JULY 2019

Annual Report of the Council of Inspectors General on Financial Oversight

Office of Inspector General
Board of Governors of the Federal Reserve System
Consumer Financial Protection Bureau

Message from the Chair

In keeping with its mission, the Council of Inspectors General on Financial Oversight (CIGFO), which is authorized to oversee the Financial Stability Oversight Council (FSOC) operations, continued its work in 2018 and 2019. In its oversight role, it has, since 2011, established working groups that are comprised of staff from the CIGFO member Inspector General offices to conduct reviews of FSOC operations—CIGFO relies on these working groups to fulfill its mission. CIGFO issued an audit report by a Working Group convened in December 2017 that assessed FSOC's monitoring of international financial regulatory proposals and developments. CIGFO also convened the following Working Groups:

- June 2018 – initiated a project to report on management and performance challenges identified in 2017 across CIGFO agencies. That report, *Top Management and Performance Challenges Facing Financial Regulatory Organizations*, was issued in September 2018.

- December 2018 – initiated a project to survey FSOC Federal members' efforts to support implementation of the Cybersecurity Information Sharing Act. This project is expected to be completed in 2019.

- March 2019 – initiated a project to report on management and performance challenges identified in 2018 across CIGFO agencies. This project is expected to be completed in 2019.

In addition to CIGFO's oversight activities, it has performed monitoring activities that included sharing financial regulatory information which enhanced the Inspectors General knowledge and insight about specific issues related to members' current and future work. For example, during its quarterly meetings, CIGFO members discussed efforts to increase cybersecurity and the resiliency of the financial sector; swaps regulations, including related reforms under the Dodd-Frank Wall Street Reform and Consumer Protection Act; and other legislative activities that could impact the financial regulatory system.

In the coming year, CIGFO members will continue, through their individual and joint work, to help strengthen the financial system by oversight of FSOC and its Federal member agencies.

/s /

Rich Delmar
Acting Chair, Council of Inspectors General on Financial Oversight
Acting Inspector General, Department of the Treasury

THIS PAGE IS INTENTIONALLY LEFT BLANK.

Table of Contents

THIS PAGE IS INTENTIONALLY LEFT BLANK.

Council of Inspectors General on Financial Oversight

The Council of Inspectors General on Financial Oversight (CIGFO) was established by the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act), and meets on a quarterly basis to facilitate the sharing of information among Inspectors General. The CIGFO members discuss the ongoing work of each Inspector General who is a member of the Council, with a focus on concerns that may apply to the broader financial sector, and exchange ideas about ways to improve financial oversight. The CIGFO publishes an annual report that includes separate sections within the exclusive editorial control of each Inspector General. Those sections describe the concerns and recommendations of each Inspector General and a discussion of ongoing and completed work.

During the course of the year, the CIGFO continued to monitor coordination efforts among and between Financial Stability Oversight Council (FSOC) members. Specifically, CIGFO members were briefed on and/or discussed the following:

- Government Accountability Office – its work in the areas of Financial Markets and Housing
- Department of the Treasury's Financial Crimes Enforcement Network – its mission and priorities
- Department of the Treasury's Office of Critical Infrastructure Protection and Compliance – its role in executing Treasury's responsibilities as the Sector Specific Agency for the Financial Sector
- Commodity Futures Trading Commission's Division of Clearing and Risk – the history of derivatives and futures markets and the impact of the Dodd-Frank Act on this market
- Department of the Treasury's implementation of the President's Core Principles on Financial Regulation
- Department of Housing and Urban Development (HUD) and HUD Office of Inspector General - their efforts to respond to natural disasters

The Council of Inspectors General on Financial Oversight Reports

The Dodd-Frank Act authorizes the CIGFO to convene a working group, by a majority vote, for the purpose of evaluating the effectiveness and internal operations of the FSOC.

To date, CIGFO has issued the following reports—

- 2012 – *Audit of the Financial Stability Oversight Council's Controls over Non-public Information*
- 2013 – *Audit of the Financial Stability Oversight Council's Designation of Financial Market Utilities*
- 2014 – *Audit of the Financial Stability Oversight Council's Compliance with Its Transparency Policy*
- 2015 – *Audit of the Financial Stability Oversight Council's Monitoring of Interest Rate Risk to the Financial System*
- 2017 – *Audit of the Financial Stability Oversight Council's Efforts to Promote Market Discipline*
- 2017 – *Corrective Action Verification of FSOC's Implementation of CIGFO's Audit Recommendations in the 2013 Audit of FSOC's Financial Market Utility Designation Process*
- 2018 – *Top Management and Performance Challenges Facing Financial Regulatory Organizations*
- 2019 – *Audit of the Financial Stability Oversight Council's Monitoring of International Financial Regulatory Proposals and Developments*

The corrective actions described by FSOC, with respect to the audits listed above, met the intent of our recommendations, and may be subject to verification in future CIGFO working group reviews.

Office of Inspector General
Board of Governors of the Federal Reserve System
Consumer Financial Protection Bureau

Office of Inspector General Board of Governors of Federal Reserve System and Bureau of Consumer Financial Protection

The Office of Inspector General (OIG) provides independent oversight by conducting audits, inspections, evaluations, investigations, and other reviews of the programs and operations of the Board of Governors of the Federal Reserve System (Board) and the Bureau of Consumer Financial Protection Bureau (Bureau) and demonstrates leadership by making recommendations to improve economy, efficiency, and effectiveness, and by preventing and detecting fraud, waste, and abuse.

Background

Congress established the OIG as an independent oversight authority for the Board, the government agency component of the broader Federal Reserve System, and the Bureau.

Under the authority of the Inspector General Act of 1978, as amended (IG Act), the OIG conducts independent and objective audits, inspections, evaluations, investigations, and other reviews related to the programs and operations of the Board and the Bureau.

- We make recommendations to improve economy, efficiency, and effectiveness, and we prevent and detect fraud, waste, and abuse.
- We share our findings and make corrective action recommendations to the Board and the Bureau, but we do not have the authority to manage agency programs or implement changes.
- We keep the Board's Chair, the Bureau's Director, and Congress fully informed of our findings and corrective action recommendations, as well as the agencies' progress in implementing corrective action.

In addition to the duties set forth in the IG Act, Congress has mandated additional responsibilities for the OIG. Section 38(k) of the Federal Deposit Insurance Act (FDI Act) requires that the OIG review failed financial institutions supervised by the Board that result in a material loss to the Deposit Insurance Fund (DIF) and produce a report within 6 months. The Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) amended section 38(k) of the FDI Act by raising the materiality threshold and requiring the OIG to report on the results of any nonmaterial losses to the DIF that exhibit unusual circumstances warranting an in-depth review.

Section 211(f) of the Dodd-Frank Act also requires the OIG to review the Board's supervision of any covered financial company that is placed into receivership under title II of the act and produce a report that evaluates the effectiveness of the Board's supervision, identifies any acts or omissions by the Board that contributed to or could have prevented the company's receivership status, and recommends appropriate administrative or legislative action.

The Federal Information Security Modernization Act of 2014 (FISMA) established a legislative mandate for ensuring the effectiveness of information security controls over resources that support federal operations and assets. In a manner consistent with FISMA requirements, we perform annual independent reviews of the Board's and the Bureau's information security programs and practices, including the effectiveness of security controls and techniques for selected information systems.

OIG Reports and Other Products Related to the Broader Financial Sector

In accordance with section 989E(a)(2)(B) of the Dodd-Frank Act, the following highlights the completed and ongoing work of our office, with a focus on issues that may apply to the broader financial sector.

Completed Work

Major Management Challenges for the Board and the Bureau

Although not required by statute, we annually report on the major management challenges facing the Board and the Bureau. These challenges identify the areas that, if not addressed, are most likely to hamper the Board's and the Bureau's accomplishment of their strategic objectives.

Among other items, we identified five major management challenges for the Board that apply to the financial sector in 2018:

- Enhancing Organizational Governance
- Enhancing Oversight of Cybersecurity at Supervised Financial Institutions
- Ensuring an Effective Information Security Program
- Advancing Efforts to Improve Human Capital Management
- Remaining Adaptable to Internal and External Developments While Refining the Regulatory and Supervisory Framework

Among other items, we identified three major management challenges for the Bureau that apply to the financial sector in 2018:

- Ensuring That an Effective Information Security Program Is in Place
- Managing the Human Capital Program
- Strengthening Controls and Managing Risks

In Accordance With Applicable Guidance, Reserve Banks Rely on the Primary Federal Regulator of the Insured Depository Institution in the Consolidated Supervision of Regional Banking Organizations, but Document Sharing Can Be Improved, OIG Report 2018-SR-B-010, June 20, 2018

The Board is the consolidated supervisor of bank holding companies (BHCs)—entities that own or control one or more banks. The Board delegates authority to each Reserve Bank to supervise the BHCs in the Reserve Bank's District. By law, the Reserve Banks must rely to the fullest extent possible on the work of the PFR of the BHCs' subsidiary depository institutions. We conducted this evaluation to assess the effectiveness of the consolidated supervision of RBOs. We reviewed how Reserve Banks rely on other federal regulators to conduct consolidated supervision of RBOs—each with $10–$50 billion in assets.

