Audit of the Financial Stability Oversight Council's Controls over Non-public Information

Report to the Financial Stability Oversight Council and the Congress

Prepared by
The Council of Inspectors General
on Financial Oversight

June 2012

Abbreviations and Acronyms

Bylaws	Rules of Organization of the Financial Stability Oversight Council
CIDI	Covered Insured Depository Institution
CIGFO	Council of Inspectors General on Financial Oversight
Dodd-Frank Act	Dodd-Frank Wall Street Reform and Consumer Protection Act
FFIEC	Federal Financial Institutions Examination Council
FISMA	Federal Information Security Management Act
FSOC or Council	Financial Stability Oversight Council
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
NIST	National Institute of Standards and Technology
OFR	Office of Financial Research
OIG	Office of Inspector General
Transparency Policy	Transparency Policy for the Financial Stability Oversight Council
Treasury	Department of the Treasury

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

June 22, 2012

The Honorable Timothy Geithner
Chair, Financial Stability Oversight Council
Washington D.C. 20220

Dear Mr. Chairman:

I am pleased to present to you a copy of the first Council of Inspectors General on Financial Oversight (CIGFO) report titled, *Audit of the Financial Stability Oversight Council's Controls over Non-public Information*.

Given the importance of protecting Financial Stability Oversight Council (FSOC) information, on December 8, 2011 Jon Rymer, Inspector General, Federal Deposit Insurance Corporation, and Vice Chair, CIGFO, proposed convening a working group to examine FSOC's controls for ensuring that its non-public information is properly safeguarded from unauthorized disclosure. The proposal was approved, and a CIGFO Working Group completed a review.

This CIGFO report encourages FSOC to continue its ongoing efforts, further examine the issues raised in our report with respect to information control differences, and prepare for possible security upgrades as economic conditions change and new threats to the stability of the United States financial system emerge.

I would like to take this opportunity to thank the Working Group members responsible for this report, each of whom is listed in Appendix III. In addition, I appreciate the support of the FSOC Member agencies' staff as well, especially those Treasury officials who assisted with this effort.

The CIGFO looks forward to working with you on this and other issues. In accordance with the Dodd-Frank Act, CIGFO is providing this report to the Congress.

Sincerely,

Eric M. Thorson
Chair
Council of Inspectors General
on Financial Oversight

Enclosure(s)

Executive Summary

Why and How We Conducted the Review

The landmark Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) created a comprehensive new regulatory and resolution framework designed to avoid the severe consequences of financial instability. The Dodd-Frank Act created, among other things, the Council of Inspectors General on Financial Oversight (CIGFO). One of CIGFO's statutory functions is to provide oversight of the Financial Stability Oversight Council (FSOC or Council). Specifically, the law grants CIGFO the authority to convene a working group, by a majority vote, for the purpose of evaluating the effectiveness and internal operations of FSOC.

FSOC is charged with identifying risks to the nation's financial stability, promoting market discipline, and responding to emerging threats to the stability of the nation's financial system. These responsibilities are significant, and any decisions coming from FSOC could impact the U.S. financial system and have repercussions for global financial institutions and systems. The information that FSOC collects, deliberations it has, and decisions it implements must be managed and controlled.

FSOC is chaired by the Secretary of the Treasury. Within the Department of the Treasury (Treasury), a dedicated policy office, led by a Deputy Assistant Secretary, functions as the FSOC Secretariat and serves as a mechanism to bring issues to the Council quickly through a coordinated process. The 10 voting members of FSOC provide a federal regulatory perspective and an independent insurance expert's view. The five nonvoting members offer different insights as state-level representatives from bank, securities, and insurance regulators or as the directors of the new offices within Treasury established by the Dodd-Frank Act – the Office of Financial Research (OFR) and the Federal Insurance Office.

On December 8, 2011, Jon Rymer, Inspector General, Federal Deposit Insurance Corporation, and Vice Chair, CIGFO, proposed convening a working group to examine FSOC's controls and protocols for ensuring that its non-public information, deliberations, and decisions are properly safeguarded from unauthorized disclosure. The proposal was approved and the CIGFO Working Group was formed.

To accomplish its objective, the CIGFO Working Group identified the controls and protocols in place at each of the FSOC federal agency members to safeguard FSOC information and the manner in which FSOC as a whole safeguards information from unauthorized disclosure. The audit was intended to capture the current information exchange environment as well as identify any potential risk or gaps in controls over information exchange and bring those issues to the attention of FSOC as it continues to carry out its mission. We did not include the FSOC independent and state members in this review.

