



U.S. Securities and Exchange Commission  
Office of Inspector General  
Office of Audits

# Evaluation of the SEC Encryption Program



REDACTED PUBLIC VERSION



OFFICE OF  
INSPECTOR GENERAL

UNITED STATES  
SECURITIES AND EXCHANGE COMMISSION  
WASHINGTON, D.C. 20549

**MEMORANDUM**

March 26, 2010

**To:** Charles Boucher, Director, Office of Information Technology  
**From:** H. David Kotz, Inspector General, Office of Inspector General (OIG) *ADK*  
**Subject:** *Evaluation of the SEC Encryption Program, Report No. 476*

This memorandum transmits the U.S. Securities and Exchange Commission, OIG's final report detailing the results of our evaluation of the Commission's encryption program.

Based on the written comments that were received and our assessment of the comments, we revised the report accordingly. This report contains three recommendations. The Office of Information Technology (OIT) did not concur with recommendations 1 and 2 and concurred with recommendation 3. The OIT's full comments to this report are included in the appendices.

Within the next 45 days, please provide OIG with a written corrective action plan that is designed to address the recommendations. The corrective action plan should include information such as the responsible official/point of contact, time frames for completing the required actions, milestone dates identifying how you will address the recommendations cited in this report, etc.

Should you have any questions regarding this report, please do not hesitate to contact me. We appreciate the courtesy and cooperation that you and your staff extended to our contractor and auditor.

Attachment

cc: Kayla J. Gillan, Deputy Chief of Staff, Office of the Chairman  
Diego Ruiz, Executive Director, Office of the Executive Director  
Lewis W. Walker, Deputy Director and Chief Technology Officer, Office of Information Technology  
Todd Scharf, Chief Information Security Officer, Office of Information Technology

# Evaluation of the SEC Encryption Program

---

## Executive Summary

In August 2009, the U.S. Securities and Exchange Commission (SEC or Commission), Office of Inspector General (OIG), contracted with C5i Federal, Inc. (C5i) to assist with the completion and coordination of the OIG's input to the Commission's response to Office of Management and Budget (OMB) Memorandum M-09-29. OMB Memorandum M-09-29 provides instructions and a template for meeting the fiscal year 2009 reporting requirements under the Federal Information Security Management Act of 2002 (FISMA), Title III, Pub. L. No. 107-347. C5i's principal tasks included completing the OIG's portion of the template and reporting the results in an executive report. In addition to coordinating the OIG response to OMB, we also examined the Commission's implementation of the encryption program and privacy processes and technologies.

C5i commenced its FISMA work for the OIG in September 2009, when the final FISMA questionnaires were promulgated by OMB. C5i completed the OIG's portion of the FISMA reporting template (Section C) and conducted an evaluation of the SEC's encryption program. This report documents the results of C5i's evaluation of the Commission's encryption program.

Overall, we found that the SEC has a comprehensive encryption program. However, we identified two findings related to mobile devices and portable media that the Office of Information Technology (OIT) should address as follows:

- Mobile devices such as [REDACTED] have not been properly encrypted throughout the SEC headquarters divisions/offices and regional offices.
- OIT has not implemented policy requiring the encryption of portable media for all Commission headquarters divisions/offices and regional offices.

OIT should take steps to ensure the rollout of new [REDACTED] handheld devices with forced encryption is completed on schedule. Until the rollout is complete, the SEC runs the risk of confidential or privacy-protected information being exposed. Further, OIT's current policy for encryption is optional, and two regional offices do not require its personnel to encrypt data that is copied to or contained on portable media. We determined that the current policy should be revised to require all removable media to be encrypted. Allowing this policy to be optional exposes the SEC to potential breaches in Personally Identifying Information (PII) and sensitive data leakage/loss. The best way to protect the Commission's data is to ensure it is encrypted.

**Objective.** The objective of this evaluation was to examine the SEC's implementation of encryption technologies and processes.