In accordance with applicable guidance related to consolidated supervision, the Reserve Banks relied on the respective PFR of RBOs' insured depository institutions to supervise the RBOs we sampled. We also noted that the Reserve Banks appear to have increased their reliance on the PFRs.

We identified an opportunity for the Board to establish general guidelines for reliance on PFR documents and to ensure that all examiners have access to those documents. In addition, we found that the Board and the Reserve Banks could improve document-sharing processes. Finally, several RBO executives noted the potentially avoidable regulatory burden created because RBO employees sometimes upload the same documentation to multiple systems in response to Reserve Bank and PFR documentation requests.

Our report contains recommendations designed to improve document sharing among the Board, the Reserve Banks, and the PFRs. The Board concurred with our recommendations.

The Board's Currency Shipment Process Is Generally Effective but Can Be Enhanced to Gain Efficiencies and to Improve Contract Administration, OIG Report 2018-FMIC-B-021, December 3, 2018

The Board's Banknote Issuance and Cash Operations section is responsible for the currency shipment process. This process includes monitoring and forecasting the demand for currency and planning and executing the issuance of currency to Reserve Bank cash offices. We assessed the efficiency and effectiveness of the Board's management of the currency shipment process and the effectiveness of related contracting activities.

The Board's currency shipment process is generally effective; however, the process can be enhanced to gain time and cost efficiencies. Streamlining the currency forecasting process could save time and minimize the potential for human error. Selecting different transportation modes for certain currency shipment routes and evaluating alternatives to transporting shipping equipment could yield transportation cost savings.

Additionally, the Board can improve the administration of its armored carrier contracts to help ensure that the Board is adequately protected against loss or damage during shipments, that armored carriers are adequately protecting Board data, and that the Board is receiving the expected level of service.

Our report contains recommendations designed to help the Board seek additional efficiencies in the currency shipment process and to improve the administration of armored carrier contracts. The Board concurred with our recommendations.

Knowledge Management for the Board's Comprehensive Liquidity Analysis and Review Is Generally Effective and Can Be Further Enhanced, OIG Report 2018-SR-B-013, September 5, 2018

Through the CLAR program, the Federal Reserve System conducts a horizontal supervisory assessment of liquidity risk and risk management practices across Large Institution Supervision Coordinating Committee (LISCC) firms—the largest, most complex financial firms under Board supervision. We assessed the System's knowledge management processes, practices, and systems in support of the CLAR program.

The CLAR program's knowledge management practices generally align with many of the leading practices described in the academic studies and *Harvard Business Review* articles we reviewed related to preserving and transferring institutional knowledge. For example, CLAR leadership has fostered a culture that prioritizes knowledge management; CLAR teams practice regular, team-based collaboration; and the CLAR program uses an information-sharing application to capture, store, and share institutional knowledge. As a result, the CLAR program appears to preserve and maintain institutional knowledge related to supervisory findings and fosters effective collaboration.

Although the CLAR program has generally effective knowledge management practices, the practices can be further strengthened by (1) increasing CLAR program employees' awareness of management's office hours, during which they can discuss the rationale for decisions made during the CLAR letter-writing process; (2) formalizing employee onboarding procedures; and (3) standardizing the CLAR Steering Committee's approach to meeting minutes.

Our report contains recommendations designed to further enhance the CLAR program's knowledge management practices. The Board concurred with our recommendations.

Review of the Failure of Fayette County Bank, OIG Report 2018-SR-B-016, September 26, 2018

In accordance with the requirements of section 38(k) of the Federal Deposit Insurance Act, as amended by the Dodd-Frank Act, we conducted an in-depth review of the failure of Fayette County Bank (FCB) because the failure presented unusual circumstances that warranted an in-depth review.

FCB failed primarily because of an aggressive growth strategy coupled with ineffective oversight by its board of directors, leading to declining asset quality and rapid capital depletion. In addition, the bank's board of directors was unable to hire and retain effective management following a long-tenured Chief Executive Officer's retirement in December 2012.

The Federal Reserve Bank of St. Louis generally took decisive supervisory action to address FCB's weaknesses and deficiencies during the time frame we reviewed, 2011 through 2017, by appropriately downgrading the bank's CAMELS composite rating consistent with its risk profile and promptly issuing an emergency supervisory directive. The Federal Reserve Bank of St. Louis's supervisory activity included formal enforcement actions and a recommendation to implement an enforcement action against an FCB bank official.

Our review resulted in a finding related to enhanced communication between the Board's Legal Division and the Federal Reserve Bank of St. Louis. Because our office has recently issued a recommendation to address that communication issue, our report contains no new recommendations.

The Bureau Can Improve Its Follow-Up Process for Matters Requiring Attention at Supervised Institutions, OIG Report 2019-SR-C-001, January 28, 2019

During the examination process, Division of Supervision, Enforcement and Fair Lending (SEFL) employees may identify corrective actions that a supervised institution needs to implement to address certain violations, deficiencies, or weaknesses. These corrective actions include MRAs. We assessed SEFL's effectiveness in monitoring MRAs and ensuring that supervised institutions address them in a timely manner.

SEFL can improve its follow-up process for MRAs. For example, we found that the Bureau's approach for measuring how timely it resolves MRAs is prone to misinterpretation and therefore appeared to overstate the agency's progress toward closing these actions. We also determined that some of the underlying data used to calculate the measurement were not reliable. Additionally, we observed inconsistent MRA follow-up documentation and workpaper retention practices in certain areas.

Our report contains recommendations designed to further enhance the MRA follow-up process. The Bureau concurred with our recommendations.

Security Control Review of the Bureau's Mosaic System, OIG Report 2018-IT-C-012R, June 27, 2018

Mosaic, a public-facing web application running on a cloud-based platform-as-a-service, is used by the Bureau to manage consumer complaints related to financial products and services. It also provides the Bureau with enhanced services and tools related to workforce and resource management; entity boarding; and the creation and management of investigative records, company ratings, and surveys. In accordance with FISMA requirements, we evaluated the effectiveness of specific (1) security controls for the Mosaic system and (2) components of the planning, development, and delivery processes used for the system as they relate to the Bureau's risk management program.

Overall, we found that the security controls we tested for the Mosaic system were operating effectively. Further, specific components of the planning, development, and delivery processes used for the system, as they relate to the Bureau's risk management program, were performed effectively. For instance, we found that controls related to continuous monitoring, vulnerability scanning and remediation, and system and information integrity were operating effectively. Further, the Bureau developed a business case, which included an analysis of the benefits and risks, prior to implementing Mosaic. However, we found that the Bureau can strengthen controls in the area of identity and access management to ensure that the security control environment for Mosaic remains effective.

We made a recommendation in the area of identity and access management controls for Mosaic. The Bureau concurred with our recommendation. In addition, our report includes matters for management's consideration in the areas of audit and accountability, contingency planning, and configuration management.

The Bureau Can Improve Its Risk Assessment Framework for Prioritizing and Scheduling Examination Activities, OIG Report 2019-SR-C-005, March 25, 2019

The scope of the Bureau's financial institution oversight authorities covers depository institutions with more than $10 billion in total assets and thousands of nondepository institutions. The Bureau seeks to prioritize its examination activities based on an annual assessment of the risks that the products offered by these financial institutions present to consumers. We assessed the effectiveness of SEFL's risk assessment framework, including the identification, analysis, and prioritization of specific institution product lines for examination, and we reviewed each region's implementation of the results of the prioritization process through examination scheduling.

We identified opportunities for the Bureau to improve its risk assessment framework for prioritizing and scheduling examinations. Specifically, SEFL's approach for assigning a key risk score to individual institution product lines is not transparent for some Bureau employees involved in the scoring process; these employees would benefit from additional training and guidance on that process. We also found that SEFL can improve its preliminary research on supervised institutions. Finally, we found that SEFL can improve the internal reporting of changes to the examination schedule.

Our report contains recommendations designed to improve the Bureau's risk assessment framework for prioritizing and scheduling examination activities. The Bureau concurred with our recommendations.

Ongoing Work

Evaluation of the Effectiveness of the Board's Cybersecurity Supervision (Phase 2)

We identified cybersecurity oversight at supervised financial institutions as a major management challenge for the Board on an annual basis from 2015 to 2018. In 2017, we issued a report focused on cybersecurity supervision of multiregional data processing servicers and financial market utilities, among other topics. We have initiated the second phase of our cybersecurity oversight activities focused on assessing the Board's cybersecurity supervision of the nation's largest and most systemically important financial institutions—those institutions in the Board's Large Institution Supervision Coordinating Committee portfolio.