What We Learned

FSOC understands that its ability to safely share information among its members is critical to its effectiveness. To date, a limited amount of non-public information, primarily information related to rulemakings, meetings, and other routine activities, has been exchanged among Council members. Joint work among FSOC members to identify and mitigate risks to financial stability has begun, and data

sharing will expand as OFR continues to build its capacity. To protect the exchange of information, the Council members entered into a memorandum of understanding governing the treatment of non-public information that relies on each agency to use the controls in place at their respective agencies.

All FSOC federal agency members are subject to the Federal Information Security Management Act (FISMA), which requires that federal agencies review their information and determine appropriate security controls over that information commensurate with risk. We did, however, identify differences in how FSOC federal agency members mark non-public information as well as differences for handling non-public information. Without addressing these differences, there is a risk that senders and receivers of FSOC non-public information may not apply a consistent level of controls. In this regard, it is important to note that FSOC has begun to address these differences among its members through a March 2012 project that is being coordinated by the FSOC Data Committee. FSOC has requested detailed information gathered during our review to assist with this project.

In preparation for the increase in new types of non-public information under the Dodd-Frank Act and mindful of its duty to safely share that information among its members, we learned that the FSOC Secretariat is developing, with OFR, two tools to support secure collaboration. As FSOC continues to develop those tools for information sharing, it should consider that some of the new information developed under the Dodd-Frank Act as well as unexpected economic events may require controls greater than those currently in place or being planned among Council members. Similarly, appropriate safeguards will need to be considered and possibly upgraded by each FSOC federal agency member to ensure timely and secure access to the information. In the interim, FSOC should consider having a contingency plan in place to quickly and safely exchange information under a crisis environment. Such a plan should also contemplate FSOC's independent and state members.

Conclusion and Matters for Consideration

We acknowledge that FSOC is still evolving and a number of information-sharing projects are under development. For this reason, we are not making recommendations at this time. However, we encourage the Council to continue ongoing efforts, further examine the issues raised in our report with respect to commonalities and differences of member agencies, and prepare for possible security upgrades for information that may need to be exchanged as economic conditions change and new threats to the stability of the U.S. financial system emerge. We underscore the importance of acting in a timely manner.

FSOC Comments

On June 12, 2012, we received comments on our draft report from the Treasury Acting General Counsel on behalf of FSOC. (See Appendix II.) The Acting General Counsel's comments acknowledged the observations and suggestions we made. His response indicates that in the event any new data is designated "high impact," meaning the release of such data could result in catastrophic adverse impact on the financial system, FSOC members and member agencies would review how to address issues associated with safeguards and protocols to accommodate the exchange of such data. We would reiterate the value of preparing for that possibility.

Results of CIGFO Working Group Review

Introduction

CIGFO is pleased to report the results of its audit of the controls that FSOC has in place to protect non-public information from unauthorized disclosure. This is the first report that a CIGFO Working Group has issued to the Council and the Congress as part of CIGFO's authority to oversee FSOC under the Dodd-Frank Act.

In light of the sensitive nature of the information that could emerge and be shared as FSOC members carry out their new mandate under the Dodd-Frank Act, CIGFO identified information security controls as an area where the Inspectors General could bring their collective expertise to bear. Thus, CIGFO undertook a review to provide a snapshot of the current information control environment at the individual federal agency member level, determine any related initiatives the federal agency members and FSOC were undertaking, and then identify potential risks or gaps that FSOC as a whole may wish to consider as it continues to evolve the control framework that will govern the exchange of information between and among its various members.

In presenting these results, we are mindful that FSOC is a new entity and has not yet exchanged large amounts of non-public information, nor has it needed to confront the type of precipitous economic distress that prompted the recent financial crisis. However, FSOC and its members need to be well positioned to address threats to the stability of the financial system. Protecting the sensitive information that they possess, exchange, and discuss as they address these threats – both as individual members and as a collective Council – is of paramount importance.

To provide context for the report, we first present background information on FSOC, its membership, and its governance structure. Next, we discuss the FSOC information control environment, including commonalities and differences among FSOC federal agency members, ongoing initiatives to safely share information, and additional controls that may be needed going forward. Finally, we provide our concluding thoughts and matters for FSOC to consider.

Appendix I presents our audit objective and approach in more detail. Appendix II includes FSOC's comments on a draft of this report. Appendix III provides a listing of the CIGFO Working Group participants.

Background

FSOC was established to create joint accountability for identifying and mitigating potential threats to the stability of the nation's financial system. By creating FSOC, Congress recognized that financial stability would require the collective engagement of the entire financial regulatory community.

FSOC consists of 10 voting members and 5 nonvoting members and brings together the expertise of federal financial regulators, state regulators, and an insurance expert appointed by the President with Senate confirmation. FSOC is an important new function designed to fill the gaps in regulatory oversight. For the first time, a single entity has the collective accountability for identifying and limiting risks to the financial system as a whole. Each FSOC member comes to the table with unique and diverse responsibilities, interests, and expertise. Some member agencies have existed for a long time, while others are newly created.