**Recommendations.** The OIT should revise its policy and require all portable media to be encrypted. Allowing the policy to be optional exposes the Commission to potential breaches in PII and sensitive data leakage/loss. The only way to protect the data is to encrypt all the data. The protection of data cannot be optional. Therefore, OIT should eliminate the option for offices to determine whether or not they will encrypt portable media such as thumb drives, CD/DVDs, etc. Finally, in the future, OIT should encrypt all PDA/ [REDACTED] [REDACTED] to ensure the protection of any confidential/proprietary/privacy information that may be contained on these devices.

# TABLE OF CONTENTS

<b>Executive Summary</b> .....	ii
<b>Table of Contents</b> .....	iv
<b>Results and Recommendations</b> .....	1
Background .....	1
Results .....	1
Recommendation 1 .....	3
Recommendation 2 .....	4
Recommendation 3 .....	5
<b>Appendices</b>	
Appendix I: Acronyms. ....	6
Appendix II: Scope and Methodology .....	7
Appendix III Criteria.....	9
Appendix IV: List of Recommendations .....	12
Appendix V: Management Comments.....	13
Appendix VI: OIG Response to Management’s Comments .....	14

# Results and Recommendations

---

## Background

Encryption is the process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. The result of the process is encrypted information (referred to as ciphertext). The reverse process of encryption is called decryption; information is decrypted to make the encrypted information readable again (i.e., to make it unencrypted).

Encryption has long been used by the military and governments to facilitate secret communication, but is now commonly used in protecting information in civilian systems and in the private sector. Encryption may be used to protect data "at rest" (e.g., files on computers, portable media<sup>1</sup> and storage devices), as well as data in transit (e.g., e-mail). Encrypting data at rest helps protect it in the event physical security measures fail.

As is true with password strength – the more complex the password, the more difficult to guess – the stronger the encryption, the safer the data.

Forced encryption is the best posture for any organization to take, as it removes the element of human error. All laptops, e-mail, and portable media should be encrypted to ensure that confidential/sensitive data is not compromised, and staff should always ensure that any data that is being copied to portable media be encrypted.

## Results

As part of the fiscal year (FY) 2009 Federal Information Security Management Act (FISMA) evaluation of the SEC, C5i Federal, Inc. (C5i) conducted an evaluation of the U.S. Securities and Exchange Commission (SEC or Commission) encryption program. C5i conducted interviews with Office of Information Technology (OIT) personnel, reviewed policies and procedures, and analyzed documents and documentation pertaining to the products the SEC uses for encryption. To formulate the OIG response to the OMB questionnaire and to support the findings in connection with this evaluation, we reviewed incidents that

---

<sup>1</sup> Portable media is a device that is capable of storing and playing digital media.

occurred within the Commission involving the loss of unencrypted data and unencrypted portable media.

We found the SEC has developed and implemented the policies and procedures surrounding encryption technology and processes. The Draft SEC Encryption policy encompasses the recommendations and best practices of National Institute of Standards and Technology (NIST) 800-53, *Recommended Security Controls for Federal Information Systems*, the Office of Management and Budget (OMB) M-06-16, *Protection of Sensitive Agency Information*, OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, and SEC Regulation (SECR) 23-2a, *Safeguarding Non-Public Information*.

All tools either currently being used or being considered for use by the SEC for the purposes of encryption must be compliant with Federal Information Processing Standards (FIPS) 140-2 and FIPS 200. What follows is a description of the encryption tools currently being used by the SEC.

