BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

AUDIT OF BLACKBERRY AND CELL PHONE INTERNAL CONTROLS

OFFICE OF INSPECTOR GENERAL

March 2009

BOARD OF GOVERNORS
OF THE
FEDERAL RESERVE SYSTEM
WASHINGTON, D. C. 20551

OFFICE OF INSPECTOR GENERAL

March 31, 2009

Ms. Maureen Hannan, Director
Information Technology Division
Board of Governors of the Federal Reserve System
Washington, DC 20551

Dear Ms. Hannan:

The Office of Inspector General (OIG) of the Board of Governors of the Federal Reserve System (Board) has completed an audit of the Division of Information Technology (IT) procedures, entitled *Board of Governors of the Federal Reserve System BlackBerry and Cell Phone Procedures and Inventory Control Process*, issued June 20, 2008. These procedures were created to strengthen controls for managing and accounting for cell phones and BlackBerrys throughout the Board. In June 2008, the IT division requested that the OIG conduct an audit of the recently issued procedures.

Background

The Board provides cell phones and BlackBerrys to certain employees for business purposes, to facilitate communication when employees are away from their desks, such as in meetings, on travel, or in training. The BlackBerry extends the Board's data and applications, including email, personal information management, and document management, to mobile users.

The Voice Communications section of the IT division is responsible for establishing, monitoring, and maintaining contracts with the service providers of cell phones and BlackBerrys. Specifically, the Voice Communications staff, in conjunction with the Lotus Notes Support Group, performs the following management-related services for cell phones and BlackBerrys: (1) placing orders for devices and service-related requests with four service providers, (2) issuing cell phone and BlackBerry equipment to Board employees, (3) conducting periodic physical inventories, (4) reviewing and approving payment for monthly bills, and (5) coordinating with the National Security Agency (NSA) for the disposal of the devices. IT also maintains a Secure Inventory Closet (SIC) to store cell phones and BlackBerrys that have been ordered but not yet assigned to an employee or that have been returned and are awaiting disposal.

Objective, Scope, and Methodology

Our audit objective was to evaluate the effectiveness of the Board's recently revised BlackBerry and cell phone procedures. Specifically, we evaluated the controls over the receiving, tracking, securing, and disposing of BlackBerrys and cell phones. As of October 2008, approximately 1,123 BlackBerrys and cell phones were in use by Board employees. During calendar year 2008, the Board paid $669,807 to four vendors for services related to such devices. To accomplish our objectives, we identified and examined the policies and procedures governing the receiving, tracking, securing, and disposing of BlackBerrys and cell phones, including the inventory control process; and met with cognizant IT staff responsible for these devices. We reviewed documentation for a judgmental sample of fourteen requests for devices to ensure they were made by authorized division personnel. We also performed tests to ensure that the devices were properly secured by evaluating the physical controls over access to devices that are stored in the SIC. We compared a random sample of seventy-five out of 426 entries from the "Badge Access" log to the SIC transaction log to ensure that all entries to the SIC were recorded.

To determine whether the tracking systems are accurate and complete, we counted BlackBerrys and cell phones stored in the SIC and compared our count (ninety) to the number of devices listed in the Inventory Control Equipment (equipment) database. We randomly selected seventeen of ninety in-stock BlackBerrys and cell phones and traced descriptive information, such as make, model, and serial number, to the equipment database. To ensure that the devices are returned when employees leave the Board and that the equipment database is updated appropriately, we compared a list of separated employees from the Board's personnel database for the period of February 1 through September 30, 2008 with the devices listed as assigned in the equipment database. To ensure proper disposal of the devices, we reviewed and verified a one month period of disposal forms to determine if they were completed in accordance with established procedures, including signatures by IT and NSA personnel. We also selected and verified that a random sample of eleven of 213 devices, listed on an inventory sheet attached to the July 2008 disposal form, were moved from the assigned status to disposed status in the equipment database.

We conducted this performance audit from July 2008 through January 2009, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Results

Overall, we found that the IT division has established a number of controls for cell phones and BlackBerrys, and that the majority of these controls are working effectively. Our testing did not identify any significant discrepancies. The documentation we reviewed was sufficient to verify that (1) requests for devices are made by authorized division staff; (2) new orders for

devices are received at the Board and can be tracked to an authorized end user; (3) devices stored temporarily or as "in-stock" devices are protected from unauthorized use and can be reconciled with inventory records; and (4) devices targeted for disposal are properly tracked.