Table 1: FSOC's Primary Purpose

- Identify risks to the financial stability of the U.S. that could arise from the material financial distress or failure, or ongoing activities, of large, interconnected bank holding companies or nonbank financial companies, or that could arise outside the financial services marketplace.
- Promote market discipline, by eliminating expectations on the part of shareholders, creditors, and counterparties of such companies that the U.S. government will shield them from losses in the event of failure.
- Respond to emerging threats to the stability of the U.S. financial system.

Table 2: FSOC Membership

Federal Agency Members	Independent and State Members
• Secretary of the Treasury, Chairperson (v)	• Independent member with insurance expertise (v)
• Chairman of the Board of Governors of the Federal Reserve System (v)	• State Insurance Commissioner
• Comptroller of the Currency (v)	• State Banking Supervisor
• Director of the Bureau of Consumer Financial Protection (v)	• State Securities Commissioner
• Chairman of the Securities and Exchange Commission (v)	
• Chairperson of the Federal Deposit Insurance Corporation (v)	
• Chairperson of the Commodity Futures Trading Commission (v)	
• Director of the Federal Housing Finance Agency (v)	
• Chairman of the National Credit Union Administration Board (v)	
• Director of the Office of Financial Research	
• Director of the Federal Insurance Office	

Source: 12 U.S.C. 5321(b)

(v) Indicates Voting Member

FSOC is chaired by the Secretary of the Treasury. Within Treasury, a dedicated policy office, led by a Deputy Assistant Secretary, functions as the FSOC Secretariat and serves as a mechanism to bring issues to the Council quickly through a coordinated process. Voting members of FSOC provide a federal regulatory

perspective and an independent insurance expert's view. The nonvoting members offer different insights as state-level representatives from bank, securities, and insurance regulators or as the directors of the new offices within the Treasury established by the Dodd-Frank Act – OFR and the Federal Insurance Office.

To carry out its mission, FSOC employs a committee structure.[1] Individual committees handle key responsibilities and require significant sharing of information to fully understand the complex issues at hand. The FSOC Data Committee, for example, supports coordination of, and consultation on, agency rulemakings on data collection, and seeks to minimize duplication of data gathering operations. This committee supports a coordinated approach to information sharing and provides direction to, and requests data from, OFR. Additionally, the committee works with OFR on data standardization.

OFR is the research arm of FSOC. As outlined in the Dodd-Frank Act, OFR supports the Council and member agencies by collecting and disseminating data to the Council and member agencies; standardizing the types and formats of data reported and collected; performing research; developing tools for risk measurement and monitoring; making the results of OFR's activities available to financial regulatory agencies; and assisting member agencies in determining the types and formats of data authorized under the Dodd-Frank Act to be collected by the member agencies.

Approach

The objective of our audit was to examine the controls and protocols that FSOC and its federal agency members employ to safeguard non-public information collected by, and exchanged with, FSOC members from unauthorized disclosure. We did not assess whether controls in place were effective or commensurate with risk, determine whether FSOC federal agency members were complying with controls, or evaluate controls and protocols of the FSOC independent and state members. We conducted our work from February through May 2012 in accordance with generally accepted government auditing standards.

As members of the CIGFO Working Group, each Office of Inspector General (OIG) conducted a survey of its FSOC federal agency member(s) to obtain information regarding the current status of each member's existing policies, procedures, and practices related to securing non-public FSOC information. The information was gathered through the use of a CIGFO Working Group-developed questionnaire based on information security control concepts in FISMA.

Each agency's OIG presented its specific findings to its respective agency management who were given the opportunity to provide additional comments. The results from each OIG and the FSOC Secretariat were reviewed to identify current controls as well as opportunities to strengthen overall controls over non-public FSOC information. We provided a briefing on the overall results of our work to FSOC and OFR staff on April 27, 2012.

1 FSOC's committee structure consists of the Deputies Committee and the Systemic Risk Committee. The Systemic Risk Committee has two sub-committees – the Institutions Sub-committee and the Markets Sub-committee. There are also five Standing Functional Committees – Designations of Nonbank Financial Companies; Designations of Financial Market Utilities and Payment, Clearing, and Settlement Activities; Heightened Prudential Standards; Orderly Liquidation Authority, Resolution Plans; and Data.

The Current FSOC Information Exchange Control Environment

Information collection, analysis, exchange, and deliberation are critical components of FSOC activity. Unauthorized disclosure of non-public information, in particular, is a risk that FSOC faces as it carries out its responsibilities under the Dodd-Frank Act. To date, exchange of information has been limited primarily to that associated with rulemakings and communications during meetings; however, the volume and nature of information exchanged could change substantially in the future. In the next sections of this report, we describe, at a high level, the internal information security control environments of FSOC federal agency members and how related security controls come into play when non-public information is exchanged beyond the members' control environment.

