



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

SEC's Controls Over Sensitive/Nonpublic
Information Collected and Exchanged With the
Financial Stability Oversight Council and
Office of Financial Research



March 25, 2013
Report No. 509



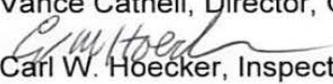
OFFICE OF
INSPECTOR GENERAL

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

MEMORANDUM

March 25, 2013

To: Elisse B. Walter, Chairman
Thomas A. Bayer, Director/Chief Information Officer, Office of
Information Technology
Vance Cathell, Director, Office of Acquisitions

From: 
Carl W. Hoecker, Inspector General, Office of Inspector General

Subject: *SEC's Controls Over Sensitive/Nonpublic Information Collected and Exchanged with the Financial Stability Oversight Council and Office of Financial Research, Report No. 509*

This memorandum transmits the U.S. Securities and Exchange Commission Office of Inspector General's (OIG) final report detailing the results of our audit of the *SEC's Controls Over Sensitive/Nonpublic Information Collected and Exchanged with the Financial Oversight Council and the Office of Financial Research*. The audit was conducted as part of our continuous effort to assess the Commission's programs and operations.

This report contains five recommendations which if fully implemented should strengthen the SEC's controls over sensitive and nonpublic information that is collected and exchanged with Financial Oversight Council and Office of Financial Research. The Chairman's office, Office of Information Technology, and Office of Acquisitions concurred with all recommendations pertaining to their respective offices. Your written responses to the draft report's recommendations are included in Appendix V.

Within the next 45 days, please provide OIG with a written corrective action plan that addresses the recommendations to your office. The corrective action plan should include information such as the responsible official/point of contact, timeframes for completing required actions, and milestones identifying how the recommendations will be addressed.

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

Attachment

cc: Erica Y. Williams, Deputy Chief of Staff, Office of the Chairman
Luis A. Aguilar, Commissioner
Troy A. Paredes, Commissioner
Daniel M. Gallagher, Commissioner
Sara Cortes, Senior Advisor to the Chairman, Office of the Chairman
Jeff Heslop, Chief Operating Officer, Office of Chief of Operations
Pamela C. Dyson, Deputy Director/Deputy CIO, Office of Information
Technology
Todd K. Scharf, Associate Director, Chief Information Security Officer,
Office of Information Technology

SEC's Controls Over Sensitive/Nonpublic Information Collected and Exchanged With the Financial Stability Oversight Council and Office of Financial Research

Executive Summary

Background. The Financial Stability Oversight Council (FSOC) was created by the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) and is charged with identifying threats to the financial stability of the United States, promoting market discipline, and responding to emerging risks that could impact the stability of the nation's financial system.¹ The Dodd-Frank Act also created the Council of Inspectors General on Financial Oversight (CIGFO).

CIGFO was established to facilitate information sharing among the Office of Inspector Generals (OIG), to provide a forum for discussing work as it relates to the broader financial sector, and provide oversight of the FSOC.

On April 15, 2011, the *Memorandum of Understanding Regarding the Treatment of Non-public Information Shared Among Parties Pursuant to the Dodd-Frank Wall Street Reform and Consumer Protection Act* (MOU) became effective. The MOU sets forth the parties' understanding with respect to the treatment of non-public information that is obtained or shared among the parties in connection with or related to the functions and activities of FSOC or the Office of Financial Research (OFR). The OFR was also created by the Dodd-Frank Act and has a mission to improve the quality of financial data that is available to policymakers and facilitate a robust and sophisticated analysis of the financial systems.

On December 8, 2011, the CIGFO committee approved the establishment of a CIGFO working group (working group) that was composed of staff from the nine OIG's that comprise CIGFO, whose objectives were to examine the controls and protocols that FSOC and its member agencies employed to ensure FSOC nonpublic information, deliberations, and decisions are properly safeguarded from unauthorized disclosure. That working group conducted a joint audit and reported the results in *Audit of the Financial Stability Oversight Council's Controls over Non-public Information*. The SEC OIG conducted this audit to follow up on deficiencies identified in the joint working group's audit.

¹The United States is also referred to as "nation."

Objectives. To examine the controls and protocols the SEC employs to ensure that sensitive and nonpublic information it collects and exchanges with FSOC, its member agencies and OFR, is properly safeguarded from unauthorized disclosure.

Results. Our audit found that SEC employees and contractors who access the SEC's e-mail system using Outlook Web Access (OWA) are not restricted from saving and uploading sensitive or nonpublic information on non-SEC computers. Consequently, sensitive or nonpublic information could potentially be disclosed to unauthorized persons.

Also, the SEC has not appointed primary information owners to oversee information it receives and shares with FSOC, its member agencies, or OFR. In addition, a protocol for inventorying and ensuring documents are appropriately marked has not been fully developed. As a result, the SEC may be unable to efficiently identify information owners and ensure documents are tracked and marked as appropriate.

Finally, new contractors are not required to take the on-line Security Awareness training on handling sensitive or nonpublic SEC information for up to 30 days after they are approved to work at the SEC and have a network user account. Thus, contractors could unintentionally mishandle or disclose sensitive or nonpublic SEC information. Therefore, new contractors should be required to read and sign the "Rules of the Road" which covers handling nonpublic or sensitive information, prior to being granted access to a network user account. Doing so will aid in the contractor being aware of how to properly handle sensitive or nonpublic SEC information.