Audit of the Federal Reserve System's Supervision and Oversight of Designated Financial Market Utilities

Title VIII of the Dodd-Frank Act grants the Board the authority to supervise certain financial market utilities designated as systemically important by the Financial Stability Oversight Council. Title VIII also grants the Board the authority to consult with federal agencies that supervise other designated financial market utilities. This project will assess the Federal Reserve System's (1) process for supervising and overseeing designated financial market utilities and (2) processes for reviewing notices of material change from these institutions. We also plan to review the System's collaboration with other federal agencies in these areas.

Evaluation of the Efficiency and Effectiveness of the Board's and the Reserve Banks' Enforcement Action Issuance and Termination Processes

The Board may take formal enforcement actions against supervised financial institutions for violations of laws, rules, or regulations; unsafe or unsound practices; breaches of fiduciary duty; and violations of final orders. The Board also may use a variety of informal enforcement tools to address deficiencies that are relatively small in number, are not material to the safety and soundness of the institution, and can be corrected by the institution's current management. We are assessing the efficiency and effectiveness of the Board's and the Federal Reserve Banks' processes and practices for issuing and terminating enforcement actions.

Evaluation of the Board's and the Reserve Banks' Enforcement Action Monitoring Practices

An enforcement action generally requires a supervised financial institution to develop and implement acceptable plans, policies, and programs to remedy the deficiencies that resulted in the action. Under delegated authority from the Board, the Federal Reserve Banks conduct supervision activities, including monitoring institutions' efforts to address the terms of enforcement actions. We are assessing the effectiveness of the Board's and the Reserve Banks' practices for monitoring open enforcement actions against supervised financial institutions.

Evaluation of Postemployment Restrictions for Senior Examiners

The Intelligence Reform and Terrorism Prevention Act of 2004 prohibits specific employees who meet the definition of a senior examiner from knowingly accepting compensation as an employee, officer, director, or consultant from a depository institution, a depository institution holding company, or certain related entities that the employee may have supervised as a Reserve Bank employee. In November 2016, the Board issued new guidance on these postemployment restrictions that expanded the definition of a senior examiner. We are assessing the implementation of these updates across the Federal Reserve System and the effectiveness of controls that seek to ensure compliance with postemployment restrictions.

Evaluation of the Bureau's Periodic Monitoring of Supervised Institutions

The Bureau has the authority to supervise depository institutions with more than $10 billion in total assets and nondepository institutions in certain markets, including credit reporting agencies. To supplement its onsite examinations of those institutions, the Bureau conducts periodic offsite monitoring of all the depository institutions within its supervisory jurisdiction and certain nondepository institutions, including credit reporting agencies. We plan to evaluate the Division of Supervision, Enforcement and Fair Lending's policies and procedures for conducting periodic monitoring. This evaluation will assess the implementation of these practices across the Bureau's regional offices and benchmark the Bureau's approach to offsite monitoring activities against the monitoring activities of other financial regulators.

Evaluation of the Bureau's Processes for Leveraging the Federal Risk and Authorization Management Program

The Federal Information Security Modernization Act of 2014 requires that we test the effectiveness of the Bureau's policies, procedures, and practices for select information systems. In support of these requirements, we are conducting an evaluation of the Bureau's risk management activities with respect to its various cloud computing platforms and providers, including the agency's reliance on the Federal Risk and Authorization Management Program.

Our evaluation objective is to determine whether the Bureau has implemented an effective life cycle process for deploying and managing its cloud-based systems, including ensuring that effective security controls are implemented.

Evaluation of the Office of Consumer Response's Efforts to Share Complaint Data Within the Bureau

The Office of Consumer Response (Consumer Response) is responsible for sharing consumer complaint information with internal stakeholders in order to help the Bureau supervise companies, enforce federal consumer financial laws, and write rules and regulations. The effective sharing of consumer complaint information can help the Bureau understand the problems consumers are experiencing in the financial marketplace and identify and prevent unfair practices from occurring before they become major issues. This evaluation is assessing the effectiveness of Consumer Response's complaint-sharing efforts. Specifically, this project is examining (1) the extent to which Consumer Response's consumer complaint-sharing efforts help to inform the work of internal stakeholders and (2) Consumer Response's controls over internal access of shared complaint data, which can contain sensitive consumer information.

Evaluation of the Bureau's Final Order Follow-Up Activities

This evaluation is assessing the Division of Supervision, Enforcement and Fair Lending's final order follow-up processes. The Bureau generally has enforcement authority over any person or entity that violates federal consumer financial protection law. In executing that authority, the Bureau can file a civil suit in federal district court that may result in a federal court order. Alternatively, through the administrative adjudication process, the Bureau and the relevant entity may agree to a consent order that includes a series of required corrective actions by that entity. Our objective is to review the Bureau's processes for monitoring and conducting follow-up activities related to final orders.

Office of Inspector General
Commodity Futures Trading Commission

The CFTC OIG acts as an independent Office within the CFTC that conducts audits, investigations, reviews, inspections, and other activities designed to identify fraud, waste and abuse in connection with CFTC programs and operations, and makes recommendations and referrals as appropriate.

Background

The CFTC OIG was created in 1989 in accordance with the 1988 amendments to the Inspector General Act of 1978 (P.L. 95-452). OIG was established as an independent unit to:

- Promote economy, efficiency and effectiveness in the administration of CFTC programs and operations and detect and prevent fraud, waste and abuse in such programs and operations;
- Conduct and supervise audits and, where necessary, investigations relating to the administration of CFTC programs and operations;
- Review existing and proposed legislation, regulations and exchange rules and make recommendations concerning their impact on the economy and efficiency of CFTC programs and operations or the prevention and detection of fraud and abuse;
- Recommend policies for, and conduct, supervise, or coordinate other activities carried out or financed by such establishment for the purpose of promoting economy and efficiency in the administration of, or preventing and detecting fraud and abuse in, its programs and operations; and
- Keep the Commission and Congress fully informed about any problems or deficiencies in the administration of CFTC programs and operations and provide recommendations for correction of these problems or deficiencies.

CFTC OIG operates independently of the Agency and has not experienced any interference from the CFTC Chairman in connection with the conduct of any investigation, inspection, evaluation, review, or audit, and our investigations have been pursued regardless of the rank or party affiliation of the target.[1] The CFTC OIG consists of the Inspector General, the Deputy Inspector General/Chief Counsel, the Assistant Inspector General for Auditing, the Assistant Inspector General for Investigations, one Attorney-Advisor, two Auditors, one Senior Program Analyst, and one part-time consultant. The CFTC OIG obtains additional audit, investigative, and administrative assistance through contracts and agreements.

1 The Inspector General Act of 1978, as amended, states: "Neither the head of the establishment nor the officer next in rank below such head shall prevent or prohibit the Inspector General from initiating, carrying out, or completing any audit or investigation…." 5 U.S.C. App. 3 sec. 3(a).

Role in Financial Oversight

The CFTC OIG has no direct statutory duties related to oversight of the futures, swaps and derivatives markets; rather, the CFTC OIG acts as an independent Office within the CFTC that conducts audits, investigations, reviews, inspections, and other activities designed to identify fraud, waste, and abuse in connection with CFTC programs and operations, and makes recommendations and referrals as appropriate. The CFTC's yearly financial statement and Customer Protection Fund audits are conducted by an independent public accounting firm, with OIG oversight.

Recent, Current or Ongoing Work in Financial Oversight

In addition to our work on CIGFO projects described elsewhere in this report, CFTC OIG completed the following projects during the past year:

Inspection & Evaluation: CFTC Stress-Testing Development Efforts (July 2018)

OIG's Office of Legal and Economic Review completed and published a report titled Inspection & Evaluation: CFTC Stress-Testing Development Efforts. This inspection was motivated by allegations of mismanagement in the Risk Surveillance Branch (RSB) of the CFTC Division of Clearing and Risk (DCR), which was conveyed to us by multiple CFTC whistleblowers. We first brought the allegations to the attention of the Chairman's Chief of Staff in July 2017. The Chairman appointed a new Director of DCR in September 2017, and OIG communicated frequently with the new DCR Director beginning in October 2017. We circulated a summary memo to the Chairman in October 2017, followed by a substantially complete version of the report in December 2017. In January 2018, we met with the Chairman, his staff, and the Director of DCR; they stated they had no major disagreements with the report. We finalized a discussion draft in February 2018 and circulated it to the Commission. We accommodated the Chairman's request for an extended time to respond to the February 2018 discussion draft. We received no formal written response or any stated disagreements, and circulated the report as final on July 30, 2018.