FSOC Memorandum of Understanding Governs Information Exchange

FSOC members have a statutory obligation to maintain the confidentiality of any data, information, and reports submitted under the Dodd-Frank Act. FSOC incorporated much of that confidentiality requirement into its governance documents, including in the *Rules of Organization of the Financial Stability Oversight Council* (known as the Bylaws) as well as the *Transparency Policy for the Financial Stability Oversight Council* (Transparency Policy). The Bylaws specifically require that FSOC members protect and maintain the confidentiality of any data, information, and reports submitted or available to them. The Transparency Policy governs FSOC meetings and requires the protection of information in order to prevent destabilizing market speculation that could occur if confidential information were to be disclosed.

The Bylaws also provide that FSOC members may enter into a memorandum of understanding regarding the treatment of confidential information. In this regard, all FSOC members signed 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), which sets forth the understanding of all FSOC members regarding the treatment of non-public information. The MOU, with an effective date of April 15, 2011, is the foundation for the secure exchange of non-public FSOC information.

The MOU defines "non-public information" as any data, information, or reports submitted, received, or shared among FSOC members in connection with or related to the functions and activities of FSOC or OFR. Non-public information includes the information itself, in any form, including oral communication, and any document to the extent it contains such information. The MOU presumes that non-public information exchanged under its terms is confidential.

According to the MOU, each FSOC member "will take all steps reasonably necessary to preserve, protect and maintain all privileges and claims of confidentiality." In effect, the MOU relies on the controls of each FSOC member to safeguard non-public FSOC information. The premise underlying that requirement is that all FSOC members know what steps are, in fact, reasonably necessary to safeguard FSOC non-public information both internally and when exchanging non-public information among FSOC's membership.

FSOC Federal Agency Members Use a Common Information Security Framework

An important commonality among FSOC federal agency members is that each member is subject to FISMA. FISMA tasked the National Institute of Standards and Technology (NIST) with various responsibilities, including, among other things, the development of information security standards to be used by federal agencies to categorize information and information systems collected or maintained by or on behalf of each agency. The objective of such categorization is to provide appropriate levels of information security according to a range of impact levels.

NIST Federal Information Processing Standard 199[2] requires that federal agencies assess the potential impact on an organization should certain events – in this case the release of information to the public – occur. Such a release would jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. NIST establishes three levels of potential impact – "low," "moderate," or "high"– as defined in Table 3. The standards primarily relate to information system controls.

Table 3: Impact-Level Designations

- Low – Limited adverse impact.
- Moderate – Serious adverse impact.
- High – Severe or catastrophic adverse impact.

Source: Federal Information Processing Standard 199

During our review, we determined that all FSOC federal agency members are subject to FISMA. Further, all FSOC federal agency members currently handle information designated at a "moderate" impact level.

NIST standards and guidelines require that federal agencies implement baseline controls for their systems commensurate with their impact-level designations. Those standards and guidelines allow agencies flexibility to determine how to implement controls and provide agencies with the ability to implement controls that are greater than baseline requirements. As a result, controls in place at one federal agency may not be commensurate with controls in place at another federal agency even though the agencies' impact-level designations may be the same. As discussed later in this report, we found that there were control differences among FSOC federal agency members.

FISMA requires that the agency that owns or is the steward of information is responsible for ensuring that proper security controls govern that information even when it is transferred to another agency. Additionally, automated systems that house information at various impact-level designations must set controls at the greatest of those impact levels. Finally, FISMA along with OMB policy lays out a framework for annual information technology security reviews, reporting, and remediation planning.[3]

Agency FISMA reports and related OIG evaluations describe the strengths and weaknesses of the information security controls within each FSOC federal agency member. This report focuses on security controls impacting the exchange of information from one FSOC federal agency member to another, as those controls are most relevant to the Council.

2 Federal Information Processing Standard 199, *Standards for Security Categorization of Federal Information and Information Systems* (Feb. 2004).

3 OMB Circular No. A-130, Management of Federal Information Resources; and annual FISMA reporting instructions.

Differences in FSOC Federal Agency Member Controls

As discussed below, we identified differences in how FSOC federal agency members mark non-public information as well as differences in controls over the handling of non-public information. Those differences reduce the assurance that FSOC federal agency members receiving information will apply the same level of security controls as those sending the information.

FSOC Federal Agency Members Have Different Markings for Non-public Information

We found that FSOC federal agency members use different markings to identify non-public information, and those markings signify specific control requirements. Marking refers to the process of labeling hardcopy or electronic information as non-public information. Table 4 summarizes the seven different marking types we found during our work.