- [REDACTED] is used for encryption of SEC workstations (desktops and laptops), and is also used for encryption of portable media (USB devices, CDs, etc.). [REDACTED] has enforceable mandatory access control and strong encryption. User credentials and confidential data remain private. It enables the SEC to enforce its security policy, while providing a security solution that is easy for employees to use and does not adversely affect equipment performance. However, the encryption policy for portable media is not followed agency-wide. Additional details about the portable media encryption can be found in the findings section of this document.
- E-mail in transit is encrypted using [REDACTED]. This is an appliance that sits on the edge of the network and inspects all outbound e-mail messages to ensure they comply with SEC policies. It provides full-content scanning of the message body and attachments, and can encrypt, route, block or brand outbound e-mail based on customization by the OIT.
- [REDACTED] – the SEC uses the vendor recommended/provided software for encryption of [REDACTED]. Data in transit between the [REDACTED] and [REDACTED] is encrypted; however, not all of the handheld devices are encrypted. Additional details regarding [REDACTED] encryption can be found in the findings section of this document.

Overall, the SEC has a comprehensive encryption program that uses best in breed technologies and employs industry best practices to safeguard Commissions information. However, there are some areas of concern, which are discussed in detail below.

## ***Encryption of Portable Media***

In September 2008, the OIT Chief Technology Officer sent a memorandum to SEC Division/Office Directors and Regional Directors, outlining the SEC's portable media encryption requirements. The memorandum provided Directors with two options for encryption as follows:

- (1) *Configuration 1*: Automatically encrypts data stored on portable media when the media is connected to SEC owned equipment; or
- (2) *Configuration 2*: Gives SEC personnel the option of storing data on portable media without encrypting the data when the media is connected to SEC-owned equipment, if the user determines the stored data does not include non-public data or Personally Identifiable Information (PII).

Portable media includes, but is not limited to, USB drives, readable and/or writeable CDs, DVDs, and external hard drives. All SEC Directors elected to adopt Configuration 1, except two regional offices that opted to adopt Configuration 2. Configuration 2 essentially relies on the individual's judgment whether or not to encrypt data that is copied to or contained on portable media.

An encryption program cannot be optional in order for it to be effective. Human error is a significant contributor to security incidents and allowing encryption to be optional greatly increases the likelihood that data is compromised. While people are usually very familiar with documents on their computers, we believe that it is not possible for most people to remember for certain the information that is contained in a particular document. We found that the Division/Offices are given the option of whether they would like to encrypt their portable media. In our view, allowing SEC Division/Offices the option to encrypt removable media could result in the loss or exposure of sensitive data and/or PII. For example, in 2009 there were two incidents where information stored on portable media was lost. In Incident 138, an external device was lost that had PII stored on it. In Incident 143, a █████ USB drive was lost. Although █████s are not necessarily considered writable media,<sup>2</sup> because SEC personnel use them to attain remote access to their desktops, the incident report indicates they have a writable partition that is not encrypted.

The only way to protect the data is to encrypt all the data. Allowing the policy to be optional exposes the Commission to potential breaches in PII and sensitive data leakage/loss. Therefore, we recommend that OIT require all portable media be encrypted. Implementing this recommendation will eliminate the option given to offices to select whether or not they want to encrypt portable media, because the protection of data cannot be optional.

---

<sup>2</sup> NIST defines writeable media as information system media that includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm).



**Recommendation 1:**

The Office of Information Technology should revise its policy and require “all” portable media be encrypted.

**Management Comments.** Nonconcur. See Appendix V for management’s full comments.

**OIG Analysis.** OIG disagrees with the opt-out option in the policy that allows division and office heads the ability to determine whether or not to encrypt data on portable media because encryption is a necessary strategy for managing the risk associated with utilizing portable media. We would request that OIT reconsider its position. See Appendix VI for the OIG’s full response to management’s comments.

**Recommendation 2:**

Office of Information Technology should eliminate the option for divisions and offices to determine whether or not they will encrypt portable media such as thumb drives, CD/DVDs, etc.

**Management Comments.** Nonconcur. See Appendix V for management’s full comments.

**OIG Analysis.** As indicated in Recommendation 1, OIG disagrees with the option of allowing division and office heads the ability to determine whether on not to encrypt data on portable media because encryption is a necessary strategy for managing the risk associated with utilizing portable media. We would request that OIT reconsider its position. See Appendix VI for the OIG’s full response to management’s comments.

