U.S. Securities and Exchange Commission

Office of Inspector General

Office of Audits

Assessment of the SEC's Privacy Program

September 29, 2010
Report No. 485

Assessment and Review Conducted by C5i

OFFICE OF
INSPECTOR GENERAL

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

MEMORANDUM

September 29, 2010

To: Jeffery Heslop, Chief Operating Officer (COO), and Acting Chief Information Officer (CIO), Office of Information Technology (OIT)
Rosalind Tyson, Regional Director, Los Angeles Regional Office
Sharon Sheehan, Associate Executive Director, Office of Administrative Services

From: H. David Kotz, Inspector General, Office of Inspector General

Subject: *Assessment of the SEC's Privacy Program*, Report No. 485

This memorandum transmits the U.S. Securities and Exchange Commission Office of Inspector General's (OIG) final report detailing the results of our assessment of the SEC's Privacy Program. This review was conducted as part of our continuous effort to assess management of the Commission's programs and operations, and as a part of our annual audit plan.

The final report contains 20 recommendations, which if implemented should improve the Commission's security posture for protecting Personally Identifiable Information. The COO/Acting CIO fully concurred with 12 of the 15 recommendations addressed to its office, partially concurred with 1 recommendation, and did not concur with 2 recommendations. The LARO Regional Director and the Associate Executive Director, Office of Administrative Services concurred with all the recommendations addressed to its office. The written responses OIG received to the draft report are included in the appendices.

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

Should you have any questions regarding this report, please do not hesitate to contact me or Kelli Brown-Barnes at x-15674. We appreciate the courtesy and cooperation that you and your staff extended to our staff and contractors.

Attachment

cc:

Kayla J. Gillan, Deputy Chief of Staff, Office of the Chairman
Diego Ruiz, Executive Director, Office of the Executive Director
Rabia Cebeci, Senior Special Counsel, Los Angeles Regional Office
Todd Scharf, Chief Information Security Officer-Information Security,
  Office of Information Technology
Barbara Stance, Chief Privacy Officer, Office of Information Technology

Assessment of the SEC Privacy Program

Executive Summary

Background. The U.S. Securities and Exchange Commission (SEC or Commission) Office of Inspector General (OIG) contracted the services of C5i Federal, Inc. (C5i) to perform an assessment of the SEC's privacy policies and procedures and the proper handling of Personally Identifiable Information (PII) in its headquarters (Station Place), Operations Center (OPC), and regional offices. The privacy program assessment was conducted in two phases. First, in June 2010, C5i assessed the SEC's Los Angeles Regional Office's (LARO) handling of PII data through a physical inspection, conducting interviews, and Network Vulnerability Assessment (NVA)[1] of the SEC's computer network. Second, in July 2010, C5i performed an assessment of the SEC's systems located in Station Place and the Operations Center, to evaluate their network security postures, and conducted a re-scan of seven of the eight servers previously assessed in LARO. In addition, C5i conducted an application vulnerability assessment on the SEC's "HUB"[2] application to determine how the Commission retained and secured its PII data within this application. Additionally, C5i reviewed the status of a prior privacy assessment recommendation that was still open.

Objectives. The primary objectives of the review were to:

- Evaluate the adequacy of the SEC's Privacy Office's policies and procedures, as well as its interaction and involvement with the Commission offices and divisions to ensure SEC employees' privacy;
- Perform an in-depth analysis of the privacy requirements and identify the SEC processes and procedures that are used to conduct privacy reviews;
- Assess whether the privacy office responds to privacy issues in accordance with governing SEC, National Institute of Standards and Technology (NIST), Office of Management and Budget (OMB) and other government guidance and regulations to determine whether improvements are needed;
- Determine if the SEC has developed and implemented technical, managerial, or operational privacy-related controls to effectively mitigate known risks that are inherent to the Privacy Act's system of records;
- Determine if the SEC has established procedures and automated mechanisms to verify privacy control effectiveness;

[1] A NVA is the process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities found on a network. It is performed using commercial-off-the-shelf tools used by assessors industry-wide.

[2] The HUB application is used by the SEC's Division of Enforcement for case activity tracking and was selected to be assessed based on the sensitive data contained within the application and the maturity of the application.

- Review governing Commission policy, guidance, and follow up on prior recommendations;
- Perform an assessment of an SEC regional office for proper handling of PII and adherence to SEC privacy policies and procedures;
- Perform a NVA at the LARO, Station Place, and OPC to evaluate the security posture of the SEC network in protecting PII data; and
- Perform an application assessment to ensure PII data is protected.

Results. Overall, the assessments conducted identified significant concerns with the manner in which the SEC handles PII data. Improper handling could result in a significant data breach and the possible exploitation of PII or sensitive data. Further, the SEC's ability to complete its mission could be jeopardized as a result of lack of trust by external parties to share PII data.

Specifically, our review identified high level vulnerabilities affecting SEC computer systems in the assessments of LARO as well as headquarters and the OPC that are vulnerable to exploitation and infiltration. We further found that while software vendors provide patches and updates to remediate security vulnerabilities identified in their software, the SEC has not applied these critical patches and updates, in some cases, going back as far as 2006. We also found that the SEC has not been regularly reviewing the application of patches on a consistent basis, which leaves the Commission vulnerable to attack.

Additionally, our assessments yielded additional areas of concerns. We found that:

- Office of Information Technology's (OIT) categorization of network vulnerabilities does not accurately reflect the actual risk to the environment;
- Base images deployed on laptops are not compliant with Federal Desktop Core Configuration (FDCC) requirements and all deviations are not disclosed as required by OMB;
- SEC laptops can connect to the SEC network via a local area network (LAN) port while simultaneously connected to an external wireless network, exposing the SEC network to potential compromise by a malicious attacker;
- The existence of design flaws in the development of the HUB application could potentially result in a compromise of data;
- PII at LARO is contained on shared drives without access controls, allowing all LARO employees unfettered access to documents and data that may be misused;
- LARO employees violated the *SEC Rules of the Road* by sending documents containing PII data to personal email accounts and by using portable media that was not encrypted. In addition, LARO employees did not adequately secure unencrypted portable media.

Further, through interviews with OIT staff and a physical assessment of office space and storage areas at headquarters' offices, the OPC and LARO we found that:

- Documents containing PII data were casually left on work tables, fax machines, and desks.
- File rooms, file cabinets, and offices containing very sensitive information were unsecured.
- The SEC has no final policies or procedures for the destruction of portable media storage devices, and secured storage bins were not accessible to all Commission staff.

These findings indicate a significant risk to the SEC network and the security of the data/documents handled by the agency.

Although, OIT has already begun taking steps to mitigate and remediate risks by progressively applying certain critical patches, significant additional work must be done.

Summary of Recommendations. We provided the SEC with 20 specific and concrete recommendations to address the vulnerabilities identified in the review. Specifically, we recommend that OIT and the Chief Operating Officer:

(1) Apply patches and updates to the Commission's networks, workstations and laptops on a timely basis;

(2) Implement procedures to regularly review whether a newly-released patch should or should not be applied to the environment;

(3) Evaluate OIT's risk assessment process for scoring risk;

(4) Define a standard recognized character set for every response containing Hypertext Markup Language content;

(5) Ensure Federal Desktop Core Configuration compliance for all base images deployed on desktops and laptops;

(6) Submit a complete list of common security standard deviations to the National Institute of Standards and Technology per the Office of Management and Budget's requirements;

(7) Ensure that wireless cards installed on laptops are turned off when connected to the SEC's local area network;

(8) Implement an agency-wide policy regarding shared folder structure and access rights based on "least privilege;"

(9) Ensure personal storage tab files be saved to a protected folder;

(10) Implement a policy that all portable media must be fully secured when not in use;

(11) Appoint a privacy point of contact at each regional office;

(12) Implement a clean desk policy or require all offices be locked when not occupied;

(13) Conduct additional training to ensure that staff understands the handling of PII and sensitive data and their responsibilities in protecting SEC information;

(14) Approve and implement operating procedures for hard drive wiping and media destruction;

(15) Provide training on the handling, disposal, and storage of portable media storage devices.

In addition, we recommend that the LARO:

(1) Reemphasize the *SEC Rules of the Road* to LARO staff;

(2) Enforce its encryption policy to protect sensitive data received by the Commission;

(3) Ensure that all file rooms and file cabinets at LARO are secured; and

(4) Ensure that boxes of files in hallways are moved to secured areas.

Further, we recommend that the Office of Administrative Services provide secured bins for disposal of portable media storage devices.

TABLE OF CONTENTS

Appendices

Tables

Figures

Background and Objectives

Background

Overview. The U.S. Securities and Exchange Commission (SEC or Commission) Office of Inspector General (OIG) contracted the services of C5i Federal, Inc (C5i) to perform an expert assessment of the SEC's Privacy policies and procedures, and the proper handling of Personally Identifiable Information (PII) in its headquarters and regional offices. The SEC has headquarters offices located in Washington, D.C., commonly referred to as Station Place (SP), and in Alexandria, Virginia, at an Operations Center (OPC). The SEC also maintains 11 regional offices throughout the continental United States.

C5i's expert assessment was conducted in two phases. First, in June 2010, C5i assessed the SEC's Los Angeles Regional Office's (LARO) handling of PII data through a physical inspection and interviews, and conducted a Network Vulnerability Assessment (NVA)[3] of the SEC's computer network. LARO was selected as the regional office to be evaluated based on its size and the fact that it was last assessed by the Office of Information Technology (OIT) in 2008 and was not due to be evaluated again until 2011.

Second, in July 2010, C5i performed an NVA of SP and OPC to evaluate their respective network security postures, and conducted a re-scan of seven of the eight servers previously assessed in LARO. The purpose of the re-scan was to determine if vulnerabilities identified during the June 2010 scans were remediated by OIT. In addition, C5i conducted an application vulnerability assessment on the SEC's "HUB"[4] application to determine how the Commission retained and secured its PII data within this application.

At the onset of the assessment, C5i met with the SEC's Chief Information Officer (CIO), and Privacy Officer to establish technical Rules of Engagement (ROE) due to the requirements needed to perform the technical assessments (NVA and Application Assessment). The technical ROE set forth the limitations, requirements, and detailed specific data, information (i.e., network switches, passwords, accounts, Internet access, private rooms, etc.), and access rights and privileges C5i would need to carry-out assessments of the SEC's PII. In

[3] A Network Vulnerability Assessment is the process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities found on a network. It is performed using commercial off-the-shelf tools used by assessors industry-wide.

[4] The HUB application is used by the SEC's Division of Enforcement for case activity tracking and was selected to be assessed based on the sensitive data contained within the application and the maturity of the application.

addition, the technical ROE identified the systems that were to be assessed and was approved and signed by all respective parties on June 23, 2010.[5]

One of the key elements of the technical ROE that was discussed extensively by all parties was the OIG requirements pertaining to the appropriate level of credentials (user id and passwords) necessary to perform the assessments. The OIG informed OIT that a temporary test Domain Administrative account[6] was required to conduct an effective review of SEC security posture as it related to privacy. After the OIT Assistant Director of Infrastructure Engineering expressed concern about the level of access agreed to in the ROE, the OIG agreed that it would use an account with limited privileges (utilized previously by the General Accountability Office in a previous review), however, a separate Test Domain Administrator account would be created as a fall back, in the event that the account assigned to the OIG experienced problems or was unable to satisfy the requirements of the assessments.

Prior OIG Work Conducted in 2009/2010. The OIG conducted a prior Privacy assessment in 2009/2010,[7] which resulted in one recommendation that remains open. The report found that OIT had not finalized all its outstanding draft privacy related policies and procedures nor had they been fully implemented throughout the Commission.

Overview of Technical Assessments at LARO. C5i conducted its on-site assessment at LARO from June 25 to July 2, 2010. LARO is located in downtown Los Angeles and it consists of 162 SEC employees and contractors and five interns. LARO has offices on the [redacted] and the [redacted] of a public, 25-story building and requires an SEC access card to stop on the [redacted]. The [redacted] do not require card access for the elevators as they are shared with other tenants, but card access is required to enter the SEC space and conference rooms. The technical and physical assessments at LARO were conducted over an eight-day period, beginning on the morning of June 25, 2010. The assessments consisted of performing an NVA of the servers, workstations/laptops deployed to LARO staff, recently imaged laptops not yet deployed to personnel and a physical assessment of the LARO facilities. The purpose of this work was to verify the security of the network and workstations/laptops, the protection and proper handling of electronic PII data, and a physical inspection of the facilities for the proper handling of hard copy PII data.

[5] The respective parties were: the former Chief Information Officer; the Inspector General; the Chief Information Security Officer; and the president and CEO of C5i Federal, Inc.

[6] A domain administrator account is an account that has power over all computers, including domain controllers, within the domain. This means that this user account can logon to any computer, access any file, and install any application by default.

[7] Report No. 475, *Evaluation of the SEC Privacy Program*, issued March 26, 2010.

In order to conduct an effective assessment, in accordance with the technical ROE, the assessment of LARO was unannounced. Only the LARO Director, the Associate Director and physical security personnel were informed about C5i's visit. The purpose of conducting this "surprise" assessment was to ensure that information was not updated or modified prior to the work.

C5i began its technical assessment at LARO on June 25, 2010, at 4:00 p.m., pacific daylight time (PDT). C5i's network assessments were performed on the LARO servers, a sampling of 66 deployed workstations/laptops, and two newly imaged laptops that had not yet been deployed to the field. The scans yielded a significant number of high level vulnerabilities,[8] which were vetted through a manual verification process to ensure the accuracy of the scan data and to eliminate false positives. Once the vetting was completed, C5i and the OIG immediately notified OIT, in accordance with the technical ROE. Numerous calls were held with staff from OIT and the OIG on June 27, 2010 and the assessment findings were presented and discussed during a June 28, 2010 teleconference with the Chief Information Security Officer (CISO), the Associate Director of Infrastructure Engineering, and the OIG.