Without a common marking vocabulary and understanding of what each marking implies, it is difficult for FSOC federal agency members to know the appropriate controls to apply to information shared with other FSOC members. For example, is a "sensitive" marking for one agency's information the same as a "predecisional" marking for another agency's information, and do the same information security controls apply? As previously mentioned, the MOU requires that each agency take steps reasonably necessary to safeguard non-public information.

Table 4: FSOC Federal Agency Member Markings

- Confidential
- Sensitive But Unclassified
- Controlled Unclassified
- Sensitive
- Business Sensitive
- Restricted
- Predecisional

Source: CIGFO Working Group Analysis

While our work did not expressly cover FSOC independent and state members, we understand that these members have received non-public information. Therefore, our concern with information marking goes beyond FSOC federal agency members and could affect the sharing of information among other members. This concern is heightened because the FSOC independent and state members may change at 6- and 2-year intervals, respectively, and the continuity of established safeguards is uncertain.

We note that the issue of how federal agencies mark non-public information and the controls commensurate with those markings is a government-wide concern. The President signed Executive Order 13556, *Controlled Unclassified Information*, on November 4, 2010, to address the ad hoc, agency-specific policies, procedures, and markings for safeguarding and controlling information. The Executive Order notes that this inefficient, confusing patchwork has resulted in inconsistent marking and safeguarding of documents, led to unclear or unnecessarily restrictive dissemination policies, and created impediments to authorized information sharing. According to the Executive Order, the National Archives and Records Administration is responsible for implementing the order and overseeing agency actions. Those efforts are underway, but the program is not yet complete. In the interim, FSOC should determine how to bridge the gap of information marking and corresponding controls.

Some FSOC federal agency members who routinely share information among one another have arrangements in place to bridge this marking gap that pre-date the Dodd-Frank Act. For example, the Federal Financial Institutions Examination Council (FFIEC), whose membership includes the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, and the Office of the Comptroller of the Currency, has a Task Force on Information Sharing that promotes the sharing of electronic information among FFIEC agencies. The task force provides a forum for FFIEC members to discuss and address issues affecting the quality, consistency, efficiency, and security of interagency information sharing. Additionally, some FSOC federal agency members have their own information-sharing agreements in place with other federal agencies.

During our review, we learned that, as of March 8, 2012, the FSOC Data Committee is coordinating a project to establish an FSOC-wide framework for classifying, marking, and handling data. We understand that OFR expects to develop and share its own initial classification structure during fiscal year 2012 and will then work with Council members to either develop a common classification structure or a mapping among dissimilar classification structures in fiscal year 2013. Further, the FSOC Data Committee is reviewing information-sharing processes in place at the FFIEC.

FSOC Federal Agency Members Have Different Controls for Handling Non-public Information

FSOC federal agency members have different policies and procedures governing the handling of non-public information. Our survey included a number of questions concerning policies, procedures, and protocols over personnel who handle non-public information. We found that FSOC federal agency members fall along a continuum, with some members having robust policies and procedures over information handling while others had few policies and procedures. This continuum reflects an overall control environment with varying levels of safeguards to be used by all parties involved in the process of sharing FSOC information.

Table 5 indentifies the six most common control differences that we identified during our work. As an example, some agencies did not have explicit policies and procedures governing oral communication of non-public information, while others had specific protocols such as prohibiting discussion of non-public information while on cell phones. As other examples, although all FSOC federal agency members are subject to the Office of Government Ethics Standards of Ethical Conduct,[4] some agencies have adopted supplemental standards prohibiting the purchase and sale of securities by the employee

Table 5: Federal Agency Member Control Differences for Handling Non-public Information

- Oral communication
- Supplemental prohibition on financial interest
- Contractor confidentiality and nondisclosure
- Encryption
- Meeting-related controls
- Protocols to track information exchange

Source: CIGFO Working Group Analysis

4 5 C.F.R. Part 2635.

and the employee's family when the employee is in possession of material non-public information. Some FSOC federal agency members had specific policies and procedures on when to encrypt non-public information, but others did not. Finally, one FSOC federal agency member is initiating a formal information-sharing protocol between the agency, FSOC, and OFR to track both information sent from the agency as well as to the agency, but most FSOC federal agency members do not have such protocols in place.

During our April 27, 2012, briefing to the FSOC Secretariat and OFR staff on the results of our review, staff requested that we provide more detail on policies and procedures covering information marking and handling. Staff stated that doing so would help FSOC's review of information-sharing protocols. We agreed to provide that information.

