager. OIT has now assumed management of pagers, thereby consolidating the management of wireless devices in one office.

Currently, the Commission uses three types of pagers. High end pagers can send and receive e-mails, manage personal information, and access the Internet. Middle range pagers permit text messaging and receipt of e-mail, but cannot access the Internet. Pagers at the low end only allow receipt of a caller's telephone number or short message on their screen.

AUDIT RESULTS

We found that the Commission can improve its management of PDAs, cell phones, and pagers. The regulation covering PDAs can be expanded or supplemented to explicitly include cell phones and pagers, which are similar wireless devices.

We found that the Commission offices and divisions we surveyed had little awareness of the PDA regulation, and have not done enough to implement it. Most users have not signed service agreements, office heads have not issued guidance on appropriate use of the devices, and unannounced audits of PDA use have not been performed. Also, OIT does not have adequate inventory records for PDAs, and the number of unassigned PDAs (which the Commission is paying for) could exceed Commission needs.

Given the substantial risk to Commission information security and the significant and growing cost (approximately three-quarters of a million dollars per year) of these devices, better controls to manage them are needed. Our detailed findings and recommendations are described below.

Improve the PDA Regulation

The current PDA regulation (SECR 24-5.2) can be improved in several respects:

- The regulation can be modified to explicitly cover all wireless devices (*i.e.*, cell phones and pagers in addition to PDAs) or a separate regulation could be issued for cell phones and pagers;
- The role of the office IT Specialist can be specified (currently, no mention is made of the Specialist, who generally is responsible for processing PDA requests and for distribution of PDAs); and
- The regulation can clarify the management responsibilities of OIT (currently, the regulation only covers OIT's responsibilities for technical support), including publicizing the regulation, monitoring compliance with the regulation, and maintaining appropriate records and procedures.

Recommendation A

OIT should modify the PDA regulation as discussed above.

Implement the PDA Regulation

We contacted a number of Commission offices and divisions, and found that they were generally unfamiliar with the PDA regulation, and had not taken sufficient steps to implement it, as discussed below.

Service Agreements

The PDA regulation (6-a-1) indicates that users are required to sign a service agreement (attached to the regulation) and ensure that the authorizing office head signs the agreement prior to using a PDA for work-related purposes. Although 739 Blackberry users are listed in the Commission network (in Microsoft Outlook, under the Public Folders tab, Blackberry Contact List), we were able to obtain only 183 service agreements signed by the users. Only ten of these were signed by the office head.

All of the 183 signed service agreements appeared to be for Commission-owned, rather than employee-owned, PDAs. Thus, it appears that any employees using personal PDAs at work are not signing service agreements.

The PDA regulation also requires that the service agreements are to be maintained on file within the offices (6-b-2). We found that offices generally were not maintaining these agreements (we obtained most of the 183 agreements from the Commission contractor which distributed the PDAs).

The service agreement is a key control over PDAs. It identifies the specific PDA being issued, thereby acting as a hand receipt and inventory control mechanism.

In addition, the agreement specifies that the user will not use the device in a manner that will compromise agency data, and indicates the required security features for PDA use. The agreement also allows the agency to inspect the PDA for official purposes (such as in the course of a security audit or an investigation). Thus, the service agreement helps protect the Commission from misuse of the PDA which could compromise agency data. Without the signed service agreement, controls over PDA use are deficient.

Secure Information Practices

The PDA regulation (6-b-3) requires office heads to ensure that their employees make use of secure information practices. Specifically, office heads are to

- Determine what kinds of information used by their office should be treated as sensitive or non-public;
- Provide regular guidance to staff regarding any sensitive or non-public information in the office that may not be transferred to PDAs; and
- Determine if and when the use of personally owned devices should be limited or prohibited within a particular office.

We found that the offices we surveyed had not implemented the above requirements because of a lack of familiarity with the PDA regulation. Thus, the purpose of the regulation (to ensure PDA use complies with secure information practices) is at risk.

Unannounced Audits

The PDA regulation (6-b-4) also provides that office heads are responsible for authorizing unannounced audits of PDA use within their offices if they believe that there is a significant risk that employees or contractors are not following secure information practices. This part of the regulation, like the other parts discussed previously, also has not been implemented. Given the lack of general compliance with the regulation, unannounced audits may be appropriate.

Recommendation B

OIT should issue a memorandum to office heads and division directors reminding them of the procedures required by the PDA regulation, as discussed above. The memorandum should ask the office heads and division directors to distribute PDA user's guides to their

staff; ensure that service agreements are signed for all PDAs connecting to the network (Commission or employee-owned); and ensure that their staff make use of secure information practices.

Improve Property Management for Wireless Devices

OIT has not developed inventory records for all Commission PDAs which identify the PDA and the assigned user, and list any unassigned PDAs. The only record is an unofficial list of the name, number, and office of Commission Blackberry users posted on the network. While the value of each PDA is under $5000 (and thus PDAs are not required to be recorded on the Commission's property records), the sensitivity of PDA data and the cost to use PDAs ($67 monthly for each Blackberry) make inventory records desirable.

The Commission may be paying excess costs for unassigned PDAs. The September 2004 Blackberry invoice included charges for 799 devices. However, the Blackberry contact list on the network includes only 744 devices, 55 less than the invoice. The monthly cost of these 55 devices is approximately $3,700.

Recommendation C

In consultation with affected offices, OIT should prepare inventory records for all Commission PDAs, including unassigned PDAs as discussed above. Any PDAs that cannot be located should be deactivated and reported as lost. OIT should consider whether the number of unassigned PDAs exceeds Commission needs.

Evaluate Pager Use

Approximately 86 employees use one-way pagers. The cost of leasing these pagers is about $7.00 each, for a total of $602 per month.

Several users told us that these pagers did not meet their needs and that they no longer use them. One recurring complaint was that users did not receive all of their pages.

Recommendation D

The Office of Information Technology should review billing information on the use of one- way pagers. OIT should provide this information to Commission office heads and division directors, who can then determine whether the pagers are still required or the leases can be canceled.

Provide Cost Information

The PDA Regulation (6-a-4) requires that PDAs be used for personal purposes during non-work hours only. Any personal use must not interfere with official business and involve minimal additional expense to the government.

Currently, Blackberry users are not told how much the device costs for each use. Thus, they cannot easily determine whether their personal use of the device complies with the regulation (*i.e.*, the use involves minimal additional expense). This information should be made available to

users to help them comply with the regulation. In addition, the information would help users decide when the use of the device for official business is cost-effective (*e.g.,* when they are in travel status).

Recommendation E

OIT should notify users of wireless communication devices of the budgeted number of minutes and messages for their devices. OIT should also provide users with the Commission's policy on permissible use of PDAs.

.