In addition to the network vulnerabilities discovered, C5i's assessment identified emails containing PII sent to employees' personal email addresses, shared folders lacking access controls, and instances in which the base image for laptops was not Federal Desktop Core Configuration (FDCC) compliant. These are detailed in the findings section of this report.

Overview of Physical Assessment Conducted at LARO. As part of the evaluation of LARO, C5i also conducted a physical evaluation of the SEC space to verify the proper handling/storage of PII and compliance with SEC policies and procedures. The staff at LARO was very accommodating and cooperative, providing a secure work area, full access to the space both on and off hours, and necessary access to storage areas. C5i physically inspected all areas of the SEC space, file rooms located in the space, as well as storage space located in [redacted] [redacted] [redacted] [redacted]. The physical assessment was conducted from June 25 to June 26, 2010. During the physical evaluation, C5i found evidence of PII data being handled incorrectly – unsecured documents and files, and unencrypted media. These findings are detailed in the findings section of this report.

Overview of Assessment Conducted at SP, OPC, Re-scan of LARO, and HUB application. After undertaking an analysis of current SEC applications that stored PII data, the OIG chose to assess the Division of Enforcement's (Enforcement) HUB system to assess. The HUB system is a case management and tracking system that has been in place since 2008, and is the primary

[8] We note that OIT disagrees with the OIG's determination that the vulnerabilities should be considered at a "high level."

system used by Enforcement's staff attorneys, accountants, and branch chiefs to track and manage ongoing matters.

Since the HUB application could not be taken offline to be assessed, in light of its need to be continuously available to Commission staff, OIT provided an exact duplicate of the data and allowed the assessment to be conducted in the test/staging environment. Credentials were provided for the access required per the technical ROE and the test was conducted July 23, 2010 through July 25, 2010.

In addition to the HUB application security assessment, C5i conducted a NVA on the SP and OPC networks, as well as servers and workstations at both locations. A re-scan of the LARO network was also performed. This re-scan yielded similar results to the June 2010 scans, although there were fewer high level vulnerabilities, demonstrating that some patching/remediation had taken place.

Detailed findings from the NVA for SP and OPC, the re-scans for LARO, and the onsite application security assessment (OASA) of HUB are located in the findings section of this report.

Overview of Assessment Privacy Policies and Procedures. In addition to technical assessments, C5i conducted interviews with Privacy Office staff, and reviewed privacy policies and procedures documents, system of records notices (SORNs) and incidents involving loss of PII. These interviews and reviews were performed throughout the assessment period, April to August 2010.

Objectives

The OIG contracted with C5i to conduct an assessment of SEC's privacy policies and procedures and handling of PII in accordance with the following specific objectives:

- Evaluate the adequacy of the SEC's Privacy Office's policies and procedures, as well as its interaction and involvement with the Commission offices and divisions to ensure SEC employee's privacy.

- Perform an in-depth analysis of the privacy requirements and identify the SEC processes and procedures that are used to conduct privacy reviews.

- Assess whether the Privacy Office responds to privacy issues in accordance with governing SEC, National Institute of Standards & Technology (NIST), Office of Management and Budget (OMB) and other government guidance and regulations to determine whether improvements are needed.

- Determine if the SEC has developed and implemented technical, managerial, or operational privacy-related controls to effectively mitigate known risks that are inherent to the Privacy Act's system of records.

- Determine if the SEC has established procedures and automated mechanisms to verify privacy control effectiveness.

- Review governing Commission policy and guidance, and follow up on prior OIG recommendations.

- Perform an assessment of an SEC regional office for proper handling of Personally Identifiable Information and adherence to SEC privacy policies and procedures.

- Perform a Network Vulnerability Assessment at the Los Angeles Regional Office, Station Place, and the Operations Center to evaluate the security posture of the SEC network in protecting PII data.

- Perform an application assessment to ensure PII data is protected.

Findings and Recommendations

Finding 1: The SEC Network Vulnerability Assessment Results Showed Numerous Missing Vendor Issued Security Patches and Updates

> Critical patches and updates released by software vendors for vulnerabilities known to be exploitable have not been applied to the SEC network, which could jeopardize the confidentiality, integrity, and availability of PII or sensitive data. As a result, the network is vulnerable to compromise by known threats.

During the NVA of LARO, in June 2010, and SP and OPC, in July 2010, C5i found that critical patches issued by software vendors to correct known vulnerabilities had not been applied in a timely and effective manner. Applying these critical patches would remediate or mitigate the likelihood of exploitation of a vulnerability. Consequently, C5i found the SEC's network to be vulnerable to well-known weaknesses identified by vendors, and that it could be compromised by a malicious user, resulting in a significant data breach and possible exploitation of PII or sensitive data.

The selection of C5i's assessment locations was based on the current OIT schedule of field offices and population of staff. The LARO location provided the OIG with a view into the security posture of a field office's network that had not been assessed by OIT in the past two years, and was not scheduled for an OIT assessment until 2011. SP and OPC offices were selected due to the large amount of network servers located at these facilities. During the assessments, C5i used a number of commercial off-the-shelf and open source vulnerability assessment tools,[9] and conducted manual checks to provide adequate cross-checking and the capability to verify results and reduce or eliminate the number of false positives. These tools classify vulnerabilities as high, medium and low, based on their potential impact, severity, and potential for exploitability.

The technical ROE provided that the OIG was to receive the following network credentials to provide sufficient access to conduct appropriate vulnerability scans of the network:

[9] The commercial off-the-shelf vulnerability assessment tools used during C5i's assessment included: [redacted]

- Three separate Microsoft Server Local Administrator accounts.
- Three separate Microsoft Domain Administrator accounts.
- Three separate workstation and laptop Administrator accounts.
- Three UNIX user and root level accounts, if applicable.

At the time of the assessment, the SEC network was comprised of 749 servers[10] and 5,268 workstation/laptops. C5i's network vulnerability assessment sample included eight network servers, 66 deployed workstations/laptops, and to two newly-imaged laptops located at LARO,[11] and 59 network servers and three workstations located in OPC and SP. C5i also conducted a re-scan of seven servers in LARO to identify any patching updates since the scans in June. C5i's assessment did not include routers, network switches, firewalls, intrusion detection or prevention systems, proxy servers, anti-virus, and related infrastructure security systems.

Vendors Provide Patches and Updates. Software vendors provide patches and updates to remediate security vulnerabilities identified in their software. These patches and updates are made available through the software vendors' website as they are released. It is the SEC's responsibility to download, test, and deploy these patches to their network to reduce the risk associated with the vulnerability. *NIST 800-53*, *Recommended Security Controls for Federal Information Systems and Organization* provides guidance to government organizations on flaw remediation, e.g., patching and updates. The NIST guidance provides that an organization should identify, report, and correct information system flaws; test software updates related to flaw remediation for effectiveness and potential side effects on organizational information systems before installation; and incorporate flaw remediation into the organizational configuration management process.[12]

LARO Network Vulnerability Assessment. Scanning of the LARO network began on June 25, 2010 at approximately 6:00 p.m. PDT and continued, non-stop, through the early morning hours of June 28, 2010. Verification of the accuracy, testing, and review of the findings to eliminate or reduce the number of false positives identified during the assessment of the LARO network continued through July 2, 2010. The results are described in Table 1 below, and illustrate the SEC's high level vulnerabilities identified during the assessment at LARO. C5i used a combination of commercial off-the-shelf and open source vulnerability assessment tools during the assessment and categorization by software vendors

[10] A server is a computer host on a network that runs an operating system, application software, database, etc.

[11] These workstations/laptops had not been deployed by OIT, but did receive the current SEC OIT approved image prior to conducting the assessment. In addition, these workstations/laptops were connected to the SEC network to ensure that the latest patches and security updates from OIT were applied.

[12] The National Institute of Standards and Technology's (NIST), Special Publication 800-53, Rev 3, *Recommended Security Controls for Federal Information Systems and Organization*, August 2009, page F-124.

to determine the vulnerability levels for each type of device. The assessment identified 175 high-level vulnerabilities affecting eight servers, 67 high-level vulnerabilities affecting two new workstations/laptops, and 1,613 high-level vulnerabilities affecting 66 deployed workstations/laptops, as Table 1 below indicates.

Table 1: Summary of LARO Network Vulnerability Assessment Scan Results

Vulnerability Level	Number of Vulnerabilities by Device		
	Servers - 8	New Workstations and Laptops - 2	Deployed Workstations and Laptops - 66
High	175	67	1,613
Medium	66	11	287
Low	824	163	4,679

Source: Generated by C5i

The significant number of high-level vulnerabilities increases the likelihood that the SEC's LARO network is vulnerable to exploitation and infiltration by a person with ill-intent.

Per the ROE signed by OIT, OIG, and C5i, on June 27, 2010, C5i immediately notified OIT of the high vulnerabilities found during the assessment. The assessment findings were presented and discussed during a teleconference on June 28, 2010 with the CISO, Associate Director of Infrastructure Engineering, and the OIG. OIT did not take immediate emergency action when presented with this evidence of the significant number of high-level vulnerabilities at LARO. According to OIT, immediate emergency action was not taken because the vulnerabilities did not present imminent danger and patches were subsequently deployed according to prioritization.

SP and OPC Network Vulnerability Assessment, including a re-scan of LARO. On July 24, 2010, C5i conducted a NVA of the SEC's network servers, workstations, and laptops at SP, OPC, and a re-scan of LARO servers. Altogether, C5i assessed a total of 59 network servers at SP and OPC,[13] re-scanned 7 LARO servers,[14] and assessed images from 3 SEC machines (2 workstations and one laptop). Upon conclusion of the assessment, as with the assessment at LARO, C5i verified the accuracy of the test results to eliminate and/or reduce any false positives identified during the assessment of SP, OPC, and re-scan results of LARO.

[13] Of the 59 servers assessed at SP and OPC, 46 were from the SP and 13 were from the OPC.

[14] Due to time constraints, seven servers were re-scanned. The re-scan was performed to determine if patches had been applied and the vulnerabilities remediated in approximately 30 days since the June 2010 assessment.

Table 2, shown below, illustrates the high-level vulnerabilities we identified during our assessment of SP, OPC, and the re-scan of the LARO servers. C5i used the same commercial off-the-shelf and open source vulnerability assessment tools and categorization processes as it did during the review of LARO in June 2010. The assessment of SP, OPC, and re-scan of LARO identified 1,020 high-level vulnerabilities affecting the 59 servers, 30 high-level vulnerabilities affecting three new workstations/laptops, and 109 high-level vulnerabilities affecting the seven re-scanned LARO servers.

Table 2: Summary of SP, OPC, and Re-Scan of LARO Network Vulnerability Assessment Scan Results

Vulnerability level	Number of Vulnerabilities by Device		
	Servers - 59	Deployed Workstations and Laptops - 3	Re-Scanned LARO Servers - 7
High	1,020	30	109
Medium	356	9	45
Low	5,204	239	722

Source: Generated by C5i

Based on the assessment of SP, OPC, and re-scan of LARO, C5i identified a signficant number of high level vulnerabilities affecting servers, workstations, and laptops. The significant number of high-level vulnerabilities increases the likelihood that the SEC's SP, OPC, and LARO networks are vulnerable to exploitation and infiltration by a person with ill-intent. C5i confirmed during the re-scan of the LARO servers that OIT took action to begin implementing patches and updates to the LARO servers to remediate or mitigate the risk of exposure; however, there were still a significant number of high-level findings on each server. Therefore, the SEC's SP, OPC, and LARO networks remain highly vulnerable to exploits by an individual with ill-intent.

Critical Updates and Patches Need to Be Applied. Based on the network vulnerability assessment of components of the SEC's enterprise network, C5i determined that critical patches and vendor supplied updates had not been applied going back as far back as 2006, resulting in years of potential vulnerabilities that could have been exploited. The following patches have been made available by software vendors:

Software Vendor	**Year Patches Made Available**
Sun Vulnerabilities	[redacted]
Microsoft Vulnerabilities	[redacted]
HP Vulnerabilities	[redacted]
Realplayer	[redacted]
Shockwave	[redacted]

As indicated above, C5i's review found that OIT has not applied patches and updates released by software vendors to the SEC network on a consistent basis. In addition, C5i determined that some system patches were several versions behind the current patch level that is recommended by the software vendor to adequately remediate known software vulnerabilities. It should be noted that major software vendors, such as Microsoft provide patches on a minimum of a monthly basis. Patches are also issued by the vendors on an ad-hoc basis to address a vulnerability that has severely impacted systems, e.g., in August 2010 a vulnerability was identified in Adobe Acrobat Reader that would allow remote attackers to execute arbitrary code on a user's computer. In addition, the longer the delay between the time a known vulnerability has been reported to the vendor and the time the patch is actually applied, the greater the chance that hackers have found a means of exploiting the vulnerability. Further, other agencies have established processes and procedures to regularly review whether a newly-released patch applies to the agency's needs and requirements. C5i found in its assessment that the OIT has not been regularly reviewing the application of patches on a consistent basis which leaves them vulnerable to attack.