Our fieldwork did, however, identify opportunities to improve existing controls used to manage and account for devices. Specifically, we found that all entries to the SIC are not recorded in the SIC transaction log, and that a surveillance camera positioned outside the SIC and used to provide security for the SIC does not capture the device-related activities occurring within the SIC. In addition, duties are not properly segregated which increases the risk of loss, theft, or unauthorized use of devices; IT staff responsible for storing and removing devices from the SIC were also recording the transactions to the equipment database. We also found that the IT division has not communicated to all divisions the need to make a timely return of devices or coordinated with the Management Division (MGT) to receive notification of employees separating from the Board.

Our report contains three recommendations designed to address these issues, which we believe will help reduce the risk of loss, theft, or unauthorized use of devices. Based on the work performed during the audit, we also provided IT management with updated flowcharts of the processes for receiving, tracking, securing, and disposing of BlackBerrys and cell phones. Our specific findings and the resulting three recommendations are discussed in detail in Appendix 1.

Analysis of Comments

We provided our draft report to you for review and comment. In your response, included as Appendix 2, you concurred with our assessment that opportunities exist to further strengthen several controls, and agreed or partially agreed with each of our three recommendations. In your detailed response to recommendation 1, you agreed that the SIC transaction log should be used to record the transfer of BlackBerry and cell phone devices into and out of the SIC. However, you added that the log is not intended to track when someone accesses the SIC to store or retrieve low cost, consumable items, and that a reconciliation to the "Badge Access" log is not needed at this time. We note that low cost, consumable items could be stored elsewhere, and that the SIC may then be used to store BlackBerrys and cell phones exclusively. The intent of our recommendation is to ensure that individuals who access the SIC also record their associated activities or transactions—such as adding or removing devices and conducting inventories—in the SIC transaction log, consistent with IT procedures. Periodically reconciling the SIC transaction log with the "Badge Access" log also helps to ensure accountability and provides a baseline should any devices be found missing.

Your response also stated that it would not be efficient to expand the use of cameras to record the actions by staff within the SIC, and that the camera in its current position achieves its objective of deterrence and recording who accesses the SIC. During our review, we were told that the IT Division plans to relocate the SIC to a larger area that could allow for a different camera position to record the activities within the SIC. The intent of our recommendation is to analyze how the camera position can be improved to more closely monitor BlackBerry and cell phone devices stored in the SIC. We maintain that more effective camera placement can further

strengthen controls by tracking and recording not only who is accessing the SIC, but also what devices they are accessing.

Your response indicated your general agreement with recommendation 2, noting that IT currently addresses separation of duties for mobile devices by separating purchase authority from administration authority. The intent of our recommendation is to separate duties within the inventory control function. For the same reason that IT prohibits staff who purchase mobile devices from having full access to the SIC inventory or the associated equipment database records, staff who have access to the SIC, and are responsible for removing and distributing devices, should not have full access rights to the equipment database.

You agreed with recommendation 3 and stated you intend to develop processes to more effectively identify devices that are not in use.

Major contributors to this report were Mr. Kyle Brown, Senior Auditor and Project Leader; Ms. Jennifer A. Rosholt, Auditor; Ms. Cynthia D. Gray, Project Manager; and Mr. Andrew Patchan, Jr., Assistant Inspector General for Audits and Attestations. This report will be added to our public web site and will be summarized in our next semiannual report to Congress. We will follow-up on the implementation of the recommendations as part of our future audit activities. We appreciate the cooperation of your staff during this review. Please contact me if you would like to discuss this report or any related issues.