***Encryption of Handheld Devices*** [REDACTED]

As part of our review of the encryption program, we addressed the encryption of handheld devices. While we found that data in transit between the enterprise server and the [REDACTED] is encrypted, the encryption of [REDACTED] is not enforced.

[REDACTED], as well as other personal digital assistant (PDA) handheld devices, contain a huge amount of information such as e-mail, e-mail addresses, e-mail attachments, and user information. Unencrypted PDA devices can cause a significant security impact if they are lost or stolen, because sensitive and/or confidential information on these devices can be exposed if they are not encrypted, which could bring possible damage to the Commission if non-public information is disclosed to the public.

We found in 2009 the SEC had 15 security incidents involving lost or stolen [REDACTED] that were not encrypted. For example, in June 2009 a security incident occurred when a stolen, unencrypted [REDACTED] was used to send a spoofed e-mail to the SEC Chairman, members of the press, and other media communities.

In July 2009, the SEC began replacing its [REDACTED] with updated devices with forced encryption that cannot be circumvented or disabled. As of October 15, 2009, 638 of 1,192 [REDACTED] had been replaced. OIT informed us that by the end of December 2009, it planned to replace all [REDACTED] [REDACTED] with encryption that cannot be circumvented or disabled. However, we have not received any documentation to confirm whether all [REDACTED] were replaced and have the needed encryption. We recommend that in the future, all devices are encrypted.

**Recommendation 3:**

In the future, the Office of Information Technology should encrypt all PDA/[REDACTED] to ensure the protection of confidential/proprietary/privacy information that may be contained on the devices.

**Management Comments.** Concur. See Appendix V for management's full comments.

**OIG Analysis.** We are pleased that OIT has concurred with this recommendation.

## Acronyms

---

CSIRT	Computer Security Incident Response Team
FIPS	Federal Information Processing Standards
FISMA	Federal Information Systems Management Act
NIST	National Institute of Standards and Technology
OIG	Office of the Inspector General
OIT	Office of Information Technology
OMB	Office of Management and Budget
PII	Personally Identifying Information
SEC or Commission	Securities and Exchange Commission

## Scope and Methodology

---

This evaluation was not conducted in accordance with government auditing standards.

**Scope.** The scope of this evaluation covers fiscal years 2008 through 2009.

**Methodology.** To meet the evaluation objectives to examine the SEC's implementation of encryption technologies and processes, C5i conducted interviews with key personnel, made independent observations, reviewed established policies, and obtained and examined supporting documentation. Interviews with key personnel included systems owners, business line managers, OIT representatives, and OIG personnel. The personnel were interviewed regarding the issues germane to completing the evaluation of the SEC encryption program. Interview discussion areas included:

- SEC encryption policies and procedures;
- Encryption of computers – desktop, laptops, handheld devices such as Blackberries, and portable/removable media; and
- Incidents involving unencrypted portable media.

Support documents SEC officials provided included system artifacts and documentation relating to the various SEC systems and issues that were identified.

**Internal Controls.** We reviewed the existing controls that were considered significant for FISMA and within the context of the encryption program and our objectives.

**Prior Audit Coverage.** We conducted an assessment of the Commission's FISMA program in 2008. The review looked at the FISMA major security areas as well as performed an assessment of two of the Agencies information systems; the Complaints/Tips/Referrals, and the Office of Compliance Inspections and Examinations, Adviser Surveillance Intelligence System applications. The report contained three recommendations and revealed that there were no significant issues with the systems however we found some problems with the overall security program as it related to the Commission completing security control and contingency testing for some systems. We also identified a problem with the Commission's implementation of the requirements for Federal Core Desktop Configuration.