Summary of Recommendations. This report contains five recommendations that were designed to improve the SEC's controls over sensitive and nonpublic documents it collects or exchanges with FSOC and OFR. Specifically, we recommended the Office of Information Technology (OIT) develop controls to prevent remote users from saving files accessed using Outlook Web Access to public computers.

Further, the Office of the Chairman should work with OIT to: (1) assign points of contact to serve as information owners, (2) develop a system to identify and track sensitive and nonpublic documents, and (3) devise procedures information owners should use to mark documents according to the sensitivity level, for all sensitive and nonpublic documents that are either provided to, or are received from FSOC or OFR.

Finally, the Office of Acquisitions should work with OIT to ensure new contractors are provided with the *Rules of the Road* to read and sign before they are given access to the SEC's systems.

Management's Response to the Report's Recommendations. OIG provided SEC management with the formal draft report on March 13, 2013. SEC management concurred with all recommendations in this report. OIG considers the report recommendations resolved. However, the recommendations will remain open until documentation is provided to OIG that supports each recommendation has been fully implemented. SEC management's response to each recommendation and OIG's analysis of their responses are presented after each recommendation in the body of this report.

The full version of this report includes information that the SEC considers to be sensitive and proprietary. To create this public version of the report, OIG redacted (blacked out) potentially sensitive, proprietary information from the report.

TABLE OF CONTENTS

Executive Summary	iii
Table of Contents	vii
Background and Objective	1
Background	1
Objective	3
Findings and Recommendations	4
Finding 1: Lack of Remote Access Controls May Put Sensitive and Nonpublic Information at Risk of Unauthorized Disclosure	4
Recommendation 1	7
Finding 2: The SEC's Protocol For Inventorying, Tracking, and Marking Information Collected by and Exchanged With FSOC, its Member Agencies, and OFR Needs Improvement.....	7
Recommendation 2.....	10
Recommendation 3.....	10
Recommendation 4.....	11
Finding 3: New Contractors Are Not Provided Training on Handling Sensitive and Nonpublic Information in a Timely Manner	11
Recommendation 5.....	13
Appendices	
Appendix I: Abbreviations and Definitions.....	14
Appendix II: Scope and Methodology.....	15
Appendix III: Criteria.....	17
Appendix IV: List of Recommendations	18
Appendix V: Management Comments.....	19
Tables	
Table1: Remote Operation Utilities Available at the SEC.....	5

Background and Objectives

Background

The Financial Stability Oversight Council (FSOC) was created by Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) and is charged with identifying threats to the financial stability of the United States (U.S.), promoting market discipline, and responding to emerging risks that could impact the stability of the nation's financial system.²

Among other significant provisions, Dodd-Frank Act created the Council of Inspectors General on Financial Oversight (CIGFO). CIGFO includes Inspectors General from the following nine major Federal government financial entities:

- (1) Board of Governors of the Federal Reserve System.
- (2) Commodity Futures Trading Commission.
- (3) Department of Housing and Urban Development.
- (4) Department of the Treasury.
- (5) Federal Deposit Insurance Corporation (FDIC).
- (6) Federal Housing Finance Agency.
- (7) National Credit Union Administration.
- (8) Securities and Exchange Commission (SEC or Commission).
- (9) Special Inspector General for the Troubled Asset Relief Program.

CIGFO was established to:

- (1) facilitate information sharing among the Office of Inspector Generals (OIG);
- (2) provide a forum for discussing work as it relates to the broader financial sector; and
- (3) provide oversight of the FSOC.

On April 15, 2011, the *Memorandum of Understanding Regarding the Treatment of Non-public Information Shared Among Parties Pursuant to the Dodd-Frank-Wall Street Reform and Consumer Protection Act* (MOU) became effective. The MOU was signed by SEC and 15 designated parties,³ to include other federal financial regulatory agencies.⁴ The MOU sets forth the parties' understanding

²The United States is also referred to as "nation."

³ Designated "Parties" are also referred to as member agencies. These "Parties" are comprised of the Office of Financial Research (OFR), FSOC, and its member agencies.

⁴ Financial regulatory agencies are also referred to as financial entities in the MOU.

with respect to the treatment of nonpublic information that is obtained or shared among the parties in connection with, or related to the functions and activities of FSOC or the Office of Financial Research (OFR).⁵ The OFR was established by the Dodd-Frank Wall Street Reform and Consumer Protection Act. Its mission is to improve the quality of financial data that is available to policymakers and to facilitate a robust and sophisticated analysis of the financial systems.

The MOU defines nonpublic information as:

any data, information, or reports submitted, received or shared among the Parties in connection with or related to the functions and activities of the FSOC or the Office of Financial Research.⁶

Also, the MOU provides the terms and agreements as determined by the signing parties. The MOU parties agreed not to disclose information that is shared between the parties without first receiving written consent from the providing party.

The SEC defines nonpublic information as:

information generated by or in the possession of the SEC that is commercially valuable, market sensitive, proprietary, related to an enforcement or examination matter, subject to privilege, or otherwise deemed nonpublic by a division director or office head, and not otherwise available to the public. This policy applies to nonpublic information in any form including documents, electronic mail, computer files, conversations, and audio or video recordings.⁷

On December 8, 2011, the CIGFO Committee approved the establishment of a CIGFO working group (working group) composed of staff from the nine OIG's that comprise CIGFO, whose objectives were to examine the controls and protocols that FSOC and its member agencies employed to ensure FSOC nonpublic information, deliberations, and decisions are properly safeguarded from unauthorized disclosure. To accomplish its objective, the working group conducted a joint audit of the major federal government financial entity's business practices related to the industry standards and practices that are established in the National Institute of Technology (NIST) special publications.⁸ Specifically, in March 2012, the working group members conducted an audit of their respective agency's management and internal controls over sensitive and

⁵The MOU was effective on April 15, 2011, and the SEC signed it on May 2, 2011.