Sincerely,

/signed/

Elizabeth A. Coleman
Inspector General

cc: Mr. Steve Malphrus
Mr. Po Kim
Ms. Sue Marcyz
Mr. Peter Both

Appendix 1

Findings and Recommendations

1. **We recommend that the Director of IT: (a) ensure that all entries to and transactions made in the Secure Inventory Closet (SIC) are recorded in the SIC transaction log, (b) perform a monthly reconciliation to the "Badge Access" log, and (c) analyze how the SIC security camera can be positioned to closely monitor IT personnel actions regarding devices stored in the SIC.**

Overall, the IT division uses a comprehensive security system that includes locks, camera surveillance, badge access pads, and manual and automated access logs to secure BlackBerrys and cell phones. However, we found opportunities to improve existing controls by (1) recording all entries to the SIC in the manual SIC transaction log, and (2) repositioning the SIC surveillance camera to capture activities within the SIC. During our audit, we also found weaknesses related to the design and format of the monthly automated "Badge Access" log, which the IT division corrected after we brought these matters to their attention.

We found that BlackBerrys and cell phones are stored in their own locked cabinets within the SIC. The SIC is secured by both lock and badge reader. In addition, a camera is located outside the SIC door for surveillance. A SIC transaction log is used to manually record when devices are added to or removed from the SIC and when inventories are conducted. The "Badge Access" log electronically records who entered the SIC and at what time such entry occurred.

During our review of the SIC transaction log, we found that all entries into the SIC are not manually recorded in the log, and that periodic reconciliations of the log to the monthly "Badge Access" log are not performed. According to the procedures, the SIC transaction log should be used to record the specific storage and removal of devices and to document the timing and performance of periodic inventories. The "Badge Access" log, an automated historical log, records who enters the SIC, and the date and time of entry. During our comparison of the manually recorded entries in the SIC transaction log to the automated entries captured in the "Badge Access" log, we found that fifteen of seventy-five entries captured by the "Badge Access" log did not have corresponding manual entries in the SIC transaction log to detail what actions were performed. Upon further inquiry of IT management, we found that the SIC is also entered by Voice Communications staff to gain access to miscellaneous supplies (such as spare batteries, holsters, and headsets). We were informed that entries for these purposes are not required to be recorded in the SIC transaction log. To ensure that devices stored in or removed from the SIC are properly controlled, we believe that all entries into the SIC should be recorded and that the log should be reconciled to the monthly "Badge Access" log.

In addition to the SIC transaction log and the "Badge Access" log controls, a surveillance camera is mounted outside the SIC door. We found that due to the size and structure of the SIC, the camera is not positioned to capture device-related activities occurring within the SIC. We were told that the IT Division has plans to relocate the SIC to a larger area that will allow for a surveillance camera to capture device-related activities.

During our audit, we also found weaknesses related to the design and format of the monthly "Badge Access" log, which the IT division corrected after we brought these matters to their attention. The "Badge Access" log is sent monthly by the Management Division (Technical Security) to the Voice Communications manager for review. Our review found that the log was not "locked" and that information could be altered or deleted by the reviewer. In addition, the "Badge Access" log listed only the successful entries into the SIC, and did not record unsuccessful attempts. We believe this occurred because information requirements, capabilities, and report format options were not fully discussed between the IT and Management divisions. During the course of our audit, the log was redesigned to capture successful and unsuccessful entries into the SIC and reformatted by Technical Security at the Voice Communications manager's request so that the log could not be altered.

2. We recommend that the Director of IT ensure that individuals with responsibility for storing and removing devices from the SIC do not have full access to the equipment database.

The IT division has established several controls to ensure that BlackBerrys and cell phones are adequately secured, properly tracked, and periodically inventoried. We found, however, that there is no segregation of duties between individuals who have responsibility for storing and removing devices from the SIC, and those with responsibility for recording entries in the equipment database. Three individuals who have custody of BlackBerrys and cell phones also have the ability to edit the equipment database. Segregation of duties is a fundamental, key internal control to provide assurance that errors or irregularities are prevented or detected on a timely basis by management. It requires that no single individual have control over two or more phases of a tracking or inventory process. Such phases include authorization, custody, record-keeping, and reconciliation. Although we did not identify any instances of impropriety, we believe that responsibility for the physical custody and record-keeping of these devices should be segregated to provide enhanced control and accountability.

During our fieldwork, IT staff used the equipment database (an Excel format) for tracking BlackBerrys and cell phones.[1] Specifically, IT staff tracks requests for devices, and records devices that are (1) assigned to users, including loaners; (2) assigned to the SIC as in-stock; and (3) designated for disposal. The equipment database has three types of user access levels: view, read, and full access. View and read access allows users to view information inside the web browser only, download information to a PC, and view off-line or in Excel. Full access allows users to edit information. In addition, the IT division's procedures require the BlackBerry and cell phone managers to conduct a monthly verification of the in-stock devices by comparing each device in the SIC to the equipment database.