We found that leadership in the Division of Clearing and Risk (DCR)'s Risk Surveillance Branch (RSB) retarded the development of CFTC stress-testing capabilities, undermined efforts to improve the usability of uncleared swaps data, denied various employees access to certain information technology resources, and overstated publicly the independence and coverage of its November 2016 Supervisory Stress Test of Clearing Houses report (November 2016 report). To complete our inspection and evaluation, we contracted with National Economic Research Associates, Inc. (NERA). NERA assisted our technical evaluation of two CFTC stress-test methodologies. NERA issued detailed analysis, including substantive criticism of the methodology CFTC employed in the November 2016 report. No recommendations were issued by NERA or OIG.

In our cover memo, we disclosed that, in lieu of a written response, the new DCR Director verbally informed us that a new Deputy Director of the Risk Surveillance Branch (RSB) would be named shortly, and this has occurred. In addition, we were told there will be a reorganization of RSB, including greater integration of the related endeavors of margin model review and stress-testing; that there will be greater emphasis on technical acumen, technological development, and automation; and that there will be greater quantitative analytical support of other business divisions within the CFTC. We understand these processes are ongoing, and we intend to monitor the issues identified in our report and in NERA's report.

Customer Protection Outreach Whitepaper (September 2018)

This whitepaper examined possible locations for targeted CFTC education initiatives based on the locations of high-volumes of complaints and enforcement filings ("hotspots"), coupled with the locations of airport hubs and relevant state regulators.

We compared identified hotspots with recent outreach efforts by CFTC's Office of Customer Education and Outreach (OCEO), and concluded that OCEO's educational outreach activities could better align with existing hotspots,

specifically in the Southern and Western United States, where large hotspots exist that have not been visited by OCEO (or have not been visited frequently). We noted that CFTC does not have a permanent physical presence in these regions; CFTC's furthermost western (and southern) presence is in Kansas City, Missouri. We believe OCEO should target its efforts where customer education and outreach appears most needed.

In addition, we addressed factors impacting the feasibility of increased outreach efforts by OCEO, including: 1) Consumer Protection Funds (CPF) availability and the adequacy of CFTC's financial system to track and monitor expenditures; 2) CFTC's authority to spend CPF funds on education initiatives; and 3) CFTC's ability to detail appropriate CFTC staff to strengthen OCEO on a reimbursable basis. We concluded that CFTC has the current ability to track and monitor expenditures, and agreed with the Office of General Counsel that CFTC has the authority to spend CPF funds on education initiatives. Furthermore, we concluded that CFTC has current funds available to further support education activities, and we forecast -- based on our analysis of CFTC collections activity -- that funds availability should continue.

We asked the Commission to consider –

- Establishing OCEO personnel in the CFTC Kansas City regional office;
- Opening additional CFTC field offices or establishing permanent remote OCEO employees in the hotspots;
- Detailing personnel from other Divisions to OCEO (on a reimbursable basis from the CPF); and
- Engaging appropriate Federal, State, and local government entities and other relevant entities located in hotspots to facilitate customer education initiatives.

Management expressed their appreciation for our report and provided detailed comments. Management's comments, and our responses, are published with the whitepaper.

Inspection and Evaluation of the February 2018 CFTC-SEC Harmonization Briefing (October 2018)

Under the Dodd-Frank Act, the CFTC and the Securities and Exchange Commission have certain joint responsibilities.[2] Our report titled Inspection and Evaluation of the February 2018 CFTC-SEC Harmonization Briefing responded to two outside complaints that the SEC-CFTC harmonization briefing held on February 27, 2018, might have violated the Government in the Sunshine Act.[3] Lacking a specific allegation of misconduct by any individual, we determined to conduct an inspection and evaluation of the meeting. After interviewing all CFTC attendees, as well as reviewing all matters voted on by the Commission from the date of the meeting until the appointment of a full Commission, we concluded that CFTC complied with the Government in the Sunshine Act in the conduct of the meeting.

2 See, e.g., Memorandum of Understanding Between the U.S. Securities and Exchange Commission and the U.S. Commodity Futures Trading Commission Regarding Coordination in Areas of Common Regulatory Interest and Information Sharing, July 11, 2018.

3 The Government in the Sunshine Act, 5 U.S.C. § 552b (1976), requires that meetings of multi-member federal agencies shall be open to the public, with the exception of discussions in ten narrowly defined areas. The Sunshine Act defines "meeting" as "the deliberations of at least the number of individual agency members required to take action on behalf of the agency where such deliberations determine or result in the joint conduct or disposition of official agency business" [with exceptions]. Id.

Office of Inspector General
Federal Deposit Insurance Corporation

The FDIC OIG mission is to prevent, deter, and detect fraud, waste, abuse, and misconduct in FDIC programs and operations; and to promote economy, efficiency, and effectiveness at the agency.

Background

The Federal Deposit Insurance Corporation (FDIC) was created by the Congress in 1933 as an independent agency to maintain stability in the nation's banking system by insuring deposits and independently regulating state-chartered, non-member banks. The FDIC insures more than $7.5 trillion in deposits at more than 5,400 banks and savings associations, and promotes the safety and soundness of these institutions by identifying, monitoring, and addressing risks to which they are exposed. The FDIC is the primary federal regulator for approximately 3,500 of the insured institutions. An equally important role for the FDIC is as Receiver for failed institutions; the FDIC is responsible for resolving the institution and managing and disposing of its remaining assets.

The FDIC Office of Inspector General (OIG) is an independent and objective oversight unit established under the Inspector General (IG) Act of 1978, as amended. The FDIC OIG mission is to prevent, deter, and detect fraud, waste, abuse, and misconduct in FDIC programs and operations; and to promote economy, efficiency, and effectiveness at the agency.

Importantly, also in connection with matters affecting the financial sector, in February 2019, our Office published its assessment of the Top Management and Performance Challenges Facing the FDIC. This assessment was based on our extensive oversight work and research relating to reports by other oversight bodies, review of academic and other relevant literature, perspectives from Government agencies and officials, and information from private sector entities.

In addition, we conducted significant investigations into criminal and administrative matters involving complex multi-million-dollar schemes of bank fraud, embezzlement, money laundering, and other crimes committed by corporate executives and bank insiders. Our cases reflect the cooperative efforts of other OIGs, U.S. Attorneys' Offices, FDIC Divisions and Offices, and others in the law enforcement community throughout the country. These working partnerships contribute to ensuring the continued safety and soundness of the nation's banks and help ensure integrity in the FDIC's programs and activities.

Finally, over the past year, we continued to coordinate with our financial IG counterparts on issues of mutual interest. As a member of CIGFO, the FDIC OIG is also participating in the joint project related to the Financial Stability Oversight Council members' efforts to support implementation of the Cybersecurity Information Sharing Act.

Top Management and Performance Challenges Facing the FDIC

The OIG identified the Top Management and Performance Challenges facing the FDIC and provides its assessment to the Corporation for inclusion in the FDIC's annual performance and accountability report. This year, we identified nine areas representing the most significant challenges for the FDIC, a number of which have implications to the financial sector, and ways to improve financial oversight. The identification of these challenges helps the FDIC and other policymakers to identify the primary risks at the agency, and provides guidance for our Office to focus its attention and work efforts, as shown in the following summaries of each of these challenges.

Enhancing Oversight of Banks' Cybersecurity Risk

Cybersecurity continues to be a critical risk facing the financial sector. Cyber risks can affect the safety and soundness of institutions and lead to the failure of banks, thus causing losses to the FDIC's Deposit Insurance Fund. For example, a cybersecurity incident could disrupt services at a bank, resulting in the exploitation of personal information in fraudulent or other illicit schemes, and an incident could start a contagion that spreads through established interconnected banking relationships. Despite increased spending on cybersecurity, banks are encountering difficulties in getting ahead of the increased frequency and sophistication of cyberattacks. The FDIC's IT examinations should ensure strong management practices within financial institutions and at their service providers.

Adapting to Financial Technology Innovation

FDIC policy-makers and examiners must keep pace with the adoption of new financial technology to assess safety and soundness of institutions and its impact on the stability of the banking system. The pace of change and breadth of innovation requires that the FDIC create agile and nimble regulatory processes, so that it can respond to and adjust policies, examination processes, supervisory strategies, preparedness and readiness, and resolution approaches as needed.

Strengthening FDIC Information Security Management

The FDIC maintains thousands of terabytes of sensitive data within its IT systems and has more than 180 IT systems that collect, store, or process the PII of FDIC employees; bank officials at FDIC-supervised institutions; and bank customers, depositors, and bank officials associated with failed banks. FDIC systems also hold sensitive supervisory data about the financial health of banks, bank resolution strategies, and resolution activities. The FDIC must continue to strengthen its implementation of governance and security controls around its IT systems to ensure that information is safeguarded properly.