## Criteria

---

**OMB Memorandum M-09-29**, *Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*. This memorandum provides instructions for meeting agency FY 2009 reporting requirements under the Federal Information Security Management Act of 2002, Title III, Pub. L. No. 107-347. It also includes reporting instructions for agency privacy management programs.

**OMB Memorandum M-07-16**, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information (May 22, 2007)*. This memorandum requires agencies to develop and implement a breach notification policy. This is a responsibility shared by officials accountable for administering operational and privacy and security programs, legal counsel, Agencies' Inspectors General and other law enforcement, and public and legislative affairs. It is also a function of applicable laws, such as the Federal Information Security Management Act of 2002, 2 and the Privacy Act of 1974.

**OMB Memorandum M-06-19**, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments (July 12, 2006)*. This memorandum provides updated guidance on the reporting of security incidents involving personally identifiable information and to remind you of existing requirements, and explain new requirements your agency will need to provide addressing security and privacy in your fiscal year 2009 budget submissions for information technology.

**OMB Memorandum M-06-16**, *Protection of Sensitive Agency Information (June 23, 2006)*. This memorandum recommends a number of actions necessary to protect sensitive information.

**OMB Memorandum M-06-15**, *Safeguarding Personally Identifiable Information (May 22, 2006)*. This memorandum reemphasizes agency responsibilities under law and policy to appropriately safeguard sensitive personally identifiable information and to train employees on their responsibilities.

**OMB Memorandum M-03-22**, *Guidance for Implementing Privacy Provisions of the E-Government Act of 2002 (September 30, 2003)*. This memorandum provides information to agencies on implementing the privacy provisions of the E-Government Act of 2002, which was signed by the President on December 17, 2002 and became effective on April 17, 2003.

**NIST SP 800-72, *Guidelines on PDA Forensics*.** This guide provides an in-depth look into PDAs and explaining the technologies involved and their relationship to forensic procedures. It covers three families of devices – Pocket PC, Palm OS, and Linux-based PDAs – and the characteristics of their associated operating system.

**NIST SP 800-83, *Guide to Malware Incident Prevention and Handling*.** This publication provides recommendations for improving an organizations malware incident prevention measures. It also gives extensive recommendations for enhancing an organizations existing incident response capability so that it is better prepared to handle malware incidents, particularly widespread ones. The recommendations address several major forms of malware, including viruses, worms, Trojan horses, malicious mobile code, blended attacks, spyware tracking cookies, and attacker tools such as backdoors and rootkits. The recommendations encompass various transmission mechanisms, including network services (e.g., e-mail, Web browsing, file sharing) and removable media.

**NIST SP 800-86, *Guide to Integrating Forensic Techniques into Incident Response*.** This guide provides detailed information on establishing a forensic capability, including the development of policies and procedures. Its focus is primarily on using forensic techniques to assist with computer security incident response, but much of the material is also applicable to other situations.

**NIST SP 800-101, *Guidelines on Cell Phone Forensics*.** The objective of the guide is twofold: to help organizations evolve appropriate policies and procedures for dealing with cell phones, and to prepare forensic specialists to contend with new circumstances involving cell phones, when they arise.

**CMU/SEI-2003-HB-001, *Organizational Models For Computer Security Incident Response Teams*.** This handbook describes different organizational models for implementing incident handling capabilities, including each model's advantages and disadvantages and the kinds of incident management services that best fit with it. An earlier SEI publication, the Handbook for Computer Security Incident Response Teams (CSIRT) (CMU/SEI-2003-HB-002), provided the baselines for establishing incident response capabilities.

**CMU/SEI-20030TR-001, *State of the Practice of Computer Security Incident Response Teams (CSIRT)*.** This report provides an objective study of the state of the practice of incident response, based on information about how CSIRTs around the world are operating. It covers CSIRT services, projects, processes, structures, and literature, as well as training, legal, and operational issues.