The IT staff also uses the Board's *Mobile Data Devices Disposal Form For Mobile Devices* to document disposed devices. This form, which includes procedures for disposal, requires the Board's Voice Communications staff to periodically inventory devices that are designated for disposal, close-out items from the inventory, and present an inventory list along with the devices to the BlackBerry manager. The IT division has a written agreement with the NSA to dispose of devices that are no longer used. The BlackBerry manager is responsible for verifying the

[1] As of February 2, 2009, the IT division transitioned to a web-based database.

inventory, contacting NSA to coordinate the pick-up of devices, and ensuring that a record of disposed items is kept on file.

During our review, we found that three individuals who have access to the locked cabinets located within the SIC also have full access rights to the equipment database. IT management indicated that these individuals were assigned custodial and record-keeping responsibilities because they were the most appropriate individuals to (1) ensure accurate record-keeping, and (2) notify IT management of any compliance issues. One of the keys to ensuring that a system of internal controls is reasonably sufficient for preventing the loss or theft of inventory items is to segregate responsibilities for maintaining custody of inventory from the record-keeping responsibilities.

Although we found control weaknesses in the segregation of duties, our audit did not uncover any unaccounted for devices due to these weaknesses. We counted BlackBerrys and cell phones stored in the SIC and compared our total count (ninety) to the number of devices listed in the IT division's equipment database. We randomly selected a sample of seventeen (19 percent) of ninety in-stock BlackBerrys and cell phones, and traced descriptive information, such as make, model, and serial number to the equipment database. For devices that were disposed of, we compared a sample of eleven (5 percent) of 213 devices disposed of during July 2008, as listed on an inventory sheet attached to the *Mobile Data Devices Disposal Form For Mobile Devices*, to information recorded in the equipment database. No exceptions were noted during any of these tests.

Although we did not note any exceptions, we believe that IT management assumes a number of risks when the responsibilities for custody and record-keeping are not properly segregated. These risks can include the inability to locate, or correctly identify the status of all devices during monthly inventories, and during periodic inventories of devices awaiting disposal.

3. We recommend that the Director of IT: (a) determine what additional procedures are needed to ensure the prompt return of devices that are no longer in use, such as when employees separate from the Board, and (b) coordinate efforts with MGT to receive notification of upcoming employee separations.

The IT Division's BlackBerry and cell phone procedures are not sufficient to ensure that devices are promptly returned to IT. Although we identified only one minor exception, we believe controls should be strengthened to help reduce the risk of unauthorized use, as well as lessen the likelihood of the Board incurring additional charges for BlackBerrys and cell phones.[2]

According to the IT Division's procedures, an authorized division representative should return all unused, replaced, or loaned devices to the Voice Communications staff along with a signed

[2] One employee who was assigned a device separated from Board employment on August 31, 2008. Although the employee turned in the device to the division representative on August 30, 2008, the division representative did not return it to IT until November 10, 2008. IT contacted the vendor and requested that service be discontinued for this device on November 18, 2008. The Board paid monthly recurring charges of $25.34 during October and November.

copy of the sign-out sheet indicating the reason for returning the device. However, the procedures do not specify a timeframe for the return of devices, particularly from a separated employee. As a result, the potential exists for the device to be used for unauthorized purposes and for the Board to incur unnecessary charges.

Communications can be improved between IT management and the divisions regarding the timely return of devices that are no longer in use, and to ensure Voice Communications staff are made aware of employees' separation dates, or notified by the division's authorized IT representative or MGT's human resources staff, of separation dates.

To ensure that devices are returned promptly, and that the Board does not incur any unnecessary charges for devices no longer being used, it is important for all authorized division representatives to communicate any separations to the Voice Communication staff as soon as practical.