As a result of not implementing patches and vendor-issued security updates in a timely manner, the SEC's systems were found to be highly vulnerable to compromise, infiltration, and exfiltration of PII and sensitive data. Further, lack of a proactive patch management process increases the time and effort spent by staff in responding after an exploitation has occurred. In the event that the SEC is exploited and data is compromised, the Commission's reputation and ability to have the securities industry voluntarily provide data will become more challenging, which could impact the SEC's ability to meet its mission to protect investors, maintain fair, orderly, and efficient markets, and facilitate capital formation. The OIT should review its systems, procedures, and apply patches, as appropriate, on a recurring, timely basis to the entire SEC enterprise network to ensure adequate security of its systems.

Prior OIG Reviews. The SEC's OIG performed independent assessments of the confidentiality, integrity and availability of SEC data at OPC and its Northeast and Southeast regional offices from 2004 to 2005, and issued two reports.[15] During

[15] Report No. 392, *Northeast Regional Office (NERO) Information Management*, issued February 14, 2005 and Report No. 400, *Southeast Regional Office (SERO) Information Technology Management*, issued March 24, 2005.

our present assessment, we compared the results of those Network Vulnerability Assessments with the current 2010 results of OPC, SP, and LARO. Our findings revealed that the security posture of the SEC network and systems was significantly higher during the 2004 to 2005 timeframe. Based on this analysis, C5i concluded that there has been a significant degradation in the SEC's security posture over the last five years and a significant amount of procedural, policy, and management changes in OIT may have resulted in this degradation. [redacted]

As indicated previously, since the OIG's notification to OIT regarding the lack of controls in applying patches and software vendor updates, the OIT has begun implementing patches and updates; however, we determined during the assessment of SP, OPC, and re-scans of LARO that many critical patches and vendor supplied updates have not, as of yet, been applied. As a result, the SEC network, workstations, and laptops remain highly vulnerable to attack by a malicious user and could result in a data breach. Updating the SEC servers, workstations, and laptops with the current available patches will significantly reduce the number of vulnerabilities to the SEC network and lessen the likelihood that the SEC's network will be compromised and PII or sensitive data will be exploited.

Recommendation 1:

The Office of Information Technology should apply patches and updates to the Commission's networks, workstations, and laptops on a timely basis. All future patches should be applied within [redacted] of vendor release, with emergency patches being applied on an ad-hoc basis to protect the agency's systems and data.

Management Comments. The COO/Acting CIO concurred with this recommendation. See Appendix V for management's full comments.

OIG Analysis. We are pleased that the COO/Acting CIO concurred with this recommendation.

Recommendation 2:

The Office of Information Technology should implement formal processes and procedures to regularly review whether a newly-released patch should or should not be applied to the environment.

Management Comments. The COO/Acting CIO concurred with this recommendation. See Appendix V for management's full comments.

OIG Analysis. We are pleased that the COO/Acting CIO concurred with this recommendation.

Finding 2: SEC OIT's Questionable Categorization of Network Vulnerabilities May Impact the Certification and Accreditation (C&A) Process

The SEC's questionable categorization of vulnerabilities may impact its internal C&A process.

Systems, such as the HUB application, are given a risk impact categorization based on the Federal Information Process Publication 199 (FIPS 199) *Standards for Security Categorization of Federal Information and Information Systems.* These systems are categorized as low, moderate, or high impact based on the level of adverse effect a data breach would have on an organization's operations, assets, and personnel. If a data breach occurs on a low impact system, the impact is expected to be limited, a moderate system has a more serious impact, and a high system is one that would have a severe or catastrophic impact in the event of a data breach.

Separate from the FIPS 199 rating for systems, any vulnerabilities found on an operating system such as Microsoft Windows, are classified with risk factors using a combination of the National Vulnerability Database (NVD),[16] the Common Vulnerability Scoring System (CVSS),[17] and Common Vulnerabilities and Exposures (CVE)[18] Identifiers. All use the classification of high, medium, low, or notes/Informational, depending on the severity of the vulnerability found on the operating system.

According to NIST standards, an agency must receive an Authorization to Operate (ATO)[19] prior to moving an application into the production environment

[16] NVD is a part of the NIST Computer Security Division and is sponsored by the Department of Homeland Security's National Cyber Security Division. It supports the U.S. government multi-agency (OSD, DHS, NSA, DISA, and NIST) Information Security Automation Program. It is the U.S. government content repository for the Security Content Automation Protocol (SCAP). All vulnerabilities that are reported to NVD are siphoned through US–CERT (Computer Emergency Readiness Team).

[17] CVSS is a vulnerability scoring system designed to provide an open and standardized method for rating IT vulnerabilities. CVSS helps organizations prioritize and coordinate a joint response to security vulnerabilities by communicating the base, temporal and environmental properties of vulnerability.

[18] CVE Identifiers (also called "CVE names," "CVE numbers," "CVE-IDs," and "CVEs") are unique, common identifiers for publicly known information security vulnerabilities.

[19] An ATO is the authorization, usually by the CISO, required to put a system into production.

for common use. As part of NIST's guidance for C&A, an ATO cannot be granted if high level vulnerabilities have not been remediated.[20]

C5i identified several SEC systems that would have a severe impact to the SEC's mission and operations in the event of a data breach. Further, C5i identified multiple vulnerabilities categorized as "high" by vendors, including, Microsoft and Adobe, who made these determinations using industry standard ratings for vulnerabilities (e.g., the NVD, CVSS or CVE.) Notwithstanding the fact that both C5i and these vendors identified multiple vulnerabilities at the "high" level, OIT concluded that there were no "high" level vulnerabilities and downgraded all their vulnerabilities to the "medium" level. C5i was unable to understand how the SEC came to this conclusion and has concerns that OIT did not adequately weight the determinations of the vendors in its risk calculation/classification procedures.

OIT has developed its risk calculation to include other weighted values such as mitigating controls (i.e., firewalls, intrusion detection systems) and the likelihood of the occurrence of an event and used this classification process during the mandatory Security, Test, and Evaluation[21] phase of the SEC's C&A[22] process.

OIT's determination to downgrade all vulnerabilities to a "medium" level notwithstanding the identification by the vendors of multiple vulnerabilities at the "high" level, allowed the SEC to receive an ATO, perhaps inappropriately. C5i has concerns that by not classifying risks adequately, the SEC systems could have been exposed to high-level vulnerabilities that can easily be exploited and result in a data breach, unauthorized access, as well as disclosure of PII and other sensitive information.

Recommendation 3:

The Office of Information Technology should evaluate its risk assessment process for scoring risk to ensure that it adequately weights all appropriate factors, including the identification of risk levels by vendors.

[20] The National Institute of Standards and Technology's Special Publication 800-37, revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach,* February 2010, page F-4.

[21] Security Test and Evaluation is an examination and analysis of the safeguards required to protect an information system, as they have been applied in an operational environment, to determine the security posture of that system.

[22] C&A is required by the Federal Information Security Management Act (FISMA) of 2002, and is the process used to evaluate systems and major applications ensuring adherence to formal and established security requirements that are well documented and authorized. All systems and applications that reside on U.S. government networks must be evaluated with a formal C&A before being put into production. Systems are evaluated annually. This is referred to as "Continuous Monitoring" - and are re-accredited every three years or sooner if major changes to the systems are made.

Management Comments. The COO/Acting CIO concurred with this recommendation. See Appendix V for management's full comments.

OIG Analysis. We are pleased that the COO/Acting CIO concurred with this recommendation.

Finding 3: A Significant Vulnerability Was Identified in Assessment of HUB Application

The HUB application has a significant vulnerability that may be exploited resulting in data being compromised.

As discussed above, the OIG selected the HUB application for assessment because it contains PII data and it is actively used by Commission staff. The HUB application is a web-based, SEC-internal application used by Enforcement for case management and tracking. It is accessible to all Enforcement staff, allowing each staff member to manage its assigned caseload directly, and also provides search and "read only" access to the entire Enforcement staff Division's caseload. The HUB application provides Enforcement staff "real time" access to their cases, and could not be taken offline to conduct our assessment. Consequently, OIT provided an exact duplicate of the application and supporting database in OIT's test environment for use by the OIG in this assessment.

C5i's assessment was performed using commercial off-the-shelf products[23] that are widely used throughout the industry to conduct this type of application assessment. The assessment was performed onsite at SP and began on July 23, 2010 at approximately 9:00 p.m., eastern daylight time. C5i initially encountered problems accessing the copy of the application data that was residing in the test/staging environment, but were able to resolve the issues in coordination with OIT. The assessment was successfully completed on July 24, 2010. The assessment of the HUB application identified a significant vulnerability, as described below.

The HUB Application Does Not Use a Defined Character Set. A character set (also referred to as 'Charset') is a common coding language that can be translated and understood across various applications and platforms. The HUB application does not define a character set. Instead, the HUB application uses HyperText Markup Language (HTML) to access web applications.

The use of a common character set becomes important when a user accesses the HUB application. When a user enters a username and password to log on the HUB application, HTML uses a universal coding language to translate the user input into code that the computer understands (i.e., ones and zeros). This is

[23] The tools used to assess the application were [redacted]

then translated back to HTML when the data is returned to the Web browser (i.e. Internet Explorer), and the user is then logged into the system.

Lack of a common character set becomes problematic because if a response from the computer states that it contains HTML content but does not specify a character set, the browser may then analyze the HTML and attempt to determine which character set it appears to be using. Even if the majority of the HTML actually employs a standard character set, the presence of non-standard characters anywhere in the response may cause the browser to interpret the content using a different character set, allowing for improper translation, which can lead to unexpected results and possible security vulnerabilities in which non-standard encodings can be used to bypass the HUB's defensive filters.

Recommendation 4:

The Office of Information Technology should improve the HUB application by defining a standard recognized character set for every response containing Hypertext Markup Language content.

Management Comments. The COO/Acting CIO concurred with this recommendation. See Appendix V for management's full comments.

OIG Analysis. We are pleased the COO/Acting CIO concurred with this recommendation.

Finding 4: The Base Images Currently Being Deployed to SEC Laptops are Out Of Date and Not Compliant with OMB Regulations

Critical updates have not been applied to the base images being deployed by OIT, nor are they FDCC compliant.

C5i found through its assessment that the base image[24] deployed by OIT to SEC laptops and desktops did not comply with the OMB FDCC mandate.[25] C5i found that laptops that are distributed to SEC employees are provided with an image that does not meet FDCC requirements including installation of current approved vendor patches and updates. Further, the review identified that OMB's FDCC requirements, enacted to ensure that all equipment deployed throughout the U.S.

[24] A base image is the standardized image used by OIT to install on new laptops and desktops deployed by OIT staff. A base image contains the operating system and all standard software that has been approved for use at the SEC.

[25] The FDCC, an OMB mandate, requires that all Federal Agencies standardize the configuration of approximately 300 settings on each of their Windows XP and Vista Computers. The reason for this standardization is to strengthen Federal IT security by reducing opportunities for hackers to access and exploit government computer systems.

Federal Government has a single, standardized configuration, have not been achieved.

OMB's memorandum M-07-11, "*Implementation of Commonly Accepted Security Configurations for Windows Operating Systems,*" directs agencies to improve their information security posture and reduce overall IT operating costs. The memorandum further directs agencies that have Windows XP deployed and plan to upgrade to the Vista operating system to adopt the security configurations developed by NIST, the Department of Defense and the Department of Homeland Security, referred to as FDCC.[26]

During the assessment in June 2010, OIT provided two newly-imaged laptops at LARO to complete the evaluation of base images deployed within the SEC for evaluation.

Upon completing the assessment at LARO, C5i found that vendor patches and updates supplied by Microsoft and required for FDCC compliance had not been implemented. In addition, in July 2010, C5i conducted the same assessment of three workstations, located at SP. This assessment found that these desktops were also missing required patches and updates supplied by Microsoft and, therefore, not FDCC compliant.

OMB Memorandum M-09-29, "*FY2009 Reporting Instruction for the Federal Information Security Management Act and Agency Privacy Management*" states "Agencies must document and provide NIST with any deviations from the common security configurations (send documentation to checklists@nist.gov) and be prepared to justify why they are not using them."[27] C5i was able to confirm that the SEC does maintain a list of exceptions/deviations from the common security standards (i.e., FDCC). However, C5i found that OIT has not submitted its deviations from FDCC to NIST, as required by OMB.

Recommendation 5:

The Office of Information Technology must update the base images for all laptops and workstations prior to deployment to ensure Federal Desktop Core Configuration compliance.

[26] The Office of Management and Budget, Memorandum M-07-11, "*Implementation of Commonly Accepted Security Configurations for Windows Operating Systems*," dated March 22, 2007. http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2007/m07-11.pdf.

[27] The Office of Management and Budget, Memorandum M-09-29, "*FY2009 Reporting Instruction for the Federal Information Security Management Act and Agency Privacy Managemen*t," dated August 20, 2009. http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_fy2009/m09-29.pdf.

Management Comments. The COO/Acting CIO concurred with this recommendation. See Appendix V for management's full comments.

OIG Analysis. We are pleased that the COO/Acting CIO concurred with this recommendation.

Recommendation 6:

The Office of Information Technology must submit a completed list of common security standard deviations to the National Institute of Standards and Technology per the Office of Management and Budget's requirements.

Management Comments. The COO/Acting CIO concurred with this recommendation. See Appendix V for management's full comments.

OIG Analysis. We are pleased that the COO/Acting CIO concurred with this recommendation. However, we would request that the OIT report the common security standard deviations to NIST as soon as possible.

Finding 5: SEC Laptops Can Be Connected to the SEC Network Via LAN Port While Simultaneously Connected to An External Wireless Network

Laptops can be simultaneously connected to both a local area network (LAN) port and an external wireless network, exposing the SEC network to potential infiltration.