**CMU/SEI-2003-HB-002**, *Handbook for Computer Security Incident Response Teams*. This report proposes an intrusion-aware design model called trustworthy refinement through intrusion-aware design (TRIAD). TRIAD helps information system decision makers formulate and maintain a coherent, justifiable, and affordable survivability strategy that addresses mission-compromising threats for their organization.

**CMU/SEI-2004-TR-015**, *Defining Incident Management Processes for CSIRTs*. This report presents a prototype best practice model for performing incident management processes and functions. It defines the model through five high-level incident management processes: Prepare/Sustain/Improve, Protect Infrastructure, Detect Events, Triage Events, and Respond. Workflow diagrams and descriptions are provided for each of these processes.

**CMU/SEI-2005-HB-001**, *First Responders Guide to Computer Forensics*. This handbook is for technical staff members charged with administering and securing information systems and networks. It targets a critical training gap in the fields of information security, computer forensics, and incident response: performing basic forensic data collection.

**SAND98-8667**, *A Common Language for Computer Security Incidents*. This paper presents the results of a project to develop a common language for computer security incidents. This project results from cooperation between the Security and Networking Research Group at the Sandia National Laboratories, Livermore, CA, and the CERT® Coordination Center at Carnegie Mellon University, Pittsburgh, PA.

## List of Recommendations

---

### **Recommendation 1:**

The Office of Information Technology should revise its policy and require that “all” portable media be encrypted.

### **Recommendation 2:**

Office of Information Technology should eliminate the option for divisions and offices to select whether or not they will encrypt portable media, i.e., thumb drives, CD/DVDs, etc.

### **Recommendation 3:**

In the future, the Office of Information Technology should encrypt all PDA/ [REDACTED] to ensure the protection of confidential/proprietary/privacy information that may be contained on the devices.



## Management Comments

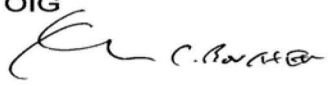
---



### Memorandum

**Date:** March 11, 2010

**To:** David Kotz, Inspector General, OIG  
Jacqueline Wilson, Assistant Inspector General, OIG

**From :** Charles Boucher, Chief Information Officer, OIT 

**Subject:** Management Response to OIG Report 476, *Evaluation of the SEC Encryption Program*

---

Thank you for the opportunity to comment on the recommendations in the draft "Evaluation of the SEC Encryption Program" report. The Office of Information Technology (OIT) takes seriously our obligation to properly safeguard the SEC's information technology assets. The protection of sensitive non-public data and Personally Identifiable Information (PII) is of the utmost importance and the OIT has implemented strong measures to ensure the safekeeping of such data. These measures include:

- Encrypting the hard drive of all SEC laptop computers,
- Encrypting all SEC Blackberry PDA devices,
- Equipping all SEC workstations with encryption software to allow for the encryption of data placed on portable media from an SEC workstation,
- Implementing an Encryption Policy that requires all sensitive non-public or PII data be encrypted,
- Providing annual privacy and security training which covers the responsibilities SEC staff have regarding the protection of sensitive non-public data and PII, and
- Sending out periodic reminders to all SEC staff on their responsibilities regarding safeguarding data.

The encryption policy of the SEC is that all sensitive non-public or PII data must be encrypted. To ensure that all employees can comply with this policy, encryption software has been installed on all SEC workstations. Our policy is consistent with the Office of Management and Budget (OMB) memorandum M-06-16, which recommends that departments and agencies encrypt all data on mobile computer/devices which carry agency data, unless the data is determined to be non-sensitive.

The SEC's encryption policy also provides that each division or office head within the SEC will determine which of two implementation methods to employ for all employees within the division or office. If the division or office chooses a "mandatory" method, then the encryption software will always automatically encrypt all portable media that has data placed on it from any SEC Workstation within the division or office. If the division or office chooses an "optional" method, then the encryption software will instead provide the user with a prompt that 1)

1

reminds the user that all sensitive non-public or PII data must be encrypted when placed on portable media and 2) allows them to determine and select whether the data being placed on the portable media requires encryption. Additionally, when the portable media is encrypted (e.g. if any data requires encryption), then all data on that portable media is encrypted. Therefore, non-sensitive data on the same media as sensitive data would be encrypted.