⁶ *Memorandum of Understanding Regarding the Treatment of Non-public Information Shared Among Parties Pursuant to the Dodd-Frank Wall Street Reform and Consumer Protection Act*, effective April 15, 2011, p. 1.

⁷ SECR 23-2a, Security-Safeguarding Non-Public Information, January 21, 2000, p. 1.

⁸ The National Institute of Technology (NIST) Special Publications consist of a series of reports on NIST research, guidelines, and outreach efforts in information system security.

proprietary (non-public) information that was collected by and exchanged with FSOC, its member agencies, and OFR. The audit was spearheaded by FDIC OIG, who met regularly with working group members. Working group members used a standardized audit program to ensure audit steps and testing among OIG's was consistent.

Findings for the joint audit were incorporated into a consolidated report, *Audit of the Financial Stability Oversight Council's Controls over Non-public Information*, which was issued on June 22, 2012, to the Chairman of FSOC. While the report did not make any recommendations, it identified differences in how FSOC and its member agencies' mark nonpublic information. For example, nonpublic information marked as "sensitive" in one agency is marked as "restricted" in another agency. In addition, the report identified control differences in how non-public information is handled in areas related to oral communication, supplemental prohibition on financial interest, contractor confidentiality and nondisclosure, encryption, and protocol for tracking information exchange.⁹

Purpose. OIG conducted this audit to follow up with the deficiencies we identified during the joint audit. Specifically, our purpose was to further assess the SEC's controls over sensitive and nonpublic information that is collected by and exchanged with FSOC, its member agencies and OFR, and determine adherence to the MOU requirements for handling sensitive and non-public information.¹⁰ Our audit did include inquiries regarding unauthorized disclosure of sensitive or nonpublic information.

Objective

To examine the controls and protocols the SEC employs to ensure that sensitive and nonpublic information it collects and exchanges with FSOC, its member agencies and OFR, is properly safeguarded from unauthorized disclosure.

⁹ *Audit of the Financial Stability Oversight Council's Controls over Non-public Information*, Report to the Financial Stability Oversight Council and the Congress, June 22, 2012, p. 9.

¹⁰ OIT defines sensitive as "Information about a company or individual that has been collected by the SEC but is not for public disclosure. In general, all such data, which are categorized as either "Non-Public (SEC Restricted)" or "Non-Public (SEC Use Only)," shall be masked."

Findings and Recommendations

Finding 1: Lack of Remote Access Controls May Put Sensitive and Nonpublic Information at Risk of Unauthorized Disclosure

SEC employees and contractors accessing SEC's e-mail system using Outlook Web Access (OWA) are not restricted from saving and uploading sensitive or nonpublic information on non-SEC computers. Consequently, sensitive or nonpublic information could potentially be disclosed to unauthorized persons.¹¹

The Office of Information Technology's (OIT) has issued policy prohibiting SEC network users (employees and contractors) from saving or uploading sensitive or nonpublic information onto non-SEC computers, unless the computer is equipped with SEC-approved remote operation utilities. Currently, the SEC does not have any controls that restrict or prevent employees and contractors who use OWA from uploading or saving information which includes sensitive/nonpublic, to a non-SEC computer. The onus is on SEC network users to comply with OIT's policy.

OIT's *Rules of the Road, Rule #7: Don't Transmit Non-public or Sensitive Information over Non-secure Systems* states,¹²

Users of the SEC network and automated systems must also understand that sensitive or nonpublic information may NOT be processed on non-SEC workstations unless such workstations are equipped with SEC-approved remote operation utilities, such as [REDACTED] software.

In addition, OIT's Implementing Instruction 24-04.02.01(01.0) *Sensitive Data Protection*, issued April 6, 2006 states,

The SEC may take appropriate action to ensure that unauthorized individuals cannot read, copy, alter, or steal printed or electronic SEC sensitive information.¹³

¹¹ SEC personnel include employees, detailees, and interns and are referred to as "SEC staff."

¹² The *Rules of the Road* apply to all SEC staff and contractors.

¹³ Implementing Instruction 24-04.02.01(01.0) *Sensitive Data Protection*, Section 5.d(5), April 6, 2006.

Currently, the Commission allows employees and contractors who handle sensitive and nonpublic information to work at offsite locations using non-SEC computers to access the SEC's network. This is done using approved, secured remote operation utilities such as OWA, SEC's remote electronic terminals portal [REDACTED], Virtual Private Network (VPN), or the [REDACTED]. Full descriptions of these remote operation utilities are identified below in Table 1. Employees and contractors can use these utilities to connect to the agency's network from a SEC-issued desktop/laptop or using a non-SEC computer such as a public, company-owned, or personal desktop/laptop.

Table 1: Remote Operation Utilities Available at the SEC

Remote Operation Utilities	Description
Outlook Web Access	A web-based application that allows users to check e-mail from both SEC-issued and non-SEC issued computers.
[REDACTED]	[REDACTED]
VPN	A remote access solution that offers a secure solution to access SEC e-mail, network drives, and applications using a SEC-issued computer.
[REDACTED]	[REDACTED]

Source: OIG Generated.