During the assessment of unauthorized wireless access at LARO, C5i found that the wireless access card in the two laptops provided by OIT for the assessment did not automatically disable when the laptop is plugged into the SEC network via the LAN port, although mitigating controls preventing bridging between the LAN and wireless interfaces inhibiting traffic flow between wireless and wired networks have been put in place.

C5i found that the wireless cards installed on laptops were in the state of [redacted] which provides potential attackers access to the SEC's network and data. An active directory automated script should be developed that would disable the wireless card on the laptop as soon as the laptop is plugged into the SEC network via the LAN port.

The NIST *Recommended Security Controls for Federal Information Systems and Organizations* provides the following guidance regarding Wireless Access controls:

The organization--

a. Establishes usage restrictions and implementation guidance for wireless access;
b. Monitors for unauthorized wireless access to the information system;
c. Authorizes wireless access to the information system prior to connection; and
d. Enforces requirements for wireless connections to the information system.[28]

Failure to adhere to this guidance exposes the SEC's network to potential compromise by a malicious attacker without knowledge of the user. An attacker looking for open wireless connections is able to see this open wireless connection and use it to access and compromise the laptop, and potentially the SEC network without user knowledge.

Recommendation 7:

The Office of Information Technology should turn off the wireless card installed on laptops when the laptops are connected to the Securities and Exchange Commission network via a Local Area Network port.

Management Comments. The COO/Acting CIO did not concur with this recommendation. See Appendix VI for management's full comments.

OIG Analysis. We urge the COO/Acting CIO to reconsider its objection and turn off the wireless card installed on laptops as we recommend. Our review found that the wireless access card in the two laptops provided by OIT for the assessment did not automatically disable when the laptop was plugged into the SEC network, thus providing potential access to the SEC's network and data. The solution we recommend removes any vulnerability as a result of this finding. We are pleased that OIT has agreed to research additional security precautions that may be enabled for the wireless configuration.

[28] National Institute of Standards and Technology's (NIST), Special Publication 800-53, revision 3, *Recommended Security Controls for Federal Information Systems and Organization*, http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf.

Finding 6: Improper Handling of PII Data at LARO

> PII Data is being improperly handled, stored, encrypted, and emailed at LARO.

PII Data is Contained on Shared Drives Without Access Controls, Allowing all LARO Employees Unfettered Access to Documents Saved to the [redacted] Drive and to Other Employees' Archived Email.

During the network and laptop assessments at LARO in June, 2010, C5i ran scans on the shared drive [redacted] to verify whether or not PII data was contained in shared resources and that access controls were properly enforced to ensure that only those who have a need to access the data have that ability.

Having shared drives is a common practice for organizations as it provides a repository for work that is on the network, and is backed up regularly, therefore reducing the possibility of data loss in the event of a computer crash. It also provides storage for employees of their work product so as not to use up the available hard drive and memory on their workstations/laptops in storing large amounts of information.

Most shared drives are set up providing certain levels of access to particular individuals, so that all members of a team working on a certain project can access data as their job function requires. Access to project folders on the shared drives can be limited to the specific team members/employees associated with that project. This is a common practice called "Least Privilege," and is a best practice that is used to lessen the possibility of confidential data compromise, exposure, or leaks from within the agency to outside sources.

The NIST *Recommended Security Controls for Federal Information Systems and Organization* provides guidance to organizations on Access Control, specifically defining "Separation of Duties" and "Least Privilege:"

Access Control

> *AC-5 Separation of Duties*
>
> a. Separates duties of individuals as necessary, to prevent malevolent activity without collusion;
> b. Documents separation of duties; and
> c. Implements separation of duties through assigned information system access authorizations.

> *AC-6 Least Privilege*
>
> The organization employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.[29]

SEC II 24-04.06.3, Access Control, provides guidance on access controls:

> ***Restricted File Access*** - All SEC information systems will prevent non-privileged accounts/users from modifying system level files and accessing system data and resources without a valid need-to-know. Where technically feasible, information access on SEC information systems will be restricted according to user role rather than by specific user identity.

In the assessment, C5i found that there are specific drives and folders setup for employees to store and access case data; however, they also discovered that employees are saving PII and case/project specific files on the [redacted] drive, to which all employees at LARO have access.

In addition to the project files, employees have also backed up their email archives (Personal Storage Tab files) to the [redacted] drive, and are therefore providing all other LARO employees unfettered access to their email archive. These email archives contain all emails sent during a specific timeframe – not necessarily pertaining to just one subject. Therefore, these archives will not only contain emails concerning certain work projects, but could also contain emails of a highly confidential manner, e.g., employee performance, upcoming staff restructure and personal email.

If PII or confidential data is going to be stored on the [redacted] drive, access control rights need to be modified to provide Least Privilege. Permitting access without exercising Least Privilege puts the data at risk for compromise (either accidental or malicious), or in the case of any confidential emails, misuse by a disgruntled employee or someone looking to discredit another person.

If an employee has malicious intent, with the current lack of access controls they can copy all the files from the shared drive, not just their own projects' data. Moreover, an outsider can gain access if a computer is logged into the network but is not secured and they would be able to copy all of the files without being detected. Accordingly, all of the data on the shared drive may be compromised.

[29] See also National Institute of Standards and Technology's (NIST) Special Publication 800-53, revision 3, *Recommended Security Controls for Federal Information Systems and Organization*, page http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf.

Recommendation 8:

The Office of Information Technology should implement an agency-wide policy regarding shared folder structure and access rights. Network "Least Privilege" access should be put in place to ensure that only the employees involved with a particular case have access to that data. If an employee backs up additional information to the shared resource, only they and their supervisor should have access.

Management Comments. The COO/Acting CIO partially concurred with the recommendation. See Appendix VI for management's full comments.

OIG Analysis. We are pleased that the COO/Acting CIO plans to implement an agency-wide policy regarding shared folder structures and access rights. While we are sensitive to the COO/Acting CIO concerns that limiting access to shared drives may impact business and group processes, we would encourage the COO/Acting CIO to reconsider approving such limitations as this approach would ensure that the data would not be compromised.

We are pleased that the COO/Acting CIO plans to conduct a risk assessment of its network to evaluate this issue and find ways to reduce the risks identified in this finding.

Recommendation 9:

The Office of Information Technology will ensure Personal Storage Tab (.PST) files should be saved to a protected folder.

Management Comments. The COO/Acting CIO did not concur with the recommendation. See Appendix VI for management's full comments.

OIG Analysis. While we are sensitive to the COO/Acting CIO's concern that requiring .PST files to be saved to a protected folder may impact business and group process, we urge the COO/Acting CIO to reconsider its opposition to this solution to the risk identified in this finding. We are pleased that the COO/Acting CIO intends to research this matter and plans to identify a course of action to protect the sensitive information contained in these files.

LARO Employees are Violating Policy by Sending Documents Containing PII to Personal Email Accounts and Using Portable Media that is Not Being Encrypted.

> Emailing PII data or sensitive data to a personal email address or account is in direct violation of the SEC Rules of the Road. LARO follows the SEC policy of forced encryption for all portable media; however, it not being adhered to by staff.

Another phase of the LARO network and workstation assessment was to verify if there was any mishandling of PII data through email, e.g., emailing documents containing PII insecurely. This involved analyzing the Personal Storage Tab files on the shared drives, as well as reviewing the email logs of sent and received messages and any attachments in staff email accounts.

Through this effort, C5i discovered two issues – emailing of PII to personal email accounts and a lack of encryption of emails. In order to protect the privacy of sensitive PII data, C5i provided examples to OIT as evidence of their findings; however, examples were not included in the report due to the sensitivity of the information. Examples of PII data we found that were stored in unsecured file cabinets and an unsecured office space can be found in Appendix II. Furthermore, in interviews with an IT specialist at LARO, C5i discovered that staff is unhappy and frustrated with the current forced encryption solution – [redacted] and has become impatient with how long it takes to save documents to portable media when they need to go out in the field. As a result, some employees have been saving unencrypted versions of the data on to CD's, which were found to be left unsecured on desktops during the physical assessment at LARO. In addition, C5i discovered that while data is received on encrypted CD's, staff makes multiple unencrypted copies for use during the investigations.

Staff Sending Unencrypted Documents to Personal Email Accounts. Rather than saving documents to removable media in an encrypted format, C5i found, in an email archive, that an attorney emailed unencrypted documents to a personal email address. This is a violation of SEC policy and a potentially reckless practice.

SECR 24-04-A01, SEC Rules of the Road, specifically states "DO NOT use e-mail to send material that is sensitive or that contains personally identifiable information (PII) to your personal e-mail account(s)."

Should the personal computer of the individual be compromised (malware, virus, etc.) in any way, the PII data, as well as any other sensitive information emailed would result in a data breach that the individual may not be aware of. Also, if the employees' login credentials for their personal email are compromised in any way, this information would be readily available and could be used against the commission maliciously, as well as possibly compromise an investigation.

Unencrypted Portable Media. In September 2008, the OIT CTO sent a memorandum to all SEC Division/Office Directors and Regional Directors outlining the SEC's portable media encryption policy. At that time, the regional offices were given two options – forced encryption of all portable media or optional encryption that is determined by the user. LARO adopted the SEC Policy of Forced Encryption for all portable media.

A physical walkthrough of the LARO office space, (cubes, offices, work areas, file rooms), was conducted on Saturday, and Sunday, June 26-27, 2010. With the exception of the file storage in [redacted] [redacted] [redacted] of the building, once inside the occupied space using card key access, we found that none of the offices were locked.

Upon inspection of the areas, we found CD's containing documentation pertaining to current investigations on desks, on top of file cabinets, file boxes, etc., all easily accessible. A random sampling of CD's was examined by opening the CD's using the assessment laptops and none of them were encrypted.[30]

While the random sampling of CD's did not contain any PII data, nevertheless, LARO has a policy of forced encryption of all portable media, and the fact that these CD's were unencrypted violates that policy.

While we did not find PII in our sampling, the ability to make unencrypted copies of CD's containing sensitive information is a dangerous practice – especially multiple copies. It is impossible for anyone to know all the information contained on a CD and whether or not there is PII, as well as keeping track of multiple copies of data. One of the copies can be lost or misplaced or removed from the office, putting that data a serious risk for a breach.

Recommendation 10:

The Los Angeles Regional Office (LARO) Director should reemphasize the *SEC Rules of the Road* to LARO staff through training and awareness programs and the policy needs to be strongly enforced.

Management Comments. LARO concurred with this recommendation. See Appendix VI for management's full comments.

OIG Analysis. We are pleased that the LARO concurred with this recommendation.

[30] C5i was unable to determine if the CD's were created prior to the LARO's implementation of the SEC Policy of Forced Encryption for all portable media.

Recommendation 11:

The Los Angeles Regional Office Director should enforce its encryption policy to protect sensitive data the Securities and Exchange Commission receives.

Management Comments. LARO concurred with this recommendation. See Appendix VI for management's full comments.

OIG Analysis. We are pleased that the LARO concurred with this recommendation.

Recommendation 12:

The Chief Operating Officer should implement a policy that all portable media must be fully secured (i.e., locked in file cabinets) when not in use.

Management Comments. The COO/Acting CIO concurred with this recommendation. See Appendix VI for management's full comments.

OIG Analysis. We are pleased that the COO/Acting CIO concurred with this recommendation.

Recommendation 13:

The Chief Operating Officer should appoint a privacy point of contact at each regional office to ensure compliance with Commission policies and procedures.

Management Comments. The COO/Acting CIO concurred with this recommendation. See Appendix VI for management's full comments.

OIG Analysis. We are pleased that the COO/Acting CIO concurred with this recommendation.

Hard Copy, Physical Documents Containing PII Are Unsecured

Due to the nature of the Commission's work, the need for hard copy documents for investigations is necessary, but there is a lack of physical security for the boxes of files, as well as individual documents and portable media (CD).

In the walk-through of LARO, C5i assessed the physical office space on the partial floors occupied by the SEC [redacted] [redacted] and the full floors [redacted], as well as [redacted] [redacted] [redacted] file storage rooms. The [redacted] storage room is accessible with card key access and the “cages” where the archives are stored are secured by padlock, to which only IT and facilities staff has keys. The [redacted] [redacted] storage area is accessible by access card, and all SEC employees have access to this area.

The SEC has an approved and implemented policy on the protection of sensitive data as follows:

> *II 24-04.02.01 (01.0) SEC Implementing Instruction – Sensitive Data Protection* states “All SEC sensitive information is protected in a manner commensurate with its sensitivity, value, and criticality, regardless of the media on which it is stored, the information systems that process, store, or transmit the information, or the methods by which the information is moved.”

As well, the SEC Rules of the Road address the proper handling of PII provide as follows:

> *SECR 24-04-A01 SEC Rules of the Road* reinforces this by stating:
>
> - **Do Not** leave PII material in uncontrolled areas.
> - **Do Not** grant access to PII material to individuals who are not authorized to handle such information.

On the SEC-occupied floors, there are open work areas, including employee offices/cubes, libraries, and large file rooms containing files pertaining to current LARO investigations. During the walk-through, C5i found the following areas of concern.

Unsecured Documents and Files. The rooms designated as “file rooms” on the occupied floors are not secured. They do not require card key access and the doors are left wide open. These rooms contain hard copy evidence pertinent to current investigations. The sheer volume of the files in these rooms means it would be very difficult for anyone to realize in a timely manner whether information had been removed.

Additionally, boxes of files in hallways and unsecured offices. Again, these are files pertaining to current investigations, and having them unsecured can lead to serious data compromise.