Our policy reflects the necessity to balance the needs of the business with appropriate safeguarding measures, and recognizes that different divisions and offices within the agency use portable media differently. Allowing SEC leadership to choose which implementation method best addresses the type of data their staff are handling allows for a more efficient and effective business operation. For example, we understand that some courts – to whom our Enforcement staff regularly provide data through portable media – require that when data is provided on portable media that it not be encrypted.

Finally, many other financial regulatory agencies have implemented encryption on portable media in the same manner that the SEC has. We have confirmed that both the Federal Deposit Insurance Corporation (FDIC) and the Federal Reserve Bank (FRB) implement their policies such that their staff determines the nature of the data and encrypts appropriately. These agencies do not require all portable media be encrypted, and do not require any divisions or offices to have mandatory encryption, which the SEC's policy allows for.

**Recommendation 1**

The Office of Information Technology should revise its policy and require "all" portable media is encrypted.

**Recommendation 2:**

Office of Information Technology should eliminate the option for offices to determine whether or not they will encrypt portable media such as thumb drives, CD/DVD, etc.

**Response to Recommendation 1 and Recommendation 2:**

For the reasons explained above, OIT does not concur with these recommendations.

**Recommendation 3:**

In the future the Office of Information Technology should encrypt all PDA/Blackberry devices to ensure the protection of confidential/proprietary/privacy information that may be contained on the devices.

**Response to Recommendation 3:**

The Office of Information Technology concurs with this recommendation. OIT encrypts all Blackberry devices.

## OIG Response to Management's Comments

---

OIT did not concur with recommendations 1 and 2, but concurred with recommendation 3. We are pleased that OIT concurred with recommendation 3, and provide our response to OIT's comments regarding recommendations 1 and 2 as follows.

The CIO states in the management comments that OIT's policy to allow a division or office to opt-out of the automatic encryption of all portable media that has data placed on it from an SEC workstation "reflects the necessity to balance the needs of the business with appropriate safeguarding measures." While the OIG understands the concern to balance the business needs of the different offices and divisions within the SEC, as we discussed in the report, an encryption program cannot be optional if it wishes to be effective. Human error is a significant contributor to security incidents and allowing encryption to be optional greatly increases the likelihood that data is compromised. In our view, the only way to protect the data is to encrypt all of it. Allowing the policy to be optional exposes the Commission to potential breaches in PII and sensitive data leakage/loss.<sup>3</sup>

Accordingly, we disagree with OIT's comments and would request that OIT reconsider its position and agree to eliminate the option for offices to determine whether or not they will encrypt portable media and in the future encrypt all PDA/blackberry devices.

---

<sup>3</sup> The fact that other agencies may also allow potential exposure to breaches in PII by not requiring that all portable media be encrypted is not a reason that the SEC should allow itself to be vulnerable.

# Audit Requests and Ideas

---

The Office of Inspector General welcomes your input. If you would like to request an audit in the future or have an audit idea, please contact us at:

U.S. Securities and Exchange Commission  
Office of Inspector General  
Attn: Assistant Inspector General, Audits (Audit Request/Idea)  
100 F Street, N.E.  
Washington D.C. 20549-2736

Tel. #: 202-551-6061  
Fax #: 202-772-9265  
E-mail: [oig@sec.gov](mailto:oig@sec.gov)

## Hotline

To report fraud, waste, abuse, and mismanagement at SEC,  
contact the Office of Inspector General at:

Phone: 877.442.0854

Web-Based Hotline Complaint Form:  
[www.reportlineweb.com/sec\\_oig](http://www.reportlineweb.com/sec_oig)