POSTAL REGULATORY COMMISSION

OFFICE OF INSPECTOR GENERAL

FINAL INSPECTION REPORT

POSTAL REGULATORY COMMISSION'S HANDLING OF NONPUBLIC INFORMATION

Report# 10-01-A01
April 30, 2010

Table of Contents

INTRODUCTION 1

BACKGROUND 1

OBJECTIVE, SCOPE AND METHODOLOGY 1

RESULTS 2

STORAGE OF NONPUBLIC INFORMATION 2

ESTABLISHING A "NEED-TO-KNOW" 3

RECEIPT AND TRANSMISSION OF NONPUBLIC INFORMATION 3

TRAINING 4

INCIDENT REPORTING 5

Introduction

Background

This report presents the results of a review by the Postal Regulatory Commission Office of Inspector General (PRC-OIG) of the PRC's procedures, policies and systems for handling information which is protected under 39 USC 504(g). PRC-OIG initiated this review in response to requests on January 26, 2010, from both Chairman Edolphus Towns of the U.S. House Committee on Oversight and Government Reform and Chairman Ruth Goldway of the PRC. PRC-OIG was assisted in this review by the Inspections and Evaluations staff of the Treasury Inspector General for Tax Administration.

In fulfilling its role in regulating and overseeing the United States Postal Service, PRC requires the Postal Service to provide a wide range of information regarding its operations. Most filings with the PRC are a matter of public record, and are posted on the PRC's website (http://www.prc.gov). However, the Postal Accountability and Enhancement Act of 2006 allows the Postal Service to file certain types of information, including commercially sensitive information, under protective conditions.

Under 39 USC 504(g), the PRC is generally prohibited from disclosing this nonpublic information; however, outside parties in matters before the PRC may move for access to nonpublic information only for purposes of participating in the matter.

On April 27, 2010, we held an exit conference with PRC management in which we described this review's findings and presented our recommendations.

Objective, Scope and Methodology

The objective of this review was to evaluate the handling of nonpublic information and material received by the PRC, and to identify whether or not the controls in place are adequate enough to safeguard the information from possible disclosure or unauthorized access.

39 CFR Part 3007, *Treatment of Non-Public Material Filed with the Commission*, establishes criteria for (1) treatment (non-disclosure) and use of nonpublic material,[1] and (2) standardized requests for access to nonpublic material.[2] However, it does not specify any particular requirement for the physical protection of nonpublic information.

There are no government-wide standards for the storage and safeguarding of nonpublic proprietary information and, as a result, federal agencies have discretion over establishing their own standards. The PRC has not established its own detailed physical security standards. Where PRC lacked specific guidelines, we compared the Commission's practices with the standards of the Treasury Security Manual applicable to sensitive but unclassified materials.

[1] 39 CFR Part 3007 § § 3007.23 and 3007.25
[2] 39 CFR Part 3007 § § § 3007.40, 3007.50 and 3007.52

The Treasury manual sets forth criteria for:

- Storing of information and documents;
- Establishing a "need-to-know" before granting access to information;
- Transmitting information via mail, courier, and/or electronic-mail;
- Training personnel to recognize and safeguard information;
- Destroying information; and
- Incident reporting.

We conducted an on-site physical security review of the PRC's office spaces on April 1, 2010, and in order to identify standard operating procedures for handling nonpublic data, we performed follow-up interviews with PRC personnel on April 6, 2010.

This review was conducted in accordance with the Quality Standards for Inspections developed by the President's Council on Integrity and Efficiency and adopted by the Council of Inspectors General on Integrity and Efficiency.

Results

Storage of Nonpublic Information

Per the Treasury Security Manual, storage of *sensitive but unclassified information shall be, **at a minimum**, in a file cabinet, desk drawer, overhead storage bin, credenza, or similar locked compartment. Sensitive but unclassified information may also be stored in a room or area with physical access control measures affording adequate protection and preventing unauthorized access by the public, visitors, or other persons without a need-to-know*."[3]

Except when checked out by PRC staff, all nonpublic information and documentation that the PRC receives is stored in a docket room controlled by an electronic keypad lock with key override. No other secondary security controls prohibit access to the docket room. Access to either the keycode or the override to enter this room is limited to six employees of the PRC's Office of the Secretary and Administration.

Aside from a public reception area, all entrances to the PRC's offices are controlled by doors with either magnetic or keyed locks. A receptionist logs all visits and prevents unescorted visitors from entering PRC offices. In addition, public access to the building is limited during non-business hours.

The PRC exceeds the minimum criteria for sensitive information established by the Treasury Security Manual, and has several satisfactory layers of physical control in place to reasonably prevent the unauthorized access and disclosure of nonpublic information in its possession.

We make no recommendations for improvement in this area.