In the library areas, C5i found spreadsheets containing PII left on work tables. These spreadsheets contained PII such as: full names and addresses, account numbers, and tax ID/social security numbers. This is information that is highly desirable to anyone with the intent of identity theft. C5i also found documents containing PII left on fax machines and on desk chairs for filing. Any of these documents could have been removed, duplicated, or the data contained copied by a person with malicious intent by anyone who has approved access to the office area, which not only includes SEC employees, but also cleaning crews, security guards, and other approved personnel.

Recommendation 14:

The Los Angeles Regional Office (LARO) Director should ensure all file rooms and file cabinets at LARO are secured.

Management Comments. LARO concurred with this recommendation. See Appendix VI for management's full comments.

OIG Analysis. We are pleased that the LARO concurred with this recommendation.

Recommendation 15:

The Los Angeles Regional Office Director should ensure that boxes of files stored in hallways are moved to secured areas.

Management Comments. LARO concurred with this recommendation. See Appendix VI for management's full comments.

OIG Analysis. We are pleased that the LARO concurred with this recommendation.

Recommendation 16:

The Chief Operating Officer should either implement a clean desk policy to ensure sensitive information is properly secured, or require that all offices be locked when not occupied.

Management Comments. The COO/Acting CIO concurred with this recommendation. See Appendix VI for management's full comments.

OIG Analysis. We are pleased that the COO/Acting CIO concurred with this recommendation.

Recommendation 17:

The Chief Operating Officer should conduct additional training to ensure that staff fully understands the rules and policies concerning the handling of Personally Identifiable Information and sensitive data and their responsibilities in protecting the Securities and Exchange Commission information.

Management Comments. The COO/Acting CIO concurred with this recommendation. See Appendix VI for management's full comments.

OIG Analysis. We are pleased that the COO/Acting CIO concurred with this recommendation.

Finding 7: The SEC Has No Final Policies or Procedures for the Destruction of Portable Media Storage Devices

The SEC does not have formal, documented, approved, and well-communicated policies or procedures for the destruction of portable media storage devices.

SEC staff regularly use portable media storage devices, such as thumb drives and CD's, to save files, including files containing sensitive, confidential, non-public, and/or PII data. C5i found that the SEC does not have a formal, documented, or approved policy for destruction of portable media storage devices in place, contrary to NIST standards and security best practices.

The NIST *Recommended Security Controls for Federal Information Systems and Organization* also provides guidance on Media Protection. This guidance also suggests, "The organization develops, disseminates, and reviews/updates: a. A formal, documented media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls."[31]

The *SEC Implementing Instructions – Sensitive Data Protection,* II 24-04.02.01 (01.0), April 6, 2006, provides instructions on the protection of sensitive data and the need for shredding of sensitive data. The *Implementing Instructions* state, "Disposal/Destruction. Sensitive materials must be destroyed by shredding or by other approved means that provide a similar level of destruction."

During the review, C5i found that OIT has drafted operating procedures concerning the destruction of portable media devices titled, *Hard Drive Wiping*

[31] NIST, Special Publication 800-53, revision 3, *Recommended Security Controls for Federal Information Systems and Organization, http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf.*

and Media Destruction.[32] These draft operating procedures outline OIT's proposed policy for disposal of media storage devices; however, they do not identify the roles and responsibilities of the originator, i.e., the employee. In addition, this draft operating procedure has not been formalized or approved by senior management.

C5i found during interviews in July and August 2010 with SEC Headquarters (HQ) staff members that HQ staff did not know where or how to properly dispose of portable media storage devices containing sensitive information. Furthermore, the physical inspection of HQ, the OPC, and LARO found that secured containers for the shredding and/or disposal of portable media storage devices were not conveniently allocated throughout the facilities.

The lack of formal, documented, and well-communicated policies and procedures could result in the mishandling and improper disposal of media containing sensitive and/or PII data. In addition, the lack of conveniently locatable, secured containers could discourage individuals from properly disposing of portable media storage devices, and increase the likelihood of unauthorized individuals accessing sensitive and PII data.

Recommendation 18:

The Office of Information Technology should finalize, approve and implement its operating procedures for *Hard Drive Wiping and Media Destruction*, and make staff aware of the procedures and their roles and responsibilities for the disposal of portable media storage devices. These operating procedures should include information concerning the roles and responsibilities of all Commission employees in the proper destruction of portable media storage devices.

Management Comments. The COO/Acting CIO concurred with this recommendation. See Appendix VI for management's full comments.

OIG Analysis. We are pleased that the COO/Acting CIO concurred with this recommendation.

Recommendation 19:

The Office of Information Technology should provide Commission staff training on the handling, disposal, and storage of portable media storage devices.

[32] DRAFT *Operating Procedure: Hard Drive Wiping and Media Destruction*, OP 24-05.02.06.10 (01.0) – January 26, 2010.

Management Comments. The COO/Acting CIO concurred with this recommendation. See Appendix VI for management's full comments.

OIG Analysis. We are pleased that the COO/Acting CIO concurred with this recommendation.

Recommendation 20:

The Office of Administrative Services should provide secured bins for the disposal of portable media storage devices that are easily accessible to all Commission employees and the use and locations of these bins should be clearly communicated to all employees.

Management Comments. OAS concurred with this recommendation. See Appendix VI for management's full comments.

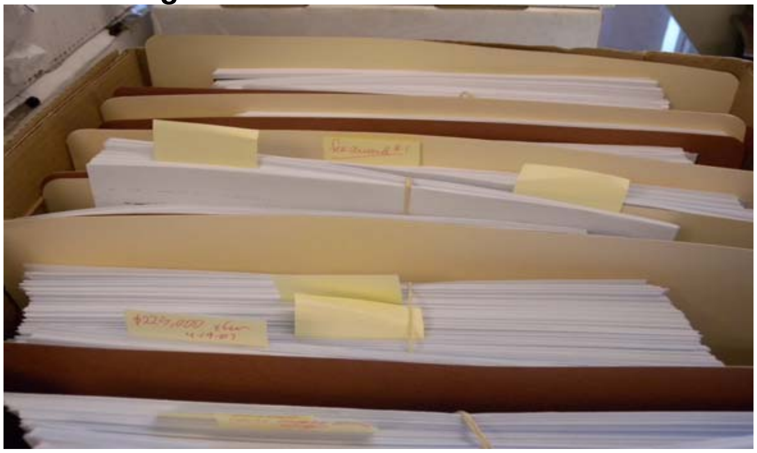
OIG Analysis. We are pleased that the OAS concurred with this recommendation.

Acronyms

C&A	Certification and Accreditation
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CPO	Chief Privacy Officer
CSIRT	Computer Security Incident Response Team
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
FDCC	Federal Desktop Core Configuration
FIPS	Federal Information Processing Standards
HP	Hewlett-Packard
HQ	Headquarters
LARO	Los Angeles Regional Office
NIST	National Institute of Standards and Technology
NVA	Network Vulnerability Assessment
NVD	Network Vulnerability Database
OASA	Onsite Application Security Assessment
OGC	Office of General Counsel
OIG	Office of Inspector General
OIT	Office of Information Technology
OMB	Office of Management and Budget
OPC	Operations Center
OWASP	Open Web Application Security Project
PAW	Privacy Assessment Worksheet
PDT	Pacific Daylight Time
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIRT	Privacy Incident Response Team
ROE	Rules of Engagement
SAOP	Senior Agency Official for Privacy
SEC	Securities and Exchange Commission
SORN	System of Records Notice
SP	Station Place
USGCB	United States Government Configuration Baseline

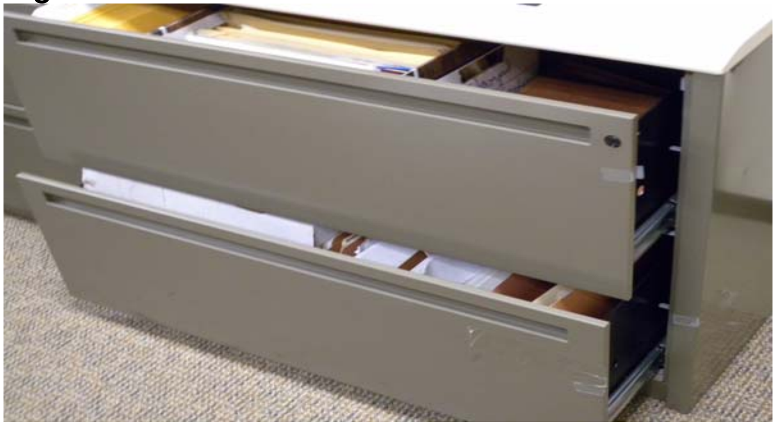
Examples of PII Violations

Figure 1: Unsecured Files Found in the Open Containing PII Data at LARO



Source: Generated by C5i

Figure 2: Unsecured Files at LARO



Source: Generated by C5i

Scope and Methodology

Scope. The scope of our review covered calendar year 2008 to July 2010 and includes the SEC headquarters offices and divisions (includes the OPC and LARO). To ensure the protection of the Commission's employees, contractors and customer's PII information, our scope also included a review of OIT's oversight of Commission offices and divisions and the SEC's governing privacy policies and procedures, NIST guidance, OMB guidelines and other governing guidance and regulations. Our review also included select workstations, laptops and servers. We further performed a network vulnerability assessment at LARO and OPC to evaluate the security posture of the SEC's network in handling and protecting PII data. Lastly, we followed up on a previous issued OIG report's recommendations that pertained to privacy and the protection of PII data.[33]

Methodology. In evaluating the adequacy of the SEC's privacy policies and procedures, OIT's interaction and involvement with the Commission's offices and divisions we identified the universe of where privacy data resides and conducted an assessment of the area. We further interviewed OIT staff to ascertain their knowledge of federal guidance on the protection of PII information and the proper procedures for protecting PII. We also reviewed the Annual Privacy Awareness Training guidance and policy that is issued to SEC employees and contractors, to verify that it addressed all issues surrounding the responsibility of Commission employees and contractors to protect PII information.

To meet the objective of performing an in depth analysis of privacy requirements and to identify the SEC's process and procedures that are used to conduct privacy reviews, we interviewed OIT staff, conducted a physical inspection of the office space that is occupied by SEC staff at LARO, conducted an assessment of the LARO network servers, and conducted an assessment on a sample selection of its deployed and un-deployed workstations. To ensure compliance with SEC policies and procedures regarding the handling and protection of PII data we conducted a physical inspection at LARO by walking through offices and storage areas. We documented our findings by taking photographic evidence of PII information that was not properly stored.

Further, to meet the objective to assess whether the SEC has developed and implemented technical, managerial, or operational privacy-related controls to effectively mitigate know risks that are inherent to the Privacy Act's system of records, C5i assessed 66 workstations/laptops, 8 servers, and 2 freshly imaged laptops, which provided an in-depth picture of LARO's network security posture. We further conducted a vulnerability assessment at the OPC. We also reviewed

[33] SEC Report No. 475, *Evaluation of the SEC Privacy Program*, March 26, 2010.

the shared drive [redacted] to verify access controls in protecting information and backed up Outlook Personal Storage Tab files to ensure that PII transmitted via email was properly protected. Lastly, we conducted a HUB application assessment to evaluate the security posture of the application in protecting PII data.

Criteria and Guidance

C5i used the following guidelines for this evaluation:

- OMB Memorandum 07-11, “Implementation of Commonly Accepted Security Configurations for Windows Operating System”
- OMB Memorandum 08-22, “Guidance on the Federal Desktop Core Configuration”
- OMB Memorandum 09-29, “FY2009 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management”
- OMB Memorandum 03-22, “OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002”
- NIST SP 800-70. “National Checklist Program for IT Products—Guidelines for Checklist Users and Developers”
- NIST SP 800-122, “Guide to Protecting the Confidentiality of Personally Identifiable Information”
- NIST SP 800-53 Rev 3, “Recommended Security Controls for Federal Information Systems”
- NIST SP 800-40, “Creating a Patch and Vulnerability Management Program”
- NIT SP 800 -111, “Guide to Storage Encryption Technologies for End User Devices”
- The Privacy Act of 1974
- Computer Security Act of 1987
- SEC/OIT, Privacy Impact Assessment Guide, January 2007
- SEC Privacy Analysis Worksheet Template
- SEC Privacy Impact Assessment Template
- Safeguarding Personally Identifiable Information (PII)
- SEC Rules of the Road
- SEC Regulation 23-2a, Safeguarding Non-Public Information
- SEC, IT Security Implementing Instruction, II 24-04.02.01 (01.0), Sensitive Data Protection

List of Recommendations

Recommendation 1:

The Office of Information Technology should apply patches and updates to the Commission's networks, workstations, and laptops on a timely basis. All future patches should be applied within [redacted] of vendor release, with emergency patches being applied on an ad-hoc basis to protect the agency's systems and data.

Recommendation 2:

The Office of Information Technology should implement formal processes and procedures to regularly review whether a newly-released patch should or should not be applied to the environment.

Recommendation 3:

The Office of Information Technology should evaluate its risk assessment process for scoring risk to ensure that it adequately weights all appropriate factors, including the identification of risk levels by vendors.

Recommendation 4:

The Office of Information Technology should improve the HUB application by defining a standard recognized character set for every response containing Hypertext Markup Language content.

Recommendation 5:

The Office of Information Technology must update the base images for all laptops and workstations prior to deployment to ensure Federal Desktop Core Configuration compliance.

Recommendation 6:

The Office of Information Technology must submit a completed list of common security standard deviations to the National Institute of Standards and Technology per the Office of Management and Budget's requirements.

Recommendation 7:

The Office of Information Technology should turn off the wireless card installed on laptops when the laptops are connected to the Securities and Exchange Commission network via a Local Area Network port.

Recommendation 8:

The Office of Information Technology should implement an agency-wide policy regarding shared folder structure and access rights. Network "Least Privilege" access should be put in place to ensure that only the employees involved with a particular case have access to that data. If an employee backs up additional information to the shared resource, only they and their supervisor should have access.

Recommendation 9:

The Office of Information Technology will ensure Personal Storage Tab (.PST) files should be saved to a protected folder.

Recommendation 10:

The Los Angeles Regional Office (LARO) Director should reemphasize the *SEC Rules of the Road* to LARO staff through training and awareness programs and the policy needs to be strongly enforced.

Recommendation 11:

The Los Angeles Regional Office Director should enforce its encryption policy to protect sensitive data the Securities and Exchange Commission receives.

Recommendation 12:

The Chief Operating Officer should implement a policy that all portable media must be fully secured (i.e., locked in file cabinets) when not in use.

Recommendation 13:

The Chief Operating Officer should appoint a privacy point of contact at each regional office to ensure compliance with Commission policies and procedures.

Recommendation 14:

The Los Angeles Regional Office (LARO) Director should ensure all file rooms and file cabinets at LARO are secured.

Recommendation 15:

The Los Angeles Regional Office Director should ensure that boxes of files stored in hallways should be moved to secured areas.

Recommendation 16:

The Chief Operating Officer should either implement a clean desk policy to ensure sensitive information is properly secured, or require that all offices be locked when not occupied.

Recommendation 17:

The Chief Operating Officer should conduct additional training to ensure that staff fully understands the rules and policies concerning the handling of Personally Identifiable Information and sensitive data and their responsibilities in protecting Securities and Exchange Commission information.

Recommendation 18:

The Office of Information Technology should finalize, approve and implement its operating procedures for *Hard Drive Wiping and Media Destruction*, and make staff aware of the procedures and their roles and responsibilities for the disposal of portable media storage devices. These operating procedures must include information concerning the roles and responsibilities of all Commission employees in the proper destruction of portable media storage devices.

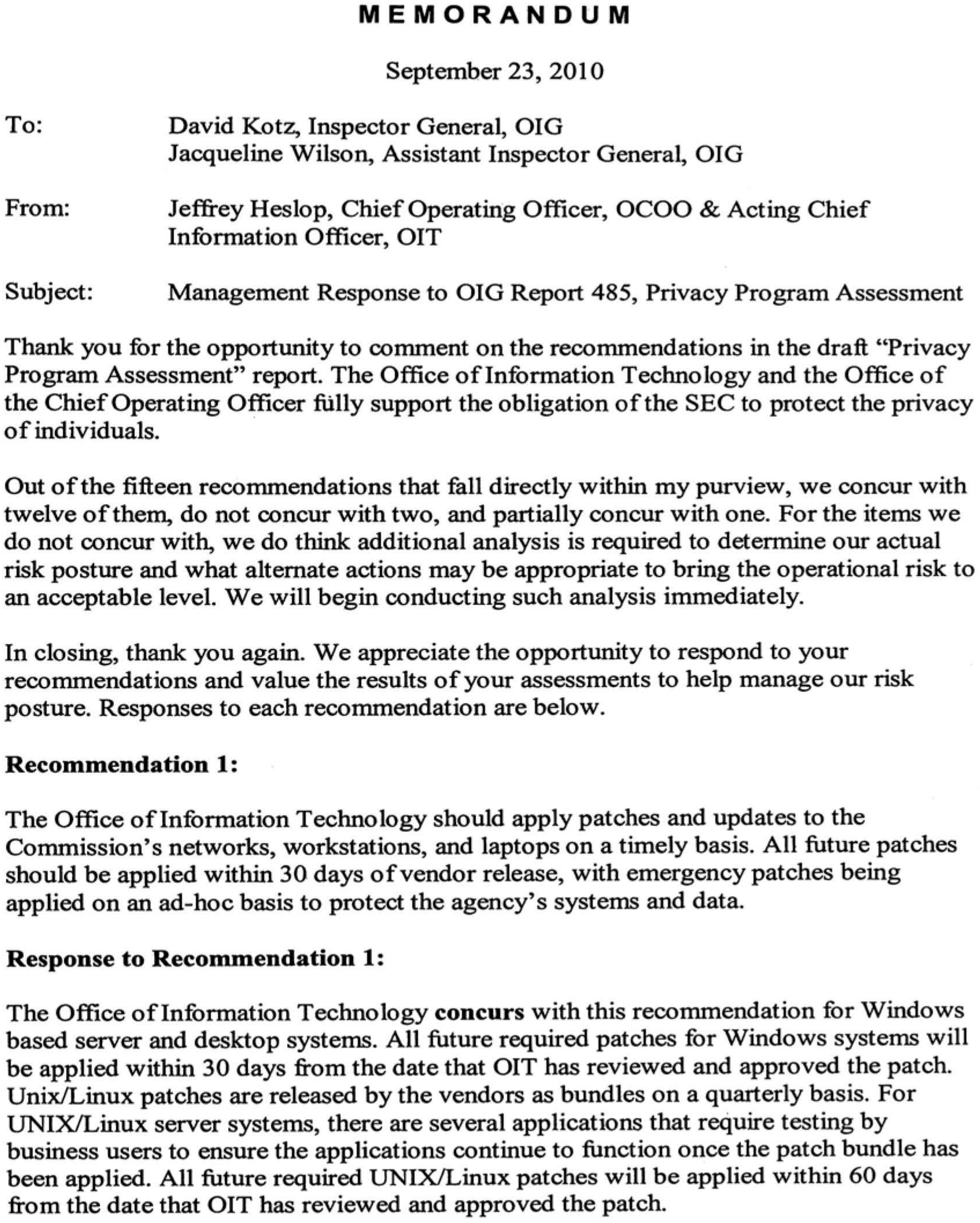
Recommendation 19:

The Office of Information Technology should provide Commission staff training on the handling, disposal, and storage of portable media storage devices.

Recommendation 20:

The Office of Administrative Services should provide secured bins for the disposal of portable media storage devices that are easily accessible to all Commission employees and the use and locations of these bins should be clearly communicated to all employees.

Management Comments



MEMORANDUM

September 23, 2010

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

From: Jeffrey Heslop, Chief Operating Officer, OCOO & Acting Chief Information Officer, OIT

Subject: Management Response to OIG Report 485, Privacy Program Assessment

Thank you for the opportunity to comment on the recommendations in the draft "Privacy Program Assessment" report. The Office of Information Technology and the Office of the Chief Operating Officer fully support the obligation of the SEC to protect the privacy of individuals.

Out of the fifteen recommendations that fall directly within my purview, we concur with twelve of them, do not concur with two, and partially concur with one. For the items we do not concur with, we do think additional analysis is required to determine our actual risk posture and what alternate actions may be appropriate to bring the operational risk to an acceptable level. We will begin conducting such analysis immediately.

In closing, thank you again. We appreciate the opportunity to respond to your recommendations and value the results of your assessments to help manage our risk posture. Responses to each recommendation are below.

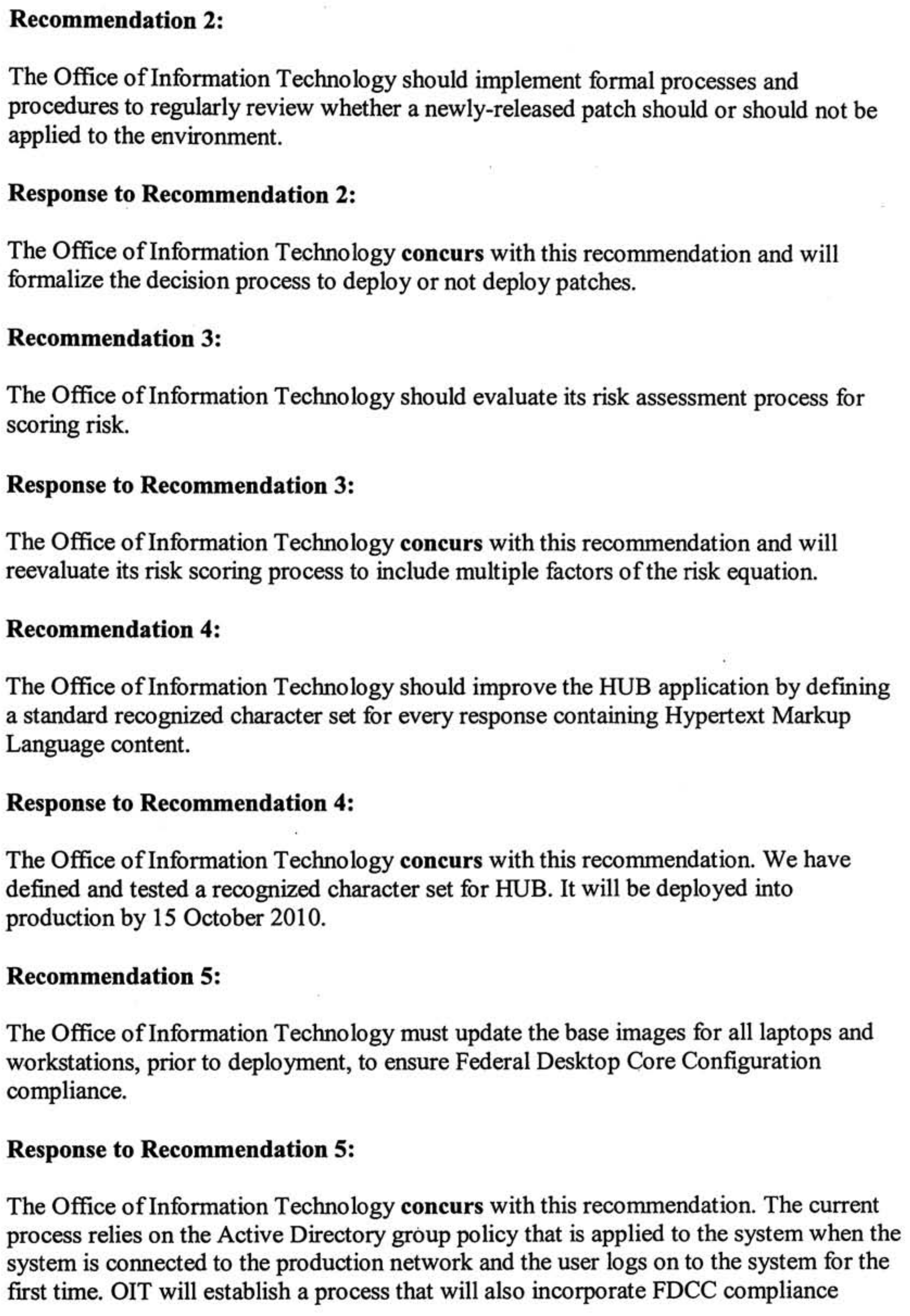
Recommendation 1:

The Office of Information Technology should apply patches and updates to the Commission's networks, workstations, and laptops on a timely basis. All future patches should be applied within 30 days of vendor release, with emergency patches being applied on an ad-hoc basis to protect the agency's systems and data.

Response to Recommendation 1:

The Office of Information Technology **concurs** with this recommendation for Windows based server and desktop systems. All future required patches for Windows systems will be applied within 30 days from the date that OIT has reviewed and approved the patch. Unix/Linux patches are released by the vendors as bundles on a quarterly basis. For UNIX/Linux server systems, there are several applications that require testing by business users to ensure the applications continue to function once the patch bundle has been applied. All future required UNIX/Linux patches will be applied within 60 days from the date that OIT has reviewed and approved the patch.

Appendix VI



Recommendation 2:

The Office of Information Technology should implement formal processes and procedures to regularly review whether a newly-released patch should or should not be applied to the environment.

Response to Recommendation 2:

The Office of Information Technology **concurs** with this recommendation and will formalize the decision process to deploy or not deploy patches.

Recommendation 3:

The Office of Information Technology should evaluate its risk assessment process for scoring risk.

Response to Recommendation 3:

The Office of Information Technology **concurs** with this recommendation and will reevaluate its risk scoring process to include multiple factors of the risk equation.

Recommendation 4:

The Office of Information Technology should improve the HUB application by defining a standard recognized character set for every response containing Hypertext Markup Language content.

Response to Recommendation 4:

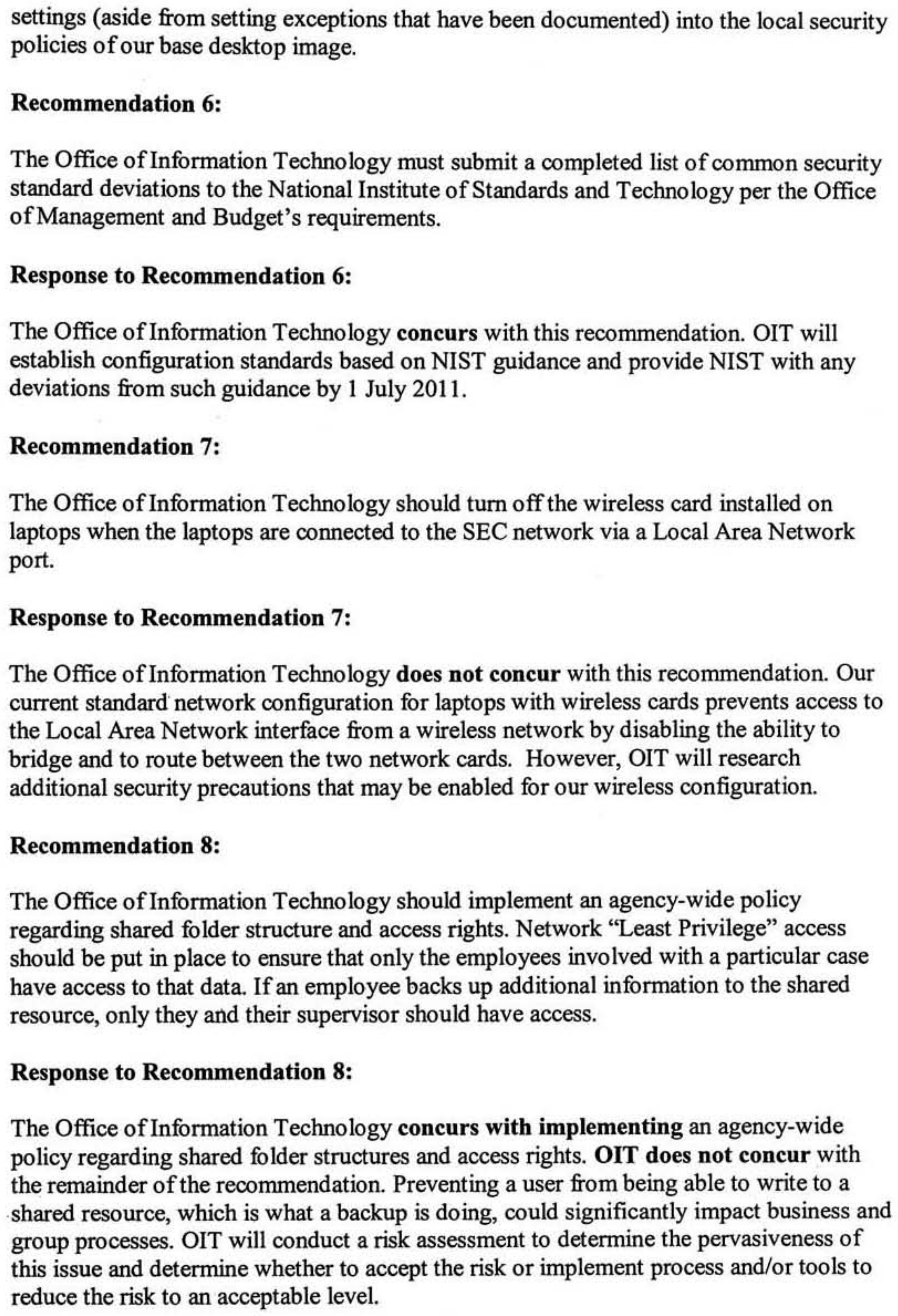
The Office of Information Technology **concurs** with this recommendation. We have defined and tested a recognized character set for HUB. It will be deployed into production by 15 October 2010.

Recommendation 5:

The Office of Information Technology must update the base images for all laptops and workstations, prior to deployment, to ensure Federal Desktop Core Configuration compliance.

Response to Recommendation 5:

The Office of Information Technology **concurs** with this recommendation. The current process relies on the Active Directory group policy that is applied to the system when the system is connected to the production network and the user logs on to the system for the first time. OIT will establish a process that will also incorporate FDCC compliance



settings (aside from setting exceptions that have been documented) into the local security policies of our base desktop image.

Recommendation 6:

The Office of Information Technology must submit a completed list of common security standard deviations to the National Institute of Standards and Technology per the Office of Management and Budget's requirements.

Response to Recommendation 6:

The Office of Information Technology **concurs** with this recommendation. OIT will establish configuration standards based on NIST guidance and provide NIST with any deviations from such guidance by 1 July 2011.

Recommendation 7:

The Office of Information Technology should turn off the wireless card installed on laptops when the laptops are connected to the SEC network via a Local Area Network port.

Response to Recommendation 7:

The Office of Information Technology **does not concur** with this recommendation. Our current standard network configuration for laptops with wireless cards prevents access to the Local Area Network interface from a wireless network by disabling the ability to bridge and to route between the two network cards. However, OIT will research additional security precautions that may be enabled for our wireless configuration.

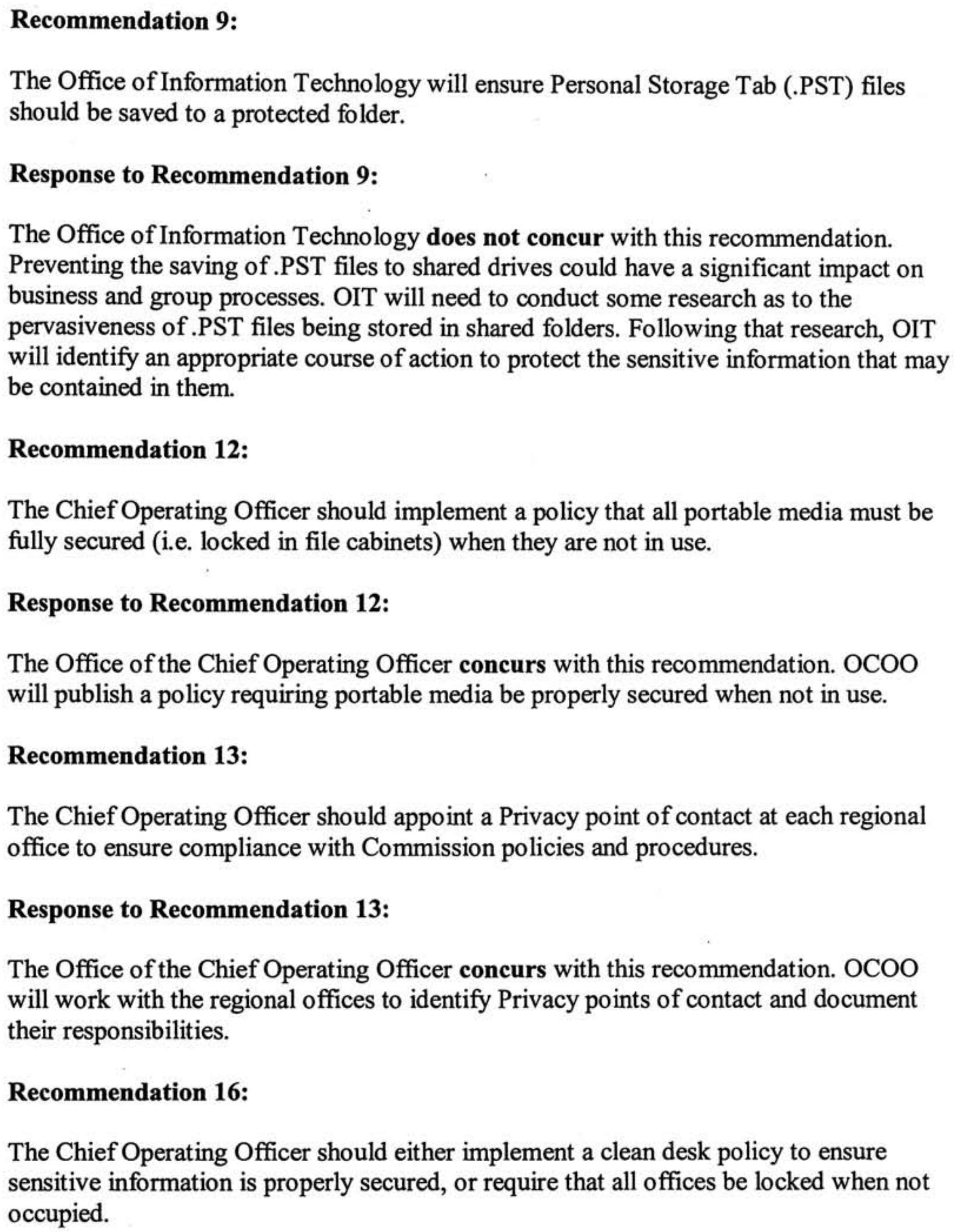
Recommendation 8:

The Office of Information Technology should implement an agency-wide policy regarding shared folder structure and access rights. Network "Least Privilege" access should be put in place to ensure that only the employees involved with a particular case have access to that data. If an employee backs up additional information to the shared resource, only they and their supervisor should have access.

Response to Recommendation 8:

The Office of Information Technology **concurs with implementing** an agency-wide policy regarding shared folder structures and access rights. **OIT does not concur** with the remainder of the recommendation. Preventing a user from being able to write to a shared resource, which is what a backup is doing, could significantly impact business and group processes. OIT will conduct a risk assessment to determine the pervasiveness of this issue and determine whether to accept the risk or implement process and/or tools to reduce the risk to an acceptable level.

Appendix VI



Recommendation 9:

The Office of Information Technology will ensure Personal Storage Tab (.PST) files should be saved to a protected folder.

Response to Recommendation 9:

The Office of Information Technology **does not concur** with this recommendation. Preventing the saving of .PST files to shared drives could have a significant impact on business and group processes. OIT will need to conduct some research as to the pervasiveness of .PST files being stored in shared folders. Following that research, OIT will identify an appropriate course of action to protect the sensitive information that may be contained in them.

Recommendation 12:

The Chief Operating Officer should implement a policy that all portable media must be fully secured (i.e. locked in file cabinets) when they are not in use.

Response to Recommendation 12:

The Office of the Chief Operating Officer **concurs** with this recommendation. OCOO will publish a policy requiring portable media be properly secured when not in use.

Recommendation 13:

The Chief Operating Officer should appoint a Privacy point of contact at each regional office to ensure compliance with Commission policies and procedures.

Response to Recommendation 13:

The Office of the Chief Operating Officer **concurs** with this recommendation. OCOO will work with the regional offices to identify Privacy points of contact and document their responsibilities.

Recommendation 16:

The Chief Operating Officer should either implement a clean desk policy to ensure sensitive information is properly secured, or require that all offices be locked when not occupied.

Response to Recommendation 16:

The Office of the Chief Operating Officer **concurs** with this recommendation. OCOO will establish a policy for the proper protection of sensitive information on portable media or in other portable formats, such as paper.

Recommendation 17:

The Chief Operating Officer should conduct additional training to ensure that staff fully understands the rules and policies concerning the handling of PII and sensitive data and their responsibilities in protecting SEC information.

Response to Recommendation 17:

The Office of the Chief Operating Officer **concurs** with this recommendation. The SEC already requires annual security and privacy training for all staff. In addition, the Privacy Officer will conduct an analysis to identify areas of staff or individuals who may require additional training on policies concerning the protection of sensitive information. When identified, they may be required to repeat their security and privacy training or receive more focused training as resources permit.

Recommendation 18:

The Office of Information Technology should finalize, approve and implement its operating procedures for Hard Drive Wiping and Media Destruction, and make staff aware of the procedures and their roles and responsibilities for the disposal of portable storage media devices. These operating procedures must include information concerning the roles and responsibilities of all Commission employees in the proper destruction of portable storage media devices.

Response to Recommendation 18:

The Office of Information Technology **concurs** with this recommendation. The procedures for media destruction will be finalized and distributed.

Recommendation 19:

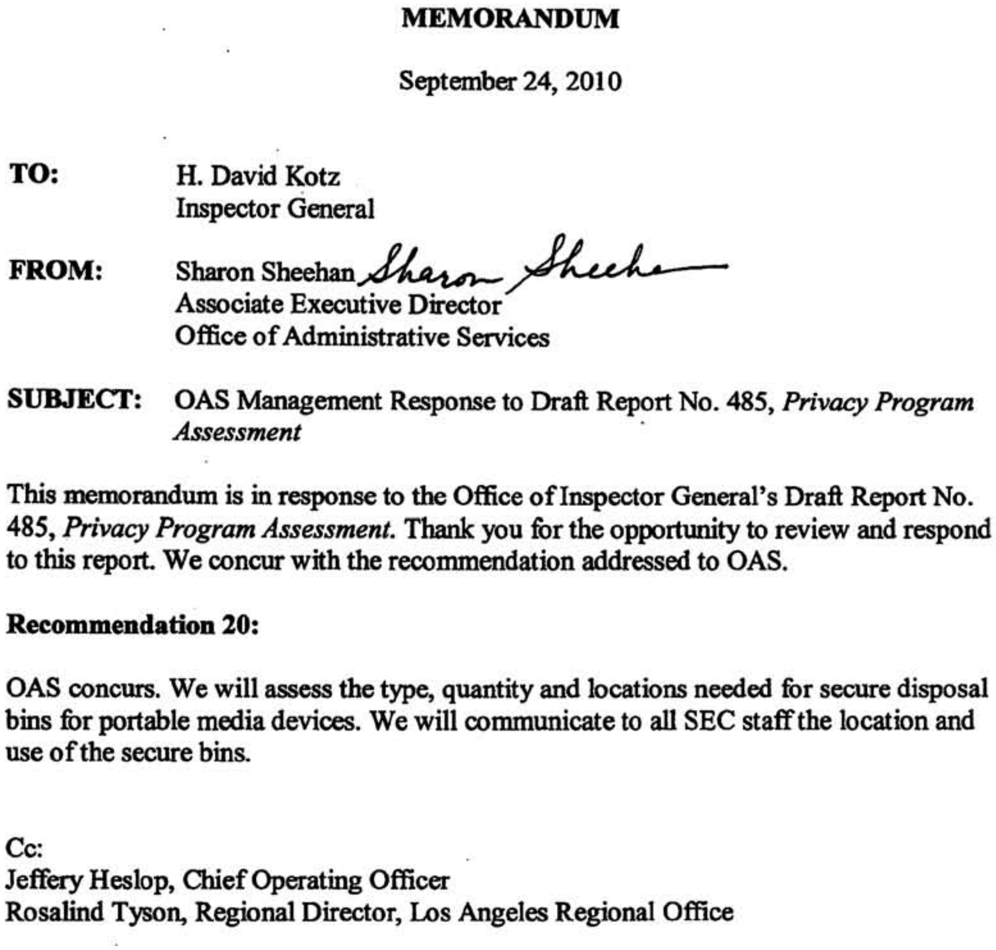
The Office of Information Technology should provide Commission staff training on the handling, disposal, and storage of portable storage media devices.