FSOC Information Exchange Efforts Should Consider Existing Member Control Differences and Potential Vulnerabilities

Joint work among FSOC members to identify and mitigate risks to financial stability has begun, and data sharing will expand as the OFR continues to build its capacity to gather information and perform analysis. That analysis includes the development of new information not previously held by or exchanged among Council members, including, among other things, information pertaining to threats to the U.S. financial system. A greater volume of this new information is anticipated in the near future, beginning with the July 1, 2012, deadline for the submission of resolution plans (known as living wills)[5] for certain institutions with $250 billion or more in total assets.

In preparation for the increase in new types of non-public information and mindful of its duty to safely share that information among its members, the FSOC Secretariat informed us that it is developing, with OFR, two tools to support secure collaboration. Based on descriptions provided by the FSOC Secretariat, the tools, which are in different stages of development, include (1) a data transmission protocol currently used by other Council members that will enable interagency data set exchange and (2) a secure collaboration tool for sharing documents. The secure collaboration tool will first be used between the FSOC Secretariat and OFR before access is provided to other Council members. The collaboration tool will reside within Treasury and access will be granted to Council members by Treasury. In addition, OFR has established a short-term analytical environment for its own researchers to use and for the FSOC Secretariat to access certain OFR datasets and related analytical tools. Whether this tool will be used to collaborate among Council members is, according to FSOC, still under review.

As the design and testing continue on these tools, FSOC and OFR need to consider the impact-level designation of the information that may be housed in those tools. As part of our review, we asked each FSOC federal agency member whether new information they would be required to develop, produce, or provide under the Dodd-Frank Act required a reassessment of their maximum impact-level designation. As discussed previously, under NIST standards, the owner or steward of information is required to make the decision regarding the impact-level designation.

5 77 Fed. Reg. 3075 (Jan. 23, 2012). The July 1, 2012, date corresponds with Covered Insured Depository Institutions (CIDI) whose parent company, as of November 30, 2011, had $250 billion or more in total nonbank assets. Plans are due on July 1, 2013, from CIDIs whose parent company, as of November 30, 2011, had $100 billion or more in total nonbank assets and on December 31, 2013, for all other CIDIs.

Nearly all of the FSOC federal agency members indicated that their existing "moderate" impact level was appropriate for their respective new Dodd-Frank Act information; however, one agency indicated that under certain economic circumstances, information it could provide to FSOC may be considered to be at the "high" impact level. The FSOC Secretariat, OFR, and Federal Insurance Office all reported that they could not rule out the possibility that new information they develop in the future under the Dodd-Frank Act would require adjustment to existing security levels. NIST defines a "moderate" impact-level designation as one in which the disclosure, modification, destruction, or disruption of access to that information would have a serious adverse effect on the agency's operations, assets or personnel. A "high" impact-level designation is one in which the disclosure, modification, destruction, or disruption of access to that information would have a severe or catastrophic adverse effect on the agency's operations, assets or personnel.[6]

Given this uncertainty and the possibility that any Council member could make a future determination that some of its information is at the "high" impact level, appropriate safeguards will need to be considered and possibly upgraded by each FSOC federal agency member for exchanging FSOC information. For example, if FSOC federal agency members have access to Treasury tools and have rights to download information onto their own servers or individual computers and print and store information, specific controls would need to be in place at the FSOC federal agency member beyond the controls used by the Treasury to grant remote access. We understand from our interviews that there are potential costs – depending on how such information could be exchanged – involved in upgrading controls for FSOC federal agency members who may receive "high" impact-level information. We were advised that FSOC intends to minimize the cost burden for its members as it continues to develop information-sharing tools. In addition, FSOC federal agency members would require lead time to put those additional controls in place before the exchange of information. The issue of lead time involved could take on greater importance, should, as indicated by one FSOC federal agency member, unexpected economic events make certain FSOC information "high" impact and require information be exchanged among FSOC members without time to ensure proper controls are in place.

As FSOC continues to consider its information-sharing protocols, it should factor in the potential for "high" impact-level information as well as the differences in information controls among its members. In the interim, FSOC should consider having a contingency plan in place to quickly exchange "high" impact-level information under a crisis environment.

6 Federal Information Processing Standards Publication 199. NIST amplifies that severe or catastrophic adverse effect means a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; results in major damage to organization assets; results in major financial loss; or severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.

Conclusion and Matters for Consideration

Given the volatility of the ever-changing economic conditions and the potential threats to the financial stability of the U.S. in a global environment, FSOC members must be ready to act quickly in carrying out their mission under the Dodd-Frank Act. We acknowledge that the Council is still evolving and a number of information-sharing projects are under development. With that in mind, we are not making recommendations at this time. However, we encourage the members of the Council, in the spirit of the MOU, to continue the ongoing efforts to protect the non-public information that they currently possess and will develop over time.