[3] Department of Treasury Security Manual (TD P 15-71), Chapter III, Section 23.10(a)

Establishing a "Need-to-Know"

Alongside setting physical controls, an important factor of safeguarding nonpublic information is determining an individual's "need-to-know" before allowing access to the information.[4]

The PRC, in accordance with 39 CFR Part 3007, established a procedural guide, *Dockets Protected Materials Procedures*, in order to establish standard operating procedures for the internal and external receipt, dissemination, and return/destruction of nonpublic information and documentation in its possession. Per the procedural guide, "*external reviewers wishing to access Protected Materials must first complete a "certification of compliance with protective conditions," which is attached to the Ruling granting protective conditions. That certification must be filed in person or electronically in the appropriate docket via the PRC's filing online system. Upon receipt of the certification the external reviewers are required to wait until the third day after filing the certification before they may access the materials under those protective conditions. Only the person who signed the certification may obtain the Protected Materials.*"[5] Access to nonpublic materials by PRC staff is similarly limited.

The PRC has also established procedures requiring staff and outside parties to either return or certify destruction of nonpublic materials at the conclusion of the matter for which access was provided.

Nonpublic information received on electronic media such as Compact Discs is also copied onto an internal file server for use by PRC staff, as an alternative to making multiple CDs for all staff working on a particular matter. Access is limited to staff with a need to know by use of file permissions. Per the PRC's IT staff, the file server is separated from the PRC's web server by a firewall, and the Commission's internal servers can only be accessed by either workstations located at the PRC's offices, or by Virtual Private Network using valid user credentials.

We find that the PRC has satisfactory standards in place in order to reasonably limit access to nonpublic information to those with a need to know.

We make no recommendations for improvement in this area.

Receipt and Transmission of Nonpublic Information

The PRC has established specific standards regarding the receipt and transmission of nonpublic information. Per 39 CFR § 3007.10, "*non-public material shall not be filed electronically pursuant to § 3001.9, but shall be filed in sealed envelopes clearly marked 'Confidential. Do Not Post to Web.' The person filing the non-public materials shall submit two copies consisting, where practicable, of two paper hard copies as well as two copies in easily usable electronic form.*" The PRC's *Dockets Protected Materials Procedures* guide establishes further criteria for the internal and external receipt, dissemination, and return/destruction of all nonpublic information and documentation in its possession, specifically:

[4] Department of Treasury Security Manual (TD P 15-71), Chapter III, Section 1.3
[5] Dockets Protected Materials Procedure, *undated*

- Protected materials may not be transmitted by any electronic medium;
- Documents may not be distributed, only checked out by authorized individuals;
- Dockets staff will inform reviewers that copies may not be made of Protected Materials; and
- Protected Materials may be shipped to reviewers outside the Washington, DC area if they have a completed certification (*"certification of compliance with protective conditions"*) on file with the PRC and they pay the applicable postage. Documents must be forwarded via registered mail, return receipt requested.

We find that the PRC has satisfactory standards in place in order to reasonably prevent the unauthorized access and disclosure of the nonpublic information as it is being transmitted or received.

We make no recommendations for improvement in this area.

Training

Per the Treasury Security Manual, "*supervisors and program managers are responsible for employees being trained to recognize and safeguard sensitive but unclassified information supporting their mission, operations and assets. Supervisors and managers shall also ensure an adequate level of education and awareness is maintained by affected employees. Education and awareness shall begin upon initial employee assignment and annually reinforced through mandatory training, staff meetings or other methods/media contributing to an informed workforce.*"[6]

The PRC provides no formal training to educate staff members on adequately safeguarding non-public information in their personal possession. Instead, Management provides an informal oral "overview" of adequate safeguarding and relies on the supervisors to enforce procedure for safeguarding nonpublic information filed with the PRC.

We recommend that the PRC:

1. Develop a more comprehensive, formal training program in order to remind PRC staff of the security requirements for safeguarding nonpublic information.

PRC management committed to implementing this recommendation at our April 27, 2010, exit conference.

[6] Department of Treasury Security Manual (TD P 15-71), Chapter III, Section 23.6

Incident Reporting

Per the Treasury Security Manual, employees or contractors shall notify their supervisor once they "*become aware of the loss, compromise, suspected compromise, or unauthorized disclosure of sensitive but unclassified information no later than the next business day*" and "*notification to appropriate officials shall be made without delay when the disclosure or compromise could result in physical harm to an individual or compromise an unclassified plan or on-going operation*."[7] The security official, or designee, is required to conduct an inquiry to determine the details and prepare a report including the following:

- Whether or not an incident actually occurred. If there was no loss, compromise, or unauthorized disclosure, the security official shall so state;
- The responsible person(s);
- The cause of the incident;
- Actions taken to minimize damage or neutralize the potential for further compromise;
- Recommendations that can be implemented to prevent recurrence of similar incidents;
- The estimated impact; and
- Any action taken or planned, including training, to prevent recurrence.[8]

The PRC does not have a formal procedure for reporting alleged compromises of nonpublic information.

We recommend that the PRC:

2. Develop a method for reporting incidents where a possible compromise of nonpublic information occurs. In developing this plan, the PRC should consider provisions to ensure affected parties are notified, that the cause is determined, and that plans are made to prevent recurrence.

PRC management committed to implementing this recommendation at our April 27, 2010 exit conference.

[7] Department of Treasury Security Manual (TD P 15-71), Chapter III, Section 23.14(a)
[8] Department of Treasury Security Manual (TD P 15-71), Chapter III, Section 23.14(b)