Preparing for Crises

Central to the FDIC's mission is readiness to address crises in the banking system. The FDIC must be prepared for a broad range of crises that could impact the banking sector. These readiness activities should help to ensure the safety and soundness of institutions, as well as the stability and integrity of our nation's banking system.

Maturing Enterprise Risk Management

Enterprise Risk Management (ERM) is a critical part of an agency's governance, as it can inform prudent decision-making at an agency, including strategic planning, budget formulation, and capital investment. ERM program requirements include identifying risks that could affect the organization (Risk Profile and Inventory), establishing the amount of risk an organization is willing to accept (Risk Appetite), prioritizing strategies to address risks in the proper sequence, and responding to and mitigating the risks. The FDIC established an ERM program office in 2011, but has neither developed the underlying ERM program requirements nor realized the benefits of a mature ERM program.

Sharing Threat Information with Banks and Examiners

Federal Government agencies and private-sector entities share information about threats to U.S. critical infrastructure sectors, including the financial sector. Sharing actionable and relevant threat information among Federal and private-sector participants protects the financial system by building threat awareness and allowing for informed decision-making. The FDIC must ensure that relevant threat information is shared with its supervised institutions and FDIC examiners as needed, in a timely manner, so that actions can be taken to address the threats. Threat information also provides FDIC examiners with context to evaluate banks' processes for risk identification and mitigation strategies.

Managing Human Capital

The FDIC relies on skilled personnel to fulfill its mission, and 68 percent of the FDIC's operating budget for 2019 ($1.8 billion) was for salaries and associated benefits for employees. Forty-two percent of FDIC employees are eligible to retire within 5 years, which may lead to knowledge and leadership gaps. To ensure mission readiness, the FDIC should find ways to manage this impending shortfall. In addition, the FDIC should seek to hire individuals with the advanced technical skills needed for IT examinations and supervision of large and complex banks.

Administering the Acquisitions Process

The FDIC relies heavily on contractors for support of its mission, especially for IT and administrative support services. The average annual expenditure by the FDIC for contractor services over the past 5 years has been approximately $587 million. The FDIC should maintain effective controls to ensure proper oversight and management of such contracts and should conduct regular reviews of contractors. In addition, the FDIC should also perform due diligence to mitigate security risks associated with supply chains for goods and services.

Improving Measurement of Regulatory Costs and Benefits

Before issuing a rule, the FDIC should ensure that the benefits accrued from a regulation justify the costs imposed. The FDIC should establish a sound mechanism to measure both costs and benefits at the time of promulgation, and it should continue to evaluate the costs and benefits of a regulation on a regular basis, even after it has been issued.

Additional information on these Challenges can be found in the full Top Management and Performance Challenges report, available on our Website, *www.fdicoig.gov*. These Challenges align with those facing the financial regulatory community as a whole, as discussed in the CIGFO report entitled Top Management and Performance Challenges Facing Financial Regulators.

FDIC OIG Audits and Evaluations Made Significant Recommendations for Improvements to the FDIC

During the 12-month period ending March 31, 2019, the FDIC OIG issued 14 audit, evaluation, and other reports and made 53 recommendations to strengthen controls in FDIC programs and operations. Our work covered diverse topics such as information security, processing of consumer complaints, and the FDIC's Forward-Looking Supervision program, among others.

The FDIC's Forward-Looking Supervision Program

The goals of the FDIC's Forward-Looking Supervision initiative are to identify and assess risk before it impacts a financial institution's financial condition and to ensure early risk mitigation. Prior to the financial crisis of 2008-2011, examiners often identified weak risk management practices at financial institutions, but they delayed taking supervisory action until the institution's financial performance declined. Forward-Looking Supervision seeks to avoid this result.

Our evaluation objective was to determine whether the Forward- Looking Supervision approach achieved its outcomes—the Division of Risk Management Supervision pursued supervisory action upon identifying risks and the financial institutions implemented corrective measures. Our review showed that examiners substantially achieved the intended outcomes of the Forward-Looking Supervision approach for our sampled institutions. Examiners applied Forward-Looking Supervision concepts during their financial institution examinations, rated institutions based on risk, and recommended corrective actions based on their risk assessments. Also, the financial institutions committed to implement the corrective actions.

We found that:

- The FDIC did not have a comprehensive policy guidance document on Forward-Looking Supervision and should clarify guidance associated with its purpose, goals, roles, and responsibilities;

- Examiners typically documented their overall conclusions regarding the financial institutions' concentration risk management practices; however, they did not always document certain Forward-Looking Supervision concepts in pre-examination planning documents and when reporting examination results;

- Examiners typically reported or elevated identified overall concentration risk management conclusions and concerns; however, a greater number of these concerns should have appeared in the report section that includes issues requiring the attention of the institution's board; and

- Examiners generally identified concentration risk management concerns on a timely basis; however, in certain instances, they identified concentration risk management concerns that had not been identified during the prior examination cycle.

We made four recommendations to the FDIC to: (1) issue a comprehensive policy guidance document defining Forward-Looking Supervision; (2) issue guidance to reinforce how and where examiners should be documenting concentrations and an institution's concentration risk management practices in the Report of Examination; (3) provide additional case studies on Forward-Looking Supervision to strengthen training for examiners; and (4) conduct recurring retrospective reviews to ensure examiners are documenting the concentration risk management analysis.

The full report is available on our Website, *www.fdicoig.gov*.

Federal Information Security Modernization Act (FISMA) Audit – 2018

We evaluated the effectiveness of the FDIC's information security program and practices. A strong information security program is needed for the protection of sensitive information the FDIC collects in conducting is work, including sensitive bank data and personal information of borrowers. The IG FISMA Reporting Metrics require IGs to assess the effectiveness of their agencies' information security programs and practices on a maturity model spectrum. We found that the FDIC's overall information security program was operating at a Maturity Level 3 (Consistently Implemented) on a scale of 1 to 5, which is an improvement from 2017 but not considered effective under the metrics.

We found that the FDIC established a number of information security program controls and practices that complied or were consistent with standards and guidelines, and took steps to strengthen controls following the 2017 FISMA report. However, ongoing security control weaknesses limited the effectiveness of the FDIC's information security program and practices and placed the confidentiality, integrity, and availability of the FDIC's information systems and data at risk. In many cases, these security control weaknesses were identified by other OIG audits or through security control assessments completed by the FDIC. Although the FDIC was working to address these previously identified control weaknesses, the FDIC had not yet completed corrective actions at the time of the audit. Accordingly, the security control weaknesses continued to pose risk to the FDIC. The highest risk weaknesses included:

- **Information Security Risk Management.** The FDIC had not fully defined or implemented an enterprise-wide and integrated approach to identifying, assessing, and addressing the full spectrum of internal and external risks, including those related to cybersecurity and the operation of information systems. This limits the ability of FDIC Divisions and Offices to make effective risk management decisions, and prevents the FDIC from ensuring it is effectively prioritizing resources toward addressing risks with the most significant potential impact on achieving strategic objectives.

- **Enterprise Security Architecture.** Our 2017 FISMA audit noted that the FDIC had not established an enterprise security architecture, which is considered a fundamental component of an effective information security program and describes the structure and behavior of an organization's security processes, systems, personnel, and subunits and shows their alignment with the organization's mission and strategic plans. In July 2018, the FDIC provided the OIG with documentation describing its enterprise security architecture. The OIG is reviewing this documentation, along with other information related to the enterprise security architecture provided by the FDIC, to determine whether it is responsive to the recommendation in our FISMA audit report issued in 2017. The lack of effective enterprise security architecture increased the risk that the FDIC's information systems would be developed with inconsistent security controls that are costly to maintain.

- **Security Control Assessments.** In separate OIG audit work, we identified instances in which contractor-performed security control assessments did not include testing of security control implementation, when warranted. Instead, assessors relied on narrative descriptions of the controls in FDIC policies, procedures, and system security plans and/or interviews of FDIC or contractor personnel. Without testing, assessors did not have a basis for concluding on the effectiveness of security controls. Inadequate FDIC oversight of security control assessments contributed to this weakness. Because the FDIC relies on the results of the assessments to support a number of important risk management activities, the FDIC must ensure that personnel perform security control assessments at an appropriate level of depth and coverage.

- **Patch Management.** The FDIC's patch management processes were not always effective in ensuring that the FDIC implemented patches within FDIC-defined timeframes. Unpatched systems increase the risk of exposing the FDIC's network to a security incident.

- **Backup and Recovery.** Our 2017 FISMA report noted that the FDIC's IT restoration capabilities were limited and that the FDIC had not taken timely action to address known limitations with respect to its ability to maintain or restore critical IT systems and applications during a disaster. In December 2017, the FDIC's Board of Directors authorized a multi-year Backup Data Center Migration Project to ensure that designated IT systems and applications supporting mission-essential functions can be recovered within targeted timeframes. While the FDIC established governance over this project, assurance that the FDIC can maintain and restore mission-essential functions during an emergency within applicable timeframes will be limited until the scheduled completion of the project in 2019.