We also believe that FSOC would be well-served to further examine the issues raised in this report to increase their understanding of the differences in members' information control environments and determine whether those differences pose a risk of unauthorized disclosure of a magnitude that the Council would need to address on an FSOC-wide basis. Additionally, in examining differences, some best practices could emerge to the benefit of the Council as a whole. To that end, as requested, we are providing the FSOC Secretariat with a more detailed summary of the work of the individual OIGs involved in our CIGFO Working Group.

Finally, with particular regard to the tools under development for secure collaboration and controlled access to data shared among FSOC members, we underscore the importance of acting in a timely manner to complete the initiatives, considering the potential heightened impact designation of new information and the control ramifications of decisions made about such information. Taken together, such actions will help to ensure the readiness of FSOC members to keep pace with and react quickly to any threats to financial stability, knowing that all information possessed and exchanged as part of those efforts is protected as appropriate.

Summary of FSOC Comments

On June 12, 2012, we received comments on our draft report from the Treasury Acting General Counsel on behalf of FSOC. These comments are included in their entirety in Appendix II. The Acting General Counsel acknowledged the observations and suggestions we made. His response references the MOU that FSOC put in place to establish protocols for protecting the confidentiality of non-public information and the Bylaws that contain a provision related to protecting such information. The Data Committee's ongoing efforts to align FSOC members' protocols for classifying, marking, and handling data are mentioned. His response also affirms that the offices and staff of the Department of the Treasury engaged in FSOC work, along with the independent member with insurance expertise and his staff, operate within Treasury's information security infrastructure.

Finally, the Acting General Counsel's response indicates that in the event any new data is designated "high impact," meaning the release of such data could result in catastrophic adverse impact on the financial system, FSOC members and member agencies would review how to address issues associated with safeguards and protocols to accommodate the exchange of such data. We would reiterate the value of preparing for that possibility.

APPENDIX I: Objective, Scope, and Methodology

Objective

The audit objective was to examine the controls and protocols that FSOC and its federal agency members employ to safeguard non-public information collected by, and exchanged with, FSOC federal agency members from unauthorized disclosure. We did not assess whether controls in place were effective or commensurate with risk, determine whether FSOC federal agency members were complying with controls, or include the FSOC independent and state members in the review.

We conducted our performance audit work from February through May 2012 in accordance with generally accepted government auditing standards applicable to the objective and scope of the survey defined in the February 2012 CIGFO Survey Program. 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 obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Consistent with standards and as called for in the survey program, we obtained and incorporated the views of responsible agency officials into the results of our work.

We also performed appropriate quality control procedures, such as indexing and referencing, consistent with each OIG's internal policies and procedures to ensure the reliability of our results.

Scope and Methodology

The scope of this audit included a survey of the controls and protocols the FSOC federal agency members employ to safeguard non-public information collected by, and exchanged with, FSOC members from unauthorized disclosure.

We conducted a survey of the FSOC federal agency members, including the Consumer Financial Protection Bureau; Commodity Futures Trading Commission; Federal Deposit Insurance Corporation; Federal Housing Finance Agency; Federal Insurance Office; Board of Governors of the Federal Reserve System; National Credit Union Administration; Office of the Comptroller of the Currency; Office of Financial Research; Securities and Exchange Commission; and the Department of the Treasury, through each agency's OIG. The survey was designed to obtain information regarding each member's existing policies, procedures, and practices related to securing non-public FSOC information. The information was gathered through the use of a questionnaire. The questions were generally developed based on NIST Special Publication 800-53 Rev. 3, *Recommended Security Controls for Federal Information Systems and Organizations* since all federal agencies are required to follow NIST information security guidelines to meet FISMA requirements.

Each agency's OIG requested that agency management provide responses through interviews or self-reporting responses to the questionnaire. As part of the questionnaire, agencies reported the names of their policies, procedures, and practices regarding safeguarding FSOC non-public information. Each OIG reviewed the responses and requested clarification if necessary. Agency management was also given the opportunity to provide additional comments prior to submission. In preparing this report, results from all OIGs were reviewed to identify current controls and opportunities to strengthen controls over non-public FSOC information.

APPENDIX II: FSOC Response

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

June 12, 2012

The Honorable Eric M. Thorson
Chair, Council of Inspectors General
on Financial Oversight
1500 Pennsylvania Avenue, NW
Washington, D.C. 20220

Re: Response to CIGFO's Draft Audit Report: *Audit of the Financial Stability Oversight Council's Controls over Non-public Information: Report to the Financial Stability Oversight Council and the Congress*

Dear Mr. Chairman:

Thank you for the opportunity to review and respond to your draft Audit Report, *Audit of the Financial Stability Oversight Council's Controls over Non-public Information: Report to the Financial Stability Oversight Council and the Congress, dated May 31, 2012* (the Report). The Financial Stability Oversight Council (Council) and its respective members and member agencies appreciate the Council of Inspectors General on Financial Oversight (CIGFO) Working Group's review of the Council's controls and protocols for safeguarding information. This letter responds, on behalf of the Secretary of the Treasury as Chairperson of the Council, to your Report. The staffs of Council members previously provided comments and technical corrections to CIGFO staff.