Appendix 2

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
DIVISION OF INFORMATION TECHNOLOGY

DATE: March 27, 2009

TO: Ms. Elizabeth A. Coleman

FROM: Maureen Hannan **/signed/**

SUBJECT: Comments on the Office of Inspector General's Audit of BlackBerry and Cell Phone Internal Controls

Thank you for the opportunity to comment on the Office of the Inspector General's (OIG's) audit of the Board's BlackBerry and Cell Phone Internal Controls. We are pleased that the audit did not identify any significant deficiencies and confirmed that the majority of the controls in place are working effectively.

Over the past year, we have enhanced our device provisioning and inventory control processes and internal controls in response to self-assessment reviews and in conjunction with the centralization of Blackberry support in the IT Division. We have been very pleased with the enhancements implemented over the past year and the efficiency and effectiveness of our services. While most of our internal controls are operating effectively, we concur with the report's assessment that opportunities exist to further strengthen several controls. We generally agree with each of the recommendations offered by the audit team and provide a more detailed response below:

OIG Recommendation 1:
We recommend that the Director of IT: (a) ensure that all entries to and transactions made in the Secure Inventory Closet (SIC) are recorded in the SIC transaction log, (b) perform a monthly reconciliation to the "Badge Access" log, and (c) analyze how the SIC security camera can be positioned to closely monitor IT personnel actions regarding devices stored in the SIC.

IT Response to Recommendation 1:
We partially agree with recommendation 1. The IT Division has implemented a number of controls in a layered fashion to prevent the loss of BlackBerry and Cell Phone devices. This includes the use of a badge reader to control access to the secure inventory closet, a camera to record all access to the closet, and the use of locked cabinets within the closet. The primary purpose of the SIC log is to track the transfer of BlackBerry and Cell Phone devices in and out of the secure inventory closet. The SIC log was not intended, however, to track when someone accesses the closet or the movement of low cost consumables. We generally agree with recommendation 1a that all transactions related to the transfer of BlackBerry and Cell Phone devices need to be

recorded in the SIC transaction log. We do not agree, however, that individual accesses to the closet or the movement of low cost consumables needs to be recorded in the SIC transaction log. We do not agree with recommendation 1b that a reconciliation process between the SIC log and the badge access log is needed at this time. We do agree, however, that the SIC door badge access log review process can be further formalized, including maintaining a signed copy of the reviewed log.

Regarding recommendation 1c, the use of a camera was originally intended to serve as a deterrent and to provide a record of who accessed or attempted to access the closet. We do not believe that it would be efficient to attempt to expand the use of cameras to record the actions by authorized staff within the closet. We believe that the current position of the camera is adequate and that the use of the camera achieves the original objective. We will reconsider this recommendation, however, if we determine that the existing controls and separations of duties are not effective in preventing losses.

OIG Recommendation 2:
We recommend that the Director of IT ensure that individuals with responsibility for storing and removing devices from the Secure Inventory Closet do not have full access to the equipment database.

IT Response to Recommendation 2:
We generally agree with recommendation 2. The IT Division currently addresses separation of duties regarding mobile devices by separating the purchase authority from the administrative authority. The IT Financial Management Analysts (ITFMAs) are responsible for purchasing mobile devices while the Voice Communications analysts are responsible for inventory control of those devices. ITFMAs are not permitted access to the SIC and are not able to make changes in the inventory control system (ICE). Voice Communications analysts in turn are not permitted to order mobile devices. Furthermore, as we implement ICE we will continue to look for opportunities to restrict individual access to minimum levels required for an individual's job function. Lastly, we intend to evaluate implementing additional detective controls to help us more quickly identify misuse of devices. This may include having the IT Financial Management unit perform a review of bills for anomalous usage or having them periodically reconcile purchasing records with the device inventory.

OIG Recommendation 3:
We recommend that the Director of IT: (a) determine what additional procedures are needed to ensure the prompt return of devices that are no longer, in use, such as, when employees separate from the Board, and (b) coordinate efforts with MGT to receive notification of upcoming employee separations.

IT Response to Recommendation 3:
We agree with recommendation 3 and intend to develop processes to more effectively identify devices that are not in use. Moreover, we intend to strengthen coordination with Division representatives to ensure that both employees and Division representatives understand their responsibilities regarding the use and administration

of mobile devices and to ensure the timely recovery of devices that are no longer in use. Lastly, we intend to implement new processes to ensure that a mobile device is deactivated on the same day an employee is separated from the Board.