We made four recommendations to improve the effectiveness of the FDIC's information security program controls and practices.

The publicly-releasable Executive Summary of this report is available on our Website, *www.fdicoig.gov*.

Our ongoing audit and evaluation reviews are addressing the FDIC's:

- Enterprise Risk Management Program;

- Cost-Benefit Analysis Process for Rulemaking;

- Anti-Sexual Harassment Program;

- Readiness for Crises;
- Contract Oversight Management Program; and
- Privacy Program.

These ongoing reviews are also listed on our Website, *www.fdicoig.gov*, and, when completed, their results will be posted there.

FDIC OIG Special Inquiry Report Made Significant Recommendations Regarding Breach Response, Reporting, and Interactions with Congress

In addition to the audit and evaluation reports listed above, the OIG issued a multi-disciplinary Special Inquiry report in April 2018.

During late 2015 and early 2016, the FDIC experienced eight information security incidents as departing employees improperly took sensitive information shortly before leaving the FDIC. Seven of the eight incidents involved Personally Identifiable Information (PII), including Social Security Numbers, and thus constituted breaches. In the eighth incident, the departing employee took highly sensitive components of resolution plans submitted by certain large systemically important financial institutions without authorization.

In April and May 2016, the Committee on Science, Space, and Technology of the House of Representatives (SST Committee) examined the FDIC's handling of these incidents, its data security policies, and reporting of the "major incidents." As part of its investigation, the SST Committee requested pertinent documents from the FDIC about the incidents. The SST Committee held two hearings in May and July 2016 about the incidents at the FDIC and issued an interim report on the matter. During the hearings and in its interim report, as well in correspondence with the FDIC, the SST Committee expressed concerns about the FDIC's information security program, the accuracy of certain FDIC statements, and the completeness of the FDIC's document productions.

On June 28, 2016, the then-Chairman of the Senate Committee on Banking, Housing, and Urban Affairs requested that our Office examine issues at the FDIC related to data security, incident reporting, and policies, as well as the representations made by FDIC officials.

The FDIC OIG conducted a Special Inquiry in response to that request. We examined the circumstances surrounding the eight information security incidents. The FDIC initially estimated that the incidents involved sensitive information that included the PII of approximately 200,000 individual bank customers related to approximately 380 financial institutions, as well as the proprietary and sensitive data of financial institutions. Based on additional analysis, the FDIC later revised the number of affected individuals to 121,633.

Our work revealed certain systemic weaknesses that hindered the FDIC's ability to handle multiple information security incidents and breaches efficiently and effectively; contributed to untimely, inaccurate, and imprecise reporting of information to the Congress; and led to document productions that did not fully comply with Congressional document requests. We also identified shortcomings in the performance of certain individuals in key leadership positions as they handled the incidents and related activities.

Importantly, in its handling of the information security incidents, the FDIC did not fully consider the range of impacts on bank customers whose information had been compromised or consider customer notification as a separate decision from whether it would provide credit monitoring services. As a result, the FDIC delayed notifying consumers and thus precluded them from taking proactive steps to protect themselves.

Also of note, when reporting incidents to the Congress, the FDIC used broad characterizations and referenced mitigating factors that were sometimes inaccurate and imprecise, and tended to diminish the potential risks. Despite

several opportunities to clarify or correct the record regarding the nature of the incidents, the FDIC did not provide the Congress with accurate and complete information about the incidents.

Finally, with regard to document production, the SST Committee had requested that the FDIC produce relevant documents and information. The FDIC did not initially respond to these requests in a complete manner and should have been clear in its communications with the Committee as to its approach and progress in complying with the document production requests. Later, the FDIC took steps to better identify and provide responsive records.

Throughout and subsequent to our Special Inquiry, the FDIC took steps to address prior recommendations pertaining to incident and breach response. In addition, we made 13 recommendations in this Special Inquiry report to address the systemic issues associated with the FDIC's incident response and reporting and interactions with the Congress.

FDIC OIG Investigations Seek to Ensure Integrity in the Banking Sector

OIG investigations over the past months continued to complement our audit and evaluation work. Our investigative results over the 12 months ending March 31, 2019, included the following: 64 indictments; 35 arrests; 43 convictions; and potential monetary recoveries (fines, restitution, and asset forfeitures) of over $354 million.

Our current cases involve fraud and other misconduct on the part of senior bank officials, and include money laundering, embezzlement, bank fraud, and other financial crimes. The perpetrators of such crimes can be those very individuals entrusted with governance responsibilities at the institutions—directors and bank officers. In other cases, parties providing professional services to the banks and customers, others working inside the bank, and customers themselves are principals in fraudulent schemes. The FDIC OIG also investigates significant matters of wrongdoing and misconduct relating to FDIC employees and contractors.

Our Office is committed to partnerships with other OIGs, the Department of Justice (DOJ), and other state and local law enforcement agencies in pursuing criminal acts in open and closed banks and helping to deter fraud, waste, and abuse. The OIG also actively participates in many financial fraud working groups nation-wide to keep current with new threats and fraudulent schemes that can undermine the integrity of the FDIC's operations and the financial services industry as a whole.

The FDIC OIG's Office of Investigations also continues to identify emerging financial fraud schemes that affect FDIC-supervised and insured institutions. Our relationships with DOJ's Money Laundering and Asset Recovery Section, and DOJ's Fraud Section and Anti-Trust Division, have allowed us to play a lead role in money laundering and foreign currency exchange rate manipulation investigations. We also work with other agencies, including the Small Business Administration, to identify fraud in the guaranteed loan portfolios of FDIC-supervised institutions. These investigations are important, as large-scale fraud schemes can significantly affect the financial industry and the financial condition of FDIC-insured institutions.

Former Senior Employee at FDIC Convicted of Stealing Confidential Documents

On December 11, 2018, a former senior employee in the FDIC's Office of Complex Financial Institutions (OCFI) was convicted of two thefts of government property in the possession of the FDIC. OCFI was created after passage of the Dodd-Frank Wall Street Reform and Consumer Protection Act to oversee and conduct, if necessary, an orderly bankruptcy of the world's largest banks and financial institutions. Each of these banks and financial institutions is required to file resolution plans, referred to as "living wills," with the FDIC. The plans contain confidential information about the bank, including its assets, business operations, data center locations, critical vendors, agreements with other banks, and potential weaknesses or other deficiencies that pose risk during a time of financial crisis.

In August 2015, the then-FDIC employee used her office computer to review listings for and apply for jobs with financial institutions that filed living wills with the FDIC. On August 27, 2015, one day after being contacted about a possible position at one of the banks, she logged on to a secure FDIC database and printed living will information

for that bank. On September 16, 2015, she resigned her position at the FDIC. A review of FDIC Data Loss Prevention software revealed that on her last day of work, the then-FDIC employee copied numerous electronic files from the FDIC network to external USB drives, including living wills for U.S. banks where she had been seeking employment.

Former Bank President Sentenced to Prison and Ordered to Pay $137 Million

On December 14, 2018, the former president and CEO of The Bank of Union in El Reno, Oklahoma, was sentenced to 4 years in federal prison followed by 2 years of supervised release for making a false statement to the FDIC. He had previously pled guilty to this charge in 2017. The sentence requires the former president to pay over $137 million in restitution, over $97 million of which is owed to the FDIC.

State banking regulators closed The Bank of Union in 2014 because of the bank's loan losses, and the FDIC was appointed as receiver. According to a 2016 indictment, the former president defrauded the bank in several ways: (1) by issuing loans with insufficient collateral and falsifying financial statements for several high-dollar bank borrowers; (2) by originating nominee loans to circumvent the bank's legal lending limit; (3) by concealing the bank's true financial condition from the Board of Directors; (4) by soliciting a fraudulent investment; and (5) by falsely representing the bank's true status to the FDIC.

Over a 4-year period, the former president conspired with borrowers by issuing them millions of dollars in loans secured by collateral they did not have and issuing them new loans to keep them off of overdraft reports. The former president misled the Board of Directors by falsely stating the borrowers were paying down their loans.

The former president also defrauded a partial owner and investor in the bank by convincing him to wire nearly $40 million. The former president falsely represented to the investor that the bank was growing rapidly and performing well and that his investment would not be at risk, despite knowing that the bank was on the brink of failure and needed an immediate capital infusion.

Finally, the former president was charged with falsely representing the bank's loan status to the FDIC. Between September 2012 and September 2013, he continued to renew certain unpaid loans by capitalizing unpaid interest. Pursuant to a 2013 FDIC examination, he allegedly falsely represented that he had not renewed or extended any loans without full collection of the interest due during that time period. He also falsely represented in writing that the bank had total equity capital of more than $36 million in July 2013, when he knew the bank's equity capital was significantly less.