The Report does not make any recommendations to the Council at this time, although it does make a number of observations and suggestions. Specifically, the Report (1) encourages the Council federal member agencies "to continue the ongoing efforts to protect the non-public information that they currently possess and will develop over time;" (2) suggests that the Council federal member agencies "further examine the issues raised in this report to increase their understanding of the differences in members' information control environments and determine whether those differences pose a risk of unauthorized disclosure of a magnitude that the Council would need to address on [a Council]-wide basis;" and (3) underscores "the importance of acting in a timely manner to complete the initiatives [under development for secure collaboration and controlled access to data shared among [Council] members]."

Safeguarding non-public information is crucial to the work of the Council. Toward that end, the Council members and member agencies entered into a Memorandum of Understanding that establishes protocols for protecting the confidentiality of "non-public information" shared among parties pursuant to the Dodd-Frank Wall Street Reform and Consumer Protection Act. The Council also has adopted in its Rules of Organization (known as the Council's Bylaws) a provision relating to the protection of confidential and other forms of non-public information. Beyond these existing protections, as the Report acknowledges, the Council Data Committee is working to further align the Council members' protocols for classifying, marking, and handling data.

The offices of the Department of the Treasury (Treasury) engaged in the Council's work – including the Federal Insurance Office, the Office of Financial Research, and the Treasury staff supporting the Council – also adhere to the security protections and compliance obligations in place at Treasury. In addition, Treasury provides administrative and infrastructure support to the Independent Member with insurance expertise and his staff of two senior advisors. As a result, the Independent Member and his staff benefit from Treasury's information technology security infrastructure.

The Report also raises the possibility that a Council member agency could generate new data that, under the National Institute of Standards and Technology classification system, would have a "high" impact-level designation – meaning release of such data could result in catastrophic adverse impact on the financial system. The Report suggests the Council federal members and member agencies may need to design additional, and potentially new, safeguards and protocols to accommodate the exchange of such data. Should such issues arise, Council members and member agencies would review how to address them.

Thank you again for your important oversight role and the observations you make in the Report. As the Report recognizes, the Council "is still evolving and a number of information-sharing projects are under development." The Council looks forward to working with you in the future.

Sincerely,

Christopher J. Meade
Acting General Counsel

Appendix III: CIGFO Working Group

Federal Deposit Insurance Corporation – Lead Agency		
Jon Rymer, Inspector General, Federal Deposit Insurance Corporation, and CIGFO Vice Chair		
Steve Beard	John Davidovich	Adriana Rojas
Arlene Boateng	Fred Gibson	Teresa Supples
Leslee Bollea	Judy Hoyle	Sharon Tushin
Danny Craven	Mark Mulholland	Peggy Wolf, Project Lead
Board of Governors of the Federal Reserve System and Consumer Financial Protection Bureau		
Tony Castaldo	Laura Shakarji	
Trevor Gaskins	Michael VanHuysen	
Charles Liuksila		
Commodity Futures Trading Commission		
Tony Baptiste	Judy Ringle	
Edward Kelley		
Department of the Treasury		
Tim Cargill	Jeff Dye	Jen Ksanznak
Theresa Cameron	Marla Freedman	Susan Marshall
Dana Duvall	Patrick Gallagher	Bob Taylor
Federal Housing Finance Agency		
Brian Baker	Brent Melson	
Andrew Gegor	Russell Rau	
National Credit Union Administration		
Charles Funderburk		
Marvin Stith		
Securities and Exchange Commission		
Kelli Brown-Barnes	Russell Moore	
Brenda Eberle		


BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
COMMODITY FUTURES TRADING COMMISSION
1975
OFFICE OF INSPECTOR GENERAL
DEPARTMENT OF HOUSING & URBAN DEVELOPMENT
TREASURY
INSPECTOR GENERAL
FEDERAL DEPOSIT
1933
INSURANCE CORPORATION
FEDERAL HOUSING FINANCE AGENCY
FHFA
OIG
OFFICE OF INSPECTOR GENERAL
NCUA
NATIONAL CREDIT UNION ADMINISTRATION
U.S. SECURITIES AND EXCHANGE COMMISSION
MCMXXXIV
SPECIAL INSPECTOR GENERAL
TROUBLED ASSET RELIEF PROGRAM