SEC-issued computers are equipped with remote operation utilities and are configured to meet OIT's defined baseline security requirements. Also, they have parameters that are designed to protect data that is saved on the computer from unauthorized disclosure. These computers have controls and protections (baseline security requirements) such as, anti-virus, anti-malware, firewalls, intrusion detection, and hard disk encryption that aids in preventing unauthorized access to SEC data.

In contrast, non-SEC computers which include public computers, are configured to meet the computer owner's requirements, which likely do not meet OIT's defined baseline security requirements for protecting SEC data. Consequently, these computers may not have adequate controls and protections (e.g., encryption, anti-virus, anti-spyware) to prevent unauthorized access of nonpublic SEC information or the information from being disclosed to unauthorized persons.

¹⁴ The Commission employs four remote operation utilities that provide similar, but somewhat different attributes. These remote operation utilities serve as alternative solutions SEC personnel can use to access the SEC's network in the event one of the four solutions becomes unstable or is inoperable.

Employees and contractors can remotely connect onto the SEC's network via SEC-issued computers by using OWA, [REDACTED], or VPN. Also, they can remotely connect to the network via non-SEC computers by using OWA, [REDACTED]. [REDACTED] allow staff using a non-SEC computer to save and upload files directly to the SEC's network, but the files cannot be uploaded and saved to the computer. Conversely, agency network users who remotely access their e-mail via a non-SEC computer using OWA can save and upload e-mails and attachments, which could include sensitive or nonpublic information, to the non-SEC computer.

OWA does not have controls to prevent users accessing the agency's network from non-SEC computers from saving and uploading information onto a non-SEC computer. As a result, sensitive or nonpublic information could potentially be saved to a non-SEC computer. Therefore, there is a risk that an unauthorized person could gain access to sensitive or nonpublic SEC information if the user saved files that were obtained using OWA onto a non-SEC computer.

Though the SEC has policies and procedures regarding handling and safeguarding sensitive/nonpublic information and requires staff to attend annual security awareness training, this information could potentially be disclosed because SEC employees and contractors have the ability to save and upload documents onto non-SEC computers when using OWA. For example, if a user remotely accesses the SEC network using OWA from a hotel computer and downloads sensitive information or nonpublic from their e-mail to the hotel's computer and does not remove or delete it from the hotel computer, the file can be accessed by subsequent users. Therefore, there is a risk that sensitive or nonpublic SEC information can potentially be seen, read, copied, altered, printed, or stolen by unauthorized persons.

Conclusion. The ability for SEC personnel who access SEC e-mails using OWA to save and upload information onto non-SEC computers is an internal control weakness that should be further reviewed to assess risk to the Commission. Implementing Instruction 24-04.02.01 (01.0) requires that appropriate action is taken to ensure "unauthorized individuals cannot read, copy, alter, print, or steal electronic SEC sensitive information."¹⁵ However, by not having a control in place that restricts or prevents SEC personnel using OWA from saving or uploading documents onto a non-SEC computer, sensitive or non-public information could potentially be disclosed to unauthorized persons. OIT should ensure controls are developed for OWA users that are consistent with [REDACTED] that disallow files from being uploaded and saved onto non-SEC computers.

¹⁵ Implementing Instruction 24-04.02.01(01.0) *Sensitive Data Protection*, Section 5.d(5), April 6, 2006.

Recommendation 1:

The Office of Information Technology should develop controls that prevent remote users from saving files accessed using Outlook Web Access to public computers.

Management Comments. OIT concurred with this recommendation. See Appendix V for management's full comments.

OIG Analysis. We are pleased that OIT concurred with this recommendation. OIG considers this recommendation resolved. However, this recommendation will remain open until documentation is provided to OIG that supports it has been fully implemented.

Finding 2: The SEC's Protocol for Inventorying, Tracking, and Marking Information Collected by and Exchanged with FSOC, its Member Agencies, and OFR Needs Improvement

The SEC has not appointed a primary information owner to oversee information it receives and shares with FSOC, its member agencies, or OFR. In addition, a protocol for inventorying and ensuring that information is appropriately marked has not been fully developed. As a result, the SEC may be unable to readily identify information owners and ensure documents are tracked and marked as appropriate.

The SEC does not have any primary points of contact (POC) to oversee sensitive and nonpublic information that is requested, provided, or received to/from its parties to the FSOC MOU. Additionally, the SEC has not fully developed a protocol for inventorying, tracking, and ensuring that sensitive/nonpublic information that is shared among the FSOC, its member agencies, and the OFR is appropriately marked for classification purposes and to assure the confidentiality of the information is maintained in accordance with the MOUs terms. OIG was informed the SEC exchanges sensitive or nonpublic information with FSOC using a secured e-mail portal.

The Commission's policy for handling and marking sensitive information that is obtained from third parties. Specifically, the policy II 24-04.02.01 (01.0) states,

...all 'Non-Public (SEC Restricted)' or 'Non-Public (SEC Use Only)' must be labeled in accordance with the SEC's guidance for labeling or marking, handling, and safeguarding such information as provided in SECR 23-2a.¹⁶ In the course of normal business activities, the SEC often takes possession of third-party unclassified sensitive information. Whenever a non-disclosure agreement (NDA) has been signed, an internal SEC information owner should be assigned for information so received. ...This third-party information must be labeled with the appropriate data category and treated as though it was 'Non-Public (SEC Restricted)' or 'Non-Public (SEC Use Only)' internal information with the same security categorization.¹⁷

...sensitive information [to] be marked as appropriate by the primary information user. Internal/External labeling is required for all sensitive material and may be in the form of special handling instructions, classification, or control logging information such as serial/controls numbers or bar codes.¹⁸

To ensure full compliance with its MOU with FSOC, the SEC must be able to track the information it receives and exchanges with the MOU parties. While SEC policy requires information owners are assigned to receive information from third parties, the SEC has not designated a primary person or persons to serve in this capacity for FSOC purposes. Although a primary POC has not been designated, Commission employees who have collected or have exchanged data with FSOC, member agencies or OFR, have individually assumed responsibility for sensitive/non-public data. The current process lacks sufficient controls and accountability for tracking who has accessed, collected, or exchanged data with FSOC.¹⁹

Our audit also found that the SEC does not have a formal protocol or procedures related to the FSOC's function to inventory, track, and ensure sensitive and non-public information that is shared or received with FSOC, its member agencies, and OFR is appropriately marked for classification purposes. SEC information owners informed us they primarily rely on the secured e-mail portal to inventory and track information, but do not readily "mark" the data they receive from the FSOC, its member agencies, or OFR. Hence, the email portal only provides an

¹⁶ SECR 23-2a is an SEC Administrative Regulation entitled Security: Safeguarding Non-Public Information (January 21, 2000) establishes general policies and procedures that are designed to enhance the management controls for safeguarding non-public information.

¹⁷ II 24-04.02.01, *Sensitive Data Protection*, April 6, 2006, p. 2 of 8, Section 5.b(4).

¹⁸ *Ibid*, 5.d(2).

¹⁹ Commission staff located in the Division of Trading and Markets; Division of Risk, Strategy, and Financial Innovation; Division of Investment Management, Office of General Counsel; and the Office of the Chairman are responsible for handling data collected and exchanged with FSOC, its member agencies, and OFR.

inventory of e-mails that are exchanged between the SEC information owners, FSOC, member agencies, or OFR. Consequently, the e-mail portal cannot track information that is collected or exchanged through other avenues such as CD's, thumb drives, meetings, conferences/seminars, etc. Additionally, when an SEC information owner terminates their employment with the Commission, their e-mails from the portal may need to be retrieved to identify FSOC, its member agencies, and OFR sensitive or nonpublic information. This process could prove to be time consuming. Using the secured email portal lacks sufficient controls over information exchanged between the SEC and FSOC that is outside of the e-mail system. Further, the secured e-mail system lacks efficient controls for continuity purposes.

Furthermore, our audit found that information owners who receive sensitive or nonpublic information (paper or electronic documents) from FSOC, its member agencies, or OFR, are not marking the documents in accordance with II 24-04.02.01 (01.0), or in a timely manner. Ensuring documents are properly marked when initially received increases the likelihood that the confidentiality of the information collected and exchanged with the various parties is being maintained and handled appropriately.

OIG determined that the Commission's current practices limit its ability to ensure information owners readily track and identify the universe of sensitive and non-public information the SEC receives and exchanges with FSOC, its member agencies or OFR because the SEC does not have a primary or alternate POC and relies on its secured email portal to track exchanged or collected information, they cannot readily identify its universe of information that is not transmitted via email and assure paper documents are appropriately "marked" in a timely manner. Therefore, the SEC's ability to readily identify information owners (e.g., providing or receiving party), ensure documents are properly marked and handled, or are authorized for release and are easily identified for third party SEC requests for information, cannot be assured.

We further found the SEC is collecting information using the "Reporting Form for Investment Advisers to Private Funds and Certain Commodity Pool Operators and Commodity Trading Advisors" (Form PF). The SEC adopted this form on October 31, 2011 to provide information to FSOC to assist in assessing systemic risk in the U.S. financial system. The Division of Investment Management (IM) uses the Form PF to collect reporting information from investment advisers to private funds and certain commodity pool operators and commodity trading advisers. Information collected using the Form PF is provided to OFR, on behalf of FSOC. IM's staff informed OIG it has worked with OFR to establish Form PF principles for data sharing that governs OFR's use of the information.

Though the Commission has information owners, primary POCs should be appointed to ensure the SEC has designated staff who provide oversight for information the SEC receives and exchanges with FSOC, its member agencies, or OFR. Further, the SEC should develop a viable system such as a centralized repository, to track the universe of information it receives and exchanges with the parties, to include information that is contained in secured emails, CD's, thumb drives, external drives, and at meetings, conferences, or seminars. The primary POCs should further ensure information owners appropriately "mark" the documents in a timely manner.

Adopting these changes will better align the SEC with the MOU's requirements to be able to track information it receives and exchanges with FSOC. Further, it will align the SEC with II 24-04.02.01 (01.0), which requires an information owner is assigned to receive information from third parties.

Appointing POCs and developing a viable system or protocol are crucial to the SEC's ability to efficiently identify all information that has been requested, provided, or received to/from the parties, as well as the source/owners of the information will result in the SEC having better internal controls over these areas.

Recommendation 2:

The Office of the Chairman in coordination with the Office of Information Technology should assign points of contact to serve as information owners for sensitive and nonpublic documents provided to, or received from the Financial Stability Oversight Council (FSOC), the Office of Financial Research or FSOC's member agencies.

Management Comments. The Chairman's office concurred with this recommendation. See Appendix V for management's full comments.

OIG Analysis. We are pleased the Chairman's office concurred with this recommendation. OIG considers this recommendation resolved. However, this recommendation will remain open until documentation is provided to OIG that supports it has been fully implemented.

Recommendation 3:

The Office of the Chairman in coordination with the Office of Information Technology should ensure a system or protocols are developed to identify and track all sensitive and nonpublic information provided to, or received from the Financial Stability Oversight Council (FSOC), the Office of Financial Research or FSOC's member agencies. This system should track information owner's name, date information is received/sent, who the

information is sent to/received from, and media used (e.g., CDs, thumb drives, etc.).

Management Comments. The Chairman's office concurred with this recommendation. See Appendix V for management's full comments.

OIG Analysis. We are pleased the Chairman's office concurred with this recommendation. OIG considers this recommendation resolved. However, this recommendation will remain open until documentation is provided to OIG that supports it has been fully implemented.

Recommendation 4:

The Office of the Chairman in coordination with the Office of Information Technology should ensure documented procedures are developed to assure individuals that serve as information owners for sensitive and non-public information provided to, or received from the Financial Stability Oversight Council (FSOC), the Office of Financial Research or FSOC's member agencies, properly mark the documents (or files containing documents) according to the sensitivity level.

Management Comments. The Chairman's office concurred with this recommendation. See Appendix V for management's full comments.

OIG Analysis. We are pleased the Chairman's office concurred with this recommendation. OIG considers this recommendation resolved. However, this recommendation will remain open until documentation is provided to OIG that supports it has been fully implemented.

Finding 3: New Contractors Are Not Provided Training on Handling Sensitive and Nonpublic Information in a Timely Manner

Newly assigned contractors working with FSOC, its member agencies, and the OFR information are not promptly and adequately trained on how to handle sensitive or nonpublic information. As a result, a contractor could unintentionally mishandle or disclose nonpublic information the SEC collects and exchanges with the parties.

The SEC employs contractors who could potentially work with nonpublic

information FSOC, its member agencies, and OFR.²⁰ Contractors have the same security controls requirements over sensitive and nonpublic information that applies to SEC employees. New contractors are required to read and sign an NDA before receiving approval to work at the SEC. However, they are not required to immediately complete the Security Awareness training which covers OIT's "Rules of the Road," and "Prohibited Practices Concerning Non-Public Information," or sign a compliance statement acknowledging they understand and will comply with the SEC's "Rules of the Road." According to OIT, after signing the NDA, the contractor has an understanding of how to properly handle nonpublic information and believes they are then aware of non-disclosure requirements covered in the NDA.²¹

The NDA includes language stating the contractor agrees "not to disclose to any unauthorized person any confidential or nonpublic documents or information."²² While the NDA defines confidential and nonpublic information and informs the contractor they should not disclose "confidential or non-public information in any form, including documents, electronic mail, computer files, conversations, and audio or video recordings," it does not include the SEC's requirements for handling confidential or nonpublic information. Further, the NDA does not include language that describes what the SEC defines as prohibited practices concerning nonpublic information. For example, a prohibited practice concerning nonpublic information that is outlined in the *Rules of the Road*, Rule #7 states,

DO NOT transmit non-public information or sensitive data through the Internet or via e-mail, unless you have encrypted it using the SEC's approved encryption software. DO NOT store or transmit non-public information or sensitive data on SEC IT resources without proper protection/encryption.²³

New SEC employees are required to complete on-line Security Awareness training within 30 days (15 days for interns) after receiving their user account. Further, new SEC employees receive training on handling sensitive, nonpublic information during the new employees' orientation. This training informs new employees that sensitive/nonpublic information cannot be transmitted external to the SEC unless it is encrypted. In addition, new employees are given a copy of the *Rules of the Road* to read and sign indicating they will adhere to the policy.

Unlike employees, new contractors also are not required to take the on-line Security Awareness training on how to handle sensitive or nonpublic information for up to 30 days after they are approved to work at the SEC and have received a

²⁰ The SEC uses contractors to support the agency in achieving its mission.

²¹ The Rules of the Road are available to all network users on the SEC Insider intranet.

²² Employee non-disclosure agreement, Attachment J-2, Section C.

²³ SEC's *Rules of the Road*, Rule #7.

network user account. This time gap increases the likelihood the contractor could unintentionally mishandle or disclose sensitive/nonpublic information.

Although the Office of Acquisitions (OA) asserts they provided training to Contracting Officer's Representatives regarding the requirement to have new contractors read and sign the *Rules of the Road* before starting work at the SEC, we were not provided evidence this process has started. OIT informed us they are working with OA regarding this matter.

OIG determined that upon being approved to work on a SEC contract, contractors should be given a copy of the *Rules of the Road* to read and sign indicating they will adhere to this policy which covers handling sensitive and nonpublic information.

Recommendation 5:

The Office of Acquisitions, in coordination with the Office of Information Technology should ensure that new contractors with the Commission are given a copy of the "Rules of the Road" to read and sign indicating they will adhere to the policy before they are given access to the agency's systems.

Management Comments. The Chairman's office concurred with this recommendation. See Appendix V for management's full comments.

OIG Analysis. We are pleased the Chairman's office concurred with this recommendation. OIG considers this recommendation resolved. However, this recommendation will remain open until documentation is provided to OIG that supports it has been fully implemented.

Abbreviations and Definitions

CIGFO	Council of Inspectors General on Financial Oversight
██████	██
Dodd-Frank Act	Dodd-Frank Wall Street Reform and Consumer Protection Act
FDIC	Federal Deposit Insurance Corporation
Form PF	Reporting Form for Investment Advisers to Private Funds and Certain Commodity Pool Operators and Commodity Trading Advisors
FSOC	Financial Stability Oversight Council
██████	██
IG	Inspector General
IM	Office of Investment Management
MOU	Memorandum of Understanding “Regarding the Treatment of Non-public Information Shared Among Parties Pursuant to the Dodd-Frank Wall Street Reform and Consumer Protection Act”
NDA	Non-Disclosure Agreement
NIST	National Institute of Standards and Technology
OA	Office of Acquisitions
OFR	Office of Financial Research
OIG	Office of Inspector General
OIT	Office of Information Technology
OWA	Outlook Web Access
Parties	Consist of the Financial Stability Oversight Council and the Office of Financial Research
POC	Point of Contact
SEC or Commission	U.S. Securities and Exchange Commission
SEC Information Owners	Groups identified in certain offices and divisions who serve as Financial Stability Oversight Council and the Office of Financial Research information owners.
SEC Staff	SEC employees, detailees, and interns
U.S.	United States
VPN	Virtual Private Network
Working Group	CIGFO Working Group

Scope and Methodology

The full version of this report includes information that the SEC considers to be sensitive and proprietary. To create this public version of the report, OIG redacted (blacked out) potentially sensitive, proprietary information from the report.

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

Scope. We conducted our fieldwork from February 2012 to September 2012, and reviewed the SEC's management and internal controls over sensitive and nonpublic information collected by and exchanged with the FSOC, its member agencies, and the OFR. The scope of this audit included a survey of the SEC's controls and protocols the SEC applied to safeguard from unauthorized disclosure and track sensitive and nonpublic information that was collected by or exchanged with FSOC, its member agencies, and the OFR. The scope of the audit did not include an inquiry into whether there was any unauthorized disclosure of confidential information.

Methodology. To meet the objective of examining the controls and protocols the SEC employs to ensure that FSOC, its member agencies, and the sensitive and nonpublic information, including deliberations, and decisions, were properly safeguarded against unauthorized disclosure. We distributed a survey to and conducted interviews with select personnel in the Office of the Chairman, Office of General Counsel, Office of Ethics, OIT, Division of Trading and Markets, IM, and the Division of Risk, Strategy, and Financial Innovation who had responsibilities related to safeguarding sensitive and proprietary information collected by and exchanged with the FSOC, its member agencies and the OFR. In addition, we reviewed SEC's regulations and policies and procedures related to safeguarding sensitive and proprietary information. We also reviewed relevant federal regulations, laws, and guidance.

Management Controls. We did not assess SEC's management controls because it did not pertain to the objectives of this audit. We reviewed existing controls the Commission considered specific to the Working Group's Questionnaire. To thoroughly understand the Commission's management controls pertaining to its policies and procedures and methods of operation, we

relied on information the agency provided OIG as supporting documentation to the questionnaire and during follow-up interviews we conducted with Commission personnel.

Use of Computer-Processed Data. We did not assess the reliability of any computer-processed data because it did not pertain to the objectives of this audit. Further, we did not perform any tests on the general or application controls over SEC's automated systems because such tests were not within the scope of our work. The information that was retrieved from these systems, as well as the requested documentation provided to us, was sufficient, reliable, and adequate to use in meeting our stated objectives.

Prior Audit Coverage

- OIG report *2011 Annual FISMA Executive Summary Report*, Report No. 501, February 2, 2012. This report contained 13 recommendations to strengthen the SEC's controls over information security.
- OIG report *Assessment of SEC's Continuous Monitoring Program*, Report No. 497, dated August 11, 2011. This report contained 13 recommendations to strengthen OIT's continuous monitoring program.
- OIG report *Assessment of the SEC's Privacy Program*, Report No. 485, September 29, 2010. This report contained 20 recommendations to improve the Commission's security posture for protecting Personally Identifiable Information.
- OIG report *Evaluation of the SEC Encryption Program*, Report No. 476, March 26, 2010. This report contained three recommendations to improve the Commission's encryption program.
- OIG report *Evaluation of the SEC Privacy Program*, Report No. 475, March 26, 2010. This report contained one recommendation to improve the Commission's privacy program.

Criteria

Dodd-Frank Wall Street Reform and Consumer Protection Act, Public Law No. 111-203, July 21, 2010. Reformed the financial regulatory system, including how financial regulatory agencies such as the SEC operate, and mandated that the SEC undertake a significant number of studies and rulemakings, including regulatory initiatives addressing derivatives; asset securitization; credit rating agencies; hedge funds, private equity funds, and venture capital funds; municipal securities; clearing agencies; and corporate governance and executive compensation. Created CIGFO.

Memorandum of Understanding Regarding the Treatment of Non-public Information Shared Among Parties Pursuant to the Dodd-Frank Wall Street Reform and Consumer Protection Act, April 15, 2011. Sets forth the parties' understanding with respect to the treatment of nonpublic information that is obtained or shared among the parties in connection with or related to the functions and activities of FSOC or OFR.

SECR 23-2a, Security-Safeguarding Non-Public Information, January 21, 2000. Establishes general policies and procedures for safeguarding nonpublic information.

SECR 24-04-A01, Rules of the Road. Provides guidance on the handling and safeguarding of nonpublic or sensitive information, including its transmission and storage.

Implementing Instruction 24-04.02.01(01.0), Sensitive Data Protection, April 6, 2006. Provides a uniform process for defining SEC's sensitive information for the purpose of information technology security and management.

NIST Special Publication 800-53, Revision 3, Recommended Security Controls for Federal Information Systems and Organizations. Provides guidance related to the steps in the risk management framework that address security control section.

List of Recommendations

Recommendation 1:

The Office of Information Technology should develop controls that prevent remote users from saving files accessed using Outlook Web Access to public computers.

Recommendation 2:

The Office of the Chairman in coordination with the Office of Information Technology should assign points of contact to serve as information owners for sensitive and nonpublic documents provided to, or received from the Financial Stability Oversight Council (FSOC), the Office of Financial Research or FSOC's member agencies.

Recommendation 3:

The Office of the Chairman in coordination with the Office of Information Technology should ensure a system or protocols are developed to identify and track all sensitive and nonpublic information provided to, or received from the Financial Stability Oversight Council (FSOC), the Office of Financial Research or FSOC's member agencies. This system should track information owner's name, date information is received/sent, who the information is sent to/received from, and media used (e.g., CDs, thumb drives, etc.).

Recommendation 4:

The Office of the Chairman in coordination with the Office of Information Technology should ensure documented procedures are developed to assure individuals that serve as information owners for sensitive and non-public information provided to, or received from the Financial Stability Oversight Council (FSOC), the Office of Financial Research or FSOC's member agencies, properly mark the documents (or files containing documents) according to the sensitivity level.

Recommendation 5:

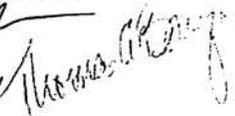
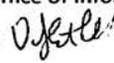
The Office of Acquisitions, in coordination with the Office of Information Technology should ensure that new contractors with the Commission are given a copy of the "Rules of the Road" to read and sign indicating they will adhere to the policy before they are given access to the agency's systems.

Management Comments

MEMORANDUM

March 22, 2013

To: Jacqueline Wilson, Assistant Inspector General for Audits, Office of Inspector General

From: Erica Williams, Deputy Chief of Staff, Office of the Chairman 
 Thomas A. Bayer, Chief Information Officer, Office of Information Technology 
 Vance Cathell, Director, Office of Acquisitions 

Subject: Management Response, *SEC's Controls Over Sensitive/Non-Public Information Collected and Exchanged With the Financial Stability Oversight Council and Office of Financial Research*, Report No. 509

Thank you for the opportunity to comment on the recommendations in the report annotated above, as we work together to protect the sensitive and non-public nature of information collected by and exchanged with the Financial Stability Oversight Council (FSOC) and Office of Financial Research (OFR). The scope of the Office of Inspector General's audit included a survey of the SEC's controls and protocols the SEC applied to safeguard from unauthorized disclosure and track sensitive and non-public information that was collected by or exchanged with FSOC, its member agencies and the OFR. The scope of the audit did not include an inquiry into whether there was any unauthorized disclosure of confidential information. We appreciate the Office of Inspector General's insights on the SEC's controls and protocols and are providing the official response from the Offices of the Chairman, Information Technology, and Acquisitions.

Recommendation 1: "The Office of Information Technology should develop controls that prevent remote users from saving files accessed using Outlook Web Access to public computers."

Management Response: The Office of Information Technology concurs and will evaluate blocking attachments through Outlook Web Access (OWA) on public computers and educating users on the difference between SEC-owned, private and public computers and the respective security risks through the annual Security Awareness Training

Recommendation 2: "The Office of the Chairman in coordination with the Office of Information Technology should assign points of contact to serve as information owners for sensitive and nonpublic documents provided to, or received from the Financial Stability Oversight Council (FSOC), the Office of Financial Research or FSOC's member agencies."

Management Response: The Office of the Chairman concurs and will assign points of contact.

Recommendation 3: "The Office of the Chairman in coordination with the Office of Information Technology should ensure a system is developed to identify and track all sensitive and nonpublic information provided to, or received from the Financial Stability Oversight Council (FSOC), the Office of Financial Research or FSOC's member agencies. This system should track information owner's name, date information is received/sent, who the information is sent to/received from, and media used (e.g., CDs, thumb drives, etc.)."

Management Response: The Office of the Chairman concurs. The SEC FSOC point of contact will work with the FSOC OFR member agencies to come up with a consensus on data tracking when exchanging data within the FSOC OFR member agencies. The Office of the Chairman will ensure a system for tracking sensitive FSOC-related information is established consistent with the signed Memorandum of Understanding among member agencies and consensus procedures.

Recommendation 4: "The Office of the Chairman in coordination with the Office of Information Technology should ensure documented procedures are developed to assure individuals that serve as information owners for sensitive and non-public information provided to, or received from the Financial Stability Oversight Council (FSOC), the Office of Financial Research or FSOC's member agencies, properly mark the documents (or files containing documents) according to the sensitivity level."

Management Response: The Office of the Chairman concurs. The SEC FSOC point of contact will work with the FSOC OFR member agencies to come up with a consensus on marking files or documents. OIT will assist the FSOC point of contact in developing internal procedures. The FSOC Data Committee Working Group is engaged in discussions concerning the proper labeling and handling of FSOC data.

Recommendation 5: "The Office of Acquisitions, in coordination with the Office of Information Technology should ensure that new contractors with the Commission are given a copy of the "Rules of the Road" to read and sign indicating they will adhere to the policy before they are given access to the agency's systems."

Management Response: The Office of Acquisitions concurs. The Office of Acquisitions is committed to supporting the Office of Information Technology in improving controls over SEC information. We will coordinate with OIT to implement your recommendation.

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