The partial owner who wired money for the bank's benefit is due $40 million of the restitution amount, and the remaining $97 million is due to the FDIC, which lost money when it assumed the bank's liabilities as receiver in January 2014.

South Florida Resident Convicted of $100 Million International Fraud Scheme that Led to Collapse of One of Puerto Rico's Largest Banks

On February 4, 2019, the former chairman and CEO of a pharmaceutical company was convicted of eight counts of wire fraud affecting a financial institution after a three-week trial in the Southern District of Florida. The former CEO's scheme triggered a series of events leading to the insolvency and collapse of Westernbank of Puerto Rico.

According to evidence presented at trial, from 2005 to 2007, the individual served as chairman and CEO of Inyx, Inc., a publicly-traded multinational pharmaceutical manufacturing company. Beginning in early 2005, the then-CEO caused Westernbank to enter into a series of loan agreements in exchange for a security interest in Inyx's assets. Under the loan agreements, Westernbank agreed to advance money based on Inyx's customer invoices from "actual and bona fide" sales.

However, the then-CEO orchestrated a scheme to defraud Westernbank by causing numerous Inyx employees to make tens of millions of dollars' worth of fake customer invoices purportedly payable by customers in the United

Kingdom, Sweden, and elsewhere. The then-CEO caused these invoices to be presented to Westernbank as valid invoices and made false representations to Westernbank about purported repayments from lenders in order to lull Westernbank into continuing to lend money to Inyx. He also fraudulently represented to Westernbank executives that he had additional collateral, including purported mines in Mexico and Canada worth hundreds of millions of dollars, to induce Westernbank to lend additional funds.

The then-CEO caused Westernbank to lend approximately $142 million and diverted tens of millions of dollars for his own personal benefit, including to buy a private jet, luxury homes and cars, luxury hotel stays, and extravagant jewelry and clothing expenditures.

In or around June 2007, Westernbank declared the loan in default and ultimately suffered losses exceeding $100 million. These losses later triggered a series of events leading to Westernbank's insolvency and ultimate collapse. At the time of its collapse, Westernbank had approximately 1,500 employees and was one of the largest banks in Puerto Rico.

In addition, the then-CEO knowingly deposited a $3 million check at Mellon Bank from the purported sale of his private jet. At the time of its deposit, he knew that the check was worthless; he had actually agreed to sell his plane to a different buyer. After receiving a provisional credit for the check from Mellon Bank, the then-CEO wired out all of the provisional credit, including a $1 million wire to his personal account in Canada. Upon Mellon Bank's request to reverse this $1 million wire, he refused to do so, resulting in at least a $1 million loss to Mellon Bank.

Office of Inspector General Federal Housing Finance Agency

Created by the Housing and Economic Recovery Act of 2008 (HERA), the Federal Housing Finance Agency (FHFA or Agency) supervises and regulates (1) the Federal National Mortgage Association (Fannie Mae) and the Federal Home Loan Mortgage Corporation (Freddie Mac) (together, the Enterprises), (2) the Federal Home Loan Banks (FHLBanks) (collectively, the regulated entities), and (3) the FHLBanks' fiscal agent, the Office of Finance. Since September 2008, FHFA has also served as conservator for the Enterprises. As of year-end 2018, the Enterprises collectively reported approximately $5.4 trillion in assets. The FHLBanks collectively reported roughly $1.1 trillion in assets.

Also created by HERA, the FHFA Office of Inspector General (OIG) conducts, supervises, and coordinates audits, evaluations, investigations, and other activities relating to the programs and operations of FHFA. OIG promotes economy, efficiency, and effectiveness and protects FHFA and the entities it regulates against fraud, waste, and abuse, contributing to the liquidity and stability of the nation's housing finance system. We accomplish this mission by providing independent, relevant, timely, and transparent oversight of the Agency to promote accountability, integrity, economy, and efficiency; advising the Director of the Agency and Congress; informing the public; and engaging in robust enforcement efforts to protect the interests of American taxpayers.

Background

FHFA serves as supervisor of the Enterprises and the FHLBanks, and as conservator of the Enterprises. FHFA's conservatorships of the Enterprises, now in their 11th year, are of unprecedented scope, scale, and complexity. FHFA's dual roles continue to present novel challenges. Consequently, OIG must structure its oversight program to examine FHFA's exercise of its dual responsibilities, which differ significantly from the typical federal financial regulator. Beginning in Fall 2014, OIG determined to focus its resources on programs and operations that pose the greatest financial, governance, and/or reputational risk to the Agency, the Enterprises, and the FHLBanks to best leverage its resources to strengthen oversight.

Our annual Audit, Evaluation, and Compliance Plan describes FHFA's and OIG's roles and missions, explains our risk-based methodology for developing this plan, provides insight into particular risks within four areas, and generally discusses areas where we will focus our audit, evaluation, and compliance resources. In addition to our risk-based work plan, OIG completes work required to fulfill its statutory mandates.

An integral part of OIG's oversight is to identify and assess FHFA's top management and performance challenges and to align our work with these challenges. On an annual basis, we assess FHFA's major management and performance challenges. In October 2018, we identified four challenges (all of which carried over from prior years) and a management concern. In our view, these are the most serious management and performance challenges facing FHFA for the foreseeable future and, if not addressed, could adversely affect FHFA's accomplishment of its mission. (See OIG, Fiscal Year 2019 Management and Performance Challenges (October 15, 2018)). During this reporting period, OIG continued to focus much of its oversight activities on identifying vulnerabilities in these areas and recommending

positive, meaningful actions that the Agency could take to mitigate these risks and remediate identified deficiencies. These challenges and the management concern are:

Supervision of the Regulated Entities – Upgrade Supervision of the Enterprises and Continue Robust Supervision of the FHLBanks

As supervisor of the Enterprises and the FHLBanks, FHFA is tasked by statute to ensure that these entities operate safely and soundly so that they serve as a reliable source of liquidity and funding for housing finance and community investment. Examinations of its regulated entities are fundamental to FHFA's supervisory mission. Within FHFA, the Division of Federal Home Loan Bank Regulation (DBR) is responsible for supervision of the FHLBanks, and the Division of Enterprise Regulation (DER) is responsible for supervision of the Enterprises.

As a former FHFA Director observed, Fannie Mae and Freddie Mac would be Systemically Important Financial Institutions (SIFIs), but for the conservatorships, and are subject to the heightened supervision requirements for SIFIs, except that they are supervised by FHFA, not the Federal Reserve. Because the asset size of the FHLBanks and Office of Finance, together, is a fraction of the asset size of the Enterprises and because the Enterprises are in conservatorship, we determined that the magnitude of risk is significantly greater for the Enterprises. Since the Fall of 2014, the majority of our work on supervision issues has focused on FHFA's supervision of the Enterprises.

Based on our assessments of different elements of DER's supervision program, over the past few years, we identified four recurring themes, which were explained in a roll-up report issued during FY 2017.[4] Those themes are:

1. FHFA lacks adequate assurance that DER's supervisory resources are devoted to examining the highest risks of the Enterprises.

2. Many supervisory standards and guidance issued by FHFA and DER lack the rigor of those issued by other federal financial regulators.

3. The flexible and less prescriptive nature of many requirements and guidance promulgated by FHFA and DER has resulted in inconsistent supervisory practices.

4. Where clear requirements and guidance for specific elements of DER's supervisory program exist, DER examiners-in-charge and subordinate examiners have not consistently followed them.

In that roll-up report, we cautioned that "[w]ithout prompt and robust Agency attention to address the shortcomings we have identified," the "safe and sound operation of the Enterprises cannot be assumed from FHFA's current supervisory program." The findings from subsequent audits, evaluations, and compliance reports regarding FHFA's supervision program for the Enterprises identified additional shortcomings. In light of the observation that the Enterprises would be SIFIs, but for the conservatorships, FHFA must make a heightened and sustained effort to improve its supervision of the Enterprises.

We also looked at elements of FHFA's supervision program for the FHLBanks. While our reports of that work identified some shortcomings, they did not identify significant weaknesses. Like any other federal financial regulator, FHFA faces challenges in appropriately tailoring and keeping current its supervisory approach to the FHLBanks.