Response to Recommendation 19:

The Office of Information Technology **concurs** with this recommendation. Training on the handling, disposal, and storage of portable media devices will be provide to support additional guidance being developed by OIT and OCOO.

:

Appendix VI



MEMORANDUM

September 24, 2010

TO: H. David Kotz
Inspector General

FROM: Sharon Sheehan Sharon Sheehan
Associate Executive Director
Office of Administrative Services

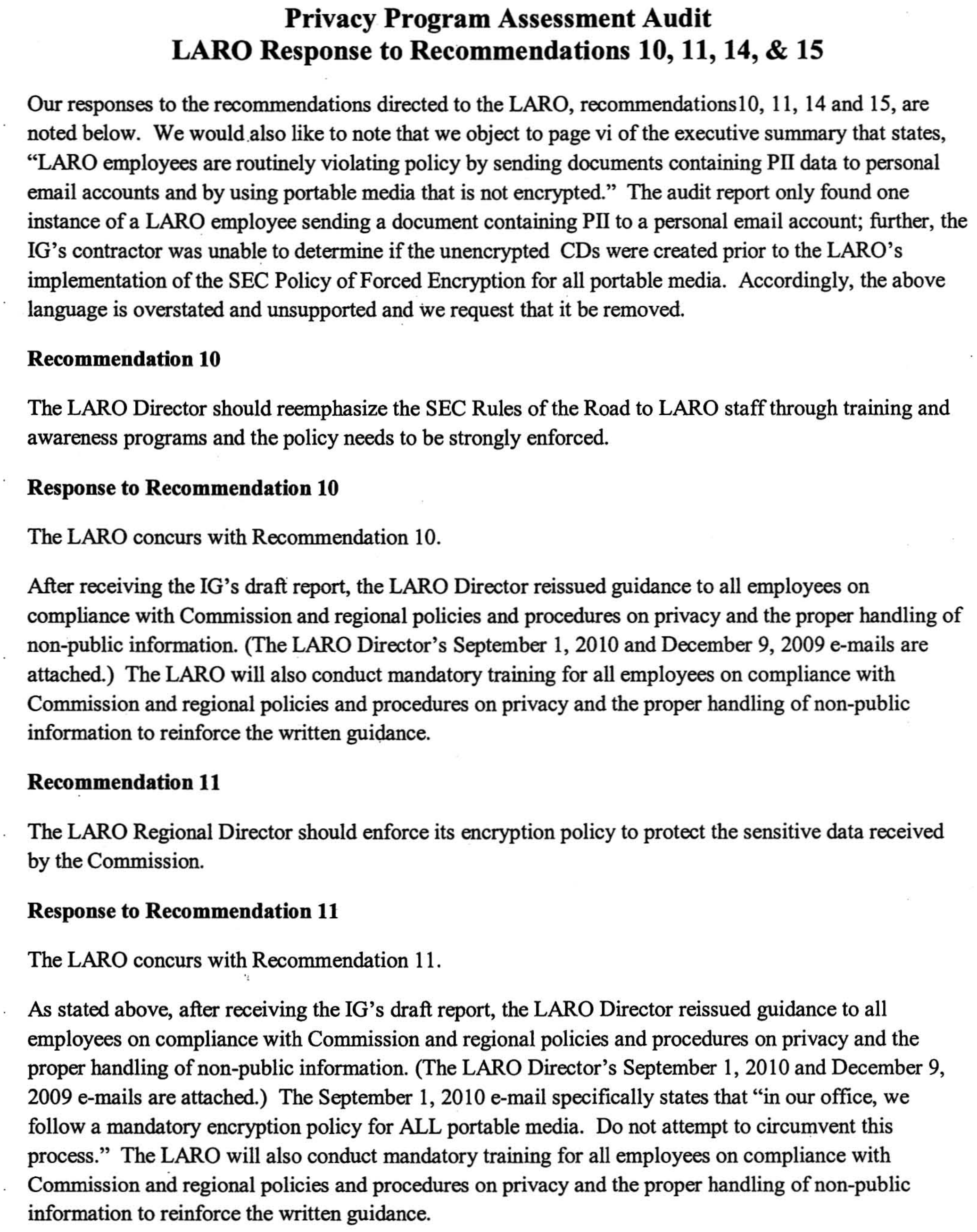
SUBJECT: OAS Management Response to Draft Report No. 485, *Privacy Program Assessment*

This memorandum is in response to the Office of Inspector General's Draft Report No. 485, *Privacy Program Assessment*. Thank you for the opportunity to review and respond to this report. We concur with the recommendation addressed to OAS.

Recommendation 20:

OAS concurs. We will assess the type, quantity and locations needed for secure disposal bins for portable media devices. We will communicate to all SEC staff the location and use of the secure bins.

Cc:
Jeffery Heslop, Chief Operating Officer
Rosalind Tyson, Regional Director, Los Angeles Regional Office



Privacy Program Assessment Audit
LARO Response to Recommendations 10, 11, 14, & 15

Our responses to the recommendations directed to the LARO, recommendations10, 11, 14 and 15, are noted below. We would also like to note that we object to page vi of the executive summary that states, "LARO employees are routinely violating policy by sending documents containing PII data to personal email accounts and by using portable media that is not encrypted." The audit report only found one instance of a LARO employee sending a document containing PII to a personal email account; further, the IG's contractor was unable to determine if the unencrypted CDs were created prior to the LARO's implementation of the SEC Policy of Forced Encryption for all portable media. Accordingly, the above language is overstated and unsupported and we request that it be removed.

Recommendation 10

The LARO Director should reemphasize the SEC Rules of the Road to LARO staff through training and awareness programs and the policy needs to be strongly enforced.

Response to Recommendation 10

The LARO concurs with Recommendation 10.

After receiving the IG's draft report, the LARO Director reissued guidance to all employees on compliance with Commission and regional policies and procedures on privacy and the proper handling of non-public information. (The LARO Director's September 1, 2010 and December 9, 2009 e-mails are attached.) The LARO will also conduct mandatory training for all employees on compliance with Commission and regional policies and procedures on privacy and the proper handling of non-public information to reinforce the written guidance.

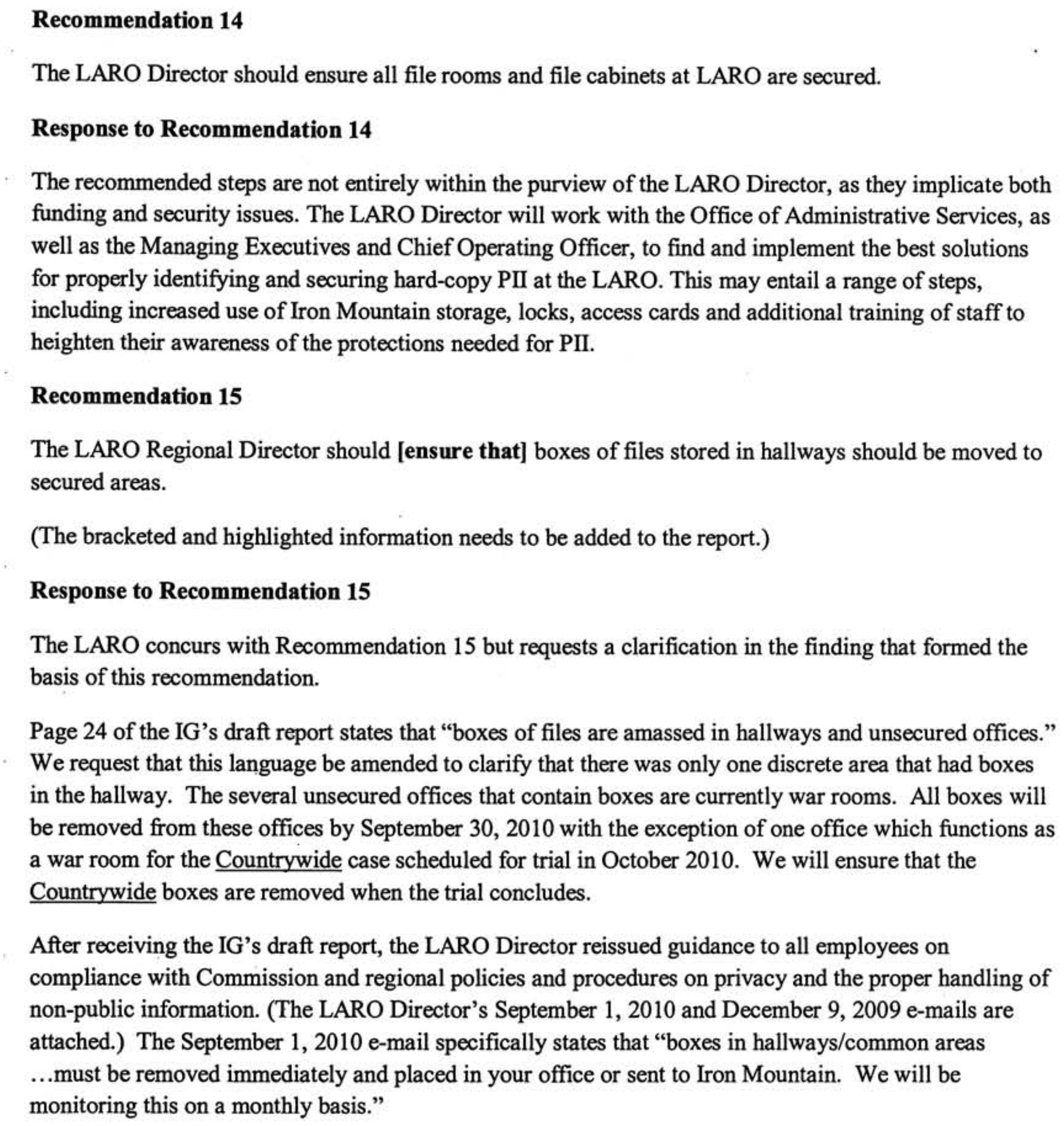
Recommendation 11

The LARO Regional Director should enforce its encryption policy to protect the sensitive data received by the Commission.

Response to Recommendation 11

The LARO concurs with Recommendation 11.

As stated above, after receiving the IG's draft report, the LARO Director reissued guidance to all employees on compliance with Commission and regional policies and procedures on privacy and the proper handling of non-public information. (The LARO Director's September 1, 2010 and December 9, 2009 e-mails are attached.) The September 1, 2010 e-mail specifically states that "in our office, we follow a mandatory encryption policy for ALL portable media. Do not attempt to circumvent this process." The LARO will also conduct mandatory training for all employees on compliance with Commission and regional policies and procedures on privacy and the proper handling of non-public information to reinforce the written guidance.



Recommendation 14

The LARO Director should ensure all file rooms and file cabinets at LARO are secured.

Response to Recommendation 14

The recommended steps are not entirely within the purview of the LARO Director, as they implicate both funding and security issues. The LARO Director will work with the Office of Administrative Services, as well as the Managing Executives and Chief Operating Officer, to find and implement the best solutions for properly identifying and securing hard-copy PII at the LARO. This may entail a range of steps, including increased use of Iron Mountain storage, locks, access cards and additional training of staff to heighten their awareness of the protections needed for PII.

Recommendation 15

The LARO Regional Director should **[ensure that]** boxes of files stored in hallways should be moved to secured areas.

(The bracketed and highlighted information needs to be added to the report.)

Response to Recommendation 15

The LARO concurs with Recommendation 15 but requests a clarification in the finding that formed the basis of this recommendation.

Page 24 of the IG's draft report states that "boxes of files are amassed in hallways and unsecured offices." We request that this language be amended to clarify that there was only one discrete area that had boxes in the hallway. The several unsecured offices that contain boxes are currently war rooms. All boxes will be removed from these offices by September 30, 2010 with the exception of one office which functions as a war room for the Countrywide case scheduled for trial in October 2010. We will ensure that the Countrywide boxes are removed when the trial concludes.

After receiving the IG's draft report, the LARO Director reissued guidance to all employees on compliance with Commission and regional policies and procedures on privacy and the proper handling of non-public information. (The LARO Director's September 1, 2010 and December 9, 2009 e-mails are attached.) The September 1, 2010 e-mail specifically states that "boxes in hallways/common areas …must be removed immediately and placed in your office or sent to Iron Mountain. We will be monitoring this on a monthly basis."

OIG Response to Management's Comments

We are pleased that the COO/Acting CIO fully concurred with 12 of the 15 recommendations that pertained to its office. However, we urge the COO/Acting CIO to reconsider its opposition to recommendation Nos. 7 and 9, and its partial opposition to recommendation No. 8, as the solutions we provided would remove any vulnerability and protect the SEC's information. We are pleased that the COO/Acting CIO acknowledges that the risks we identified in connection with recommendation Nos. 7, 8 and 9, need to be addressed and that OIT intends to conduct research to determine an appropriate course of action to remedy the concerns we identified.

We are also pleased that the LARO Regional Director concurs with all four recommendations that were addressed to her office, and has taken immediate steps to provide controls to ensure PII data is properly handled and secured.

Additionally, we are pleased that OAS concurred with the recommendation addressed to its office and has indicated that office will provide secured bins to dispose of portable media storage in accessible locations within the Commission.

We believe that the implementation of all these important recommendations will significantly improve the SEC's ability to protect PII data and ameliorate the vulnerabilities identified in this review.

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
Email: 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