Conservatorship Operations – Improve Oversight of Matters Delegated to the Enterprises and Strengthen Internal Review Processes for Non-Delegated Matters

As conservator of the Enterprises since September 2008, FHFA has expansive authority to oversee and direct operations of two large, complex financial institutions that dominate the secondary mortgage market and the

4 See OIG, Safe and Sound Operation of the Enterprises Cannot Be Assumed Because of Significant Shortcomings in FHFA's Supervision Program for the Enterprises (OIG-2017-003, Dec. 15, 2016).

mortgage securitization sector of the U.S. housing finance industry. Under HERA, FHFA, as conservator, possesses all rights and powers of any stockholder, officer, or director of the Enterprises and is vested with express authority to operate the Enterprises and conduct their business activities. Given the taxpayers' enormous investment in the Enterprises, the unknown duration of the conservatorships, the Enterprises' critical role in the secondary mortgage market, and their uncertain ability to sustain future profitability, FHFA's administration of the conservatorships remains a major risk.

FHFA has delegated authority for many matters, both large and small, to the Enterprises. FHFA, as conservator, can revoke delegated authority at any time (and retains authority for certain significant decisions).

Since the Fall of 2014, OIG's body of work has found that FHFA has limited its oversight of delegated matters largely to attendance at Enterprise internal management and board meetings as an observer and to discussions with Enterprise managers and directors. Read together, our findings in these reports show that, for the most part, FHFA, as conservator, has not assessed the reasonableness of Enterprise actions pursuant to delegated authority, including actions taken by the Enterprises to implement conservatorship directives, or the adequacy of director oversight of management actions. FHFA also has not clearly defined the Agency's expectations of the Enterprises for delegated matters and has not established the accountability standard that it expects the Enterprises to meet for such matters. Our work has identified internal control systems at the Enterprises that fail to provide directors with accurate, timely, and sufficient information to enable them to exercise their oversight duties. Likewise, we have identified a lack of rigor by some directors in seeking information from management about the matters for which they are responsible. We have also identified instances in which corporate governance decisions generally reserved to the board of directors have been delegated to management.

As the Enterprises' conservator, FHFA is ultimately responsible for actions taken by the Enterprises, pursuant to authority it has delegated to them. FHFA's challenge, therefore, is to improve the quality of its oversight of matters it has delegated to the Enterprises.

Generally, FHFA has retained authority (or has revoked previously delegated authority) to resolve issues of significant monetary and/or reputational value. FHFA has established written internal review and approval processes for non-delegated matters, designed to provide a consistent approach for analyzing and resolving such matters and for providing decision-makers with all relevant facts and existing analyses. FHFA faces challenges in ensuring that its established processes are followed.

Information Technology Security – Enhance Oversight of Cybersecurity at the Regulated Entities and Ensure an Effective Information Security Program at FHFA

Cybersecurity, as defined by the National Institute of Standards and Technology (NIST), is the process of protecting information by preventing, detecting, and responding to attacks. In May 2017, President Trump issued an executive order to strengthen the cybersecurity of federal networks and critical infrastructure. The Financial Stability Oversight Council (FSOC) has identified cybersecurity oversight as an emerging threat for increased regulatory attention. The Council reported that cybersecurity-related incidents create significant operational risk, impacting critical services in the financial system, and ultimately affecting financial stability and economic health.

As cyberthreats and attacks at financial institutions increase in number and sophistication, FHFA faces challenges in designing and implementing its supervisory activities for the financial institutions it supervises. These supervisory activities may be made increasingly difficult by FHFA's continuing need to attract and retain highly-qualified technical personnel, with expertise and experience sufficient to handle rapid developments in technology.

Computer networks maintained by federal government agencies have proven to be a tempting target for disgruntled employees, hackers, and other intruders. Over the past few years, cyber attacks against federal agencies have increased in frequency and severity. As cyber attacks continue to evolve and become more sophisticated and harder to detect, they pose an ongoing challenge for virtually every federal agency to fortify and safeguard its internal systems and operations.

As conservator of and supervisor for the Enterprises and supervisor for the FHLBanks, FHFA collects and manages sensitive information, including personally identifiable information (PII), that it must safeguard from unauthorized access or disclosure. Equally important is the protection of its computer network operations that are part of the nation's critical financial infrastructure. FHFA, like other federal agencies, faces challenges in enhancing its information security programs, ensuring that its internal and external online collaborative environments are restricted to those with a need to know, and ensuring that its third-party providers meet information security program requirements.

Counterparties and Third Parties – Enhance Oversight of the Enterprises' Relationships with Counterparties and Third Parties

The Enterprises rely heavily on counterparties and third parties for a wide array of professional services, including mortgage origination and servicing. That reliance exposes the Enterprises to counterparty risk, including the risk that the counterparty will not meet its contractual obligations, and the risk that a counterparty will engage in fraudulent conduct. FHFA has delegated to the Enterprises the management of their relationships with counterparties and reviews that management largely through its supervisory activities.

Our publicly reportable criminal investigations include inquiries into alleged fraud by different types of counterparties, including real estate brokers and agents, builders and developers, loan officers and mortgage brokers, and title and escrow companies.

In light of the financial, governance, and reputational risks arising from the Enterprises' relationships with counterparties and third parties, FHFA is challenged to effectively oversee the Enterprises' management of risks related to their counterparties.

Management Concern: Sustain and Strengthen Internal Controls Over Agency and Enterprise Operations

FHFA's programs and operations are subject to legal and policy requirements common to federal agencies. Satisfying such requirements necessitates the development and implementation of, and compliance with, effective internal controls within the Agency.

In January 2019, there was a leadership change with the appointment of an acting FHFA Director, while the Senate considered the President's nominee for the next FHFA Director (who was subsequently confirmed and took office in April 2019). Key senior positions within FHFA have been filled on an acting capacity for a long period of time (e.g., Chief Operating Officer and, until recently, the Deputy Director of the Division of Conservatorship). Our work demonstrates that FHFA is challenged to ensure that its existing controls, including its written policies and procedures, are sufficiently robust, and its personnel are adequately trained on these internal controls and comply fully with them.

Both Enterprises have also experienced significant leadership changes. For example, in late March 2019, Fannie Mae appointed a new Chief Executive Officer (CEO); that individual had been serving as Interim CEO with the departure of the previous CEO in October 2018. In addition, Freddie Mac announced that its CEO will retire with its current President to take over as CEO in July 2019. Among other things, changes in leadership can lead to lack of attention to internal controls.

Examples of OIG's Oversight Accomplishments: Audit, Evaluation, and Compliance Activities

Supervision of the Regulated Entities

FHFA's Housing Finance Examiner Commissioning Program: $7.7 Million and Four Years into the Program, the Agency has Fewer Commissioned Examiners (COM-2018-006, issued September 6, 2018)

In 2011, FHFA acknowledged that the efficiency and effectiveness of its examination program was impeded by the limited number of commissioned examiners then in its employ, totaling 46. The Agency agreed to develop a Housing Finance Examiner commission program (HFE Program) with the stated objectives of providing examiners with "broad-based knowledge to conduct successful risk-based examinations" and qualifying them "to lead the examination of a major risk area at Fannie Mae, Freddie Mac, and the Federal Home Loan Banks."

Previously, we issued four reports on FHFA's efforts to increase the size of its corps of commissioned examiners and two assessments of the HFE Program. During this semiannual period, we conducted a study to assess whether the HFE Program had increased the number of commissioned examiners on the FHFA staff and to determine how FHFA deployed its commissioned examiners and reported our findings. We found that the Agency has not achieved its goal of increasing the number of commissioned examiners nor is it on track to do so. Since the Agency began awarding HFE commissions in 2014, the total number of its commissioned examiners has decreased from 59 (as of June 2014) to 58 (as of June 2018). Almost seven years after the Agency committed to develop and implement a commissioning program and $7.7 million later, the Agency's examination program continues to be hindered by an insufficient number of commissioned examiners.

We found the HFE Program suffers from a high non-completion rate. Of the 66 examiners who enrolled when the HFE Program first began in 2013, only 6 completed the HFE Program and passed its final examination. By June 2018 more than half (36) were no longer enrolled in the HFE Program. The remaining 24 continued to be enrolled as of June 1, 2018, almost five years into the approximately four-year program, and one-third (8) had completed less than 75% of the Program's requirements after five years. Since 2014, only 9 individuals have graduated from the HFE Program and passed the final examination.

We also assessed the Agency's deployment of its commissioned examiners. FHFA, in its 2013 Performance and Accountability Report, explained that the main objective of the HFE Program was to produce commissioned examiners who are "qualified to lead" examinations of major risk areas at the entities supervised by FHFA. However, that objective has not been fulfilled in practice. DBR records reflect that, for each of the last three supervisory cycles, commissioned examiners led roughly 75% of annual DBR exams. DER records show that, for the 2016 and 2017 annual supervisory cycles, DER initiated a total of 53 targeted examinations (defined by FHFA as "a deep or comprehensive assessment" of areas of high importance or risk) and none of these 53 targeted exams was led by an HFE commissioned examiner.

Based on our prior reports and the fieldwork for our September 2018 report, we hold the view that the multiple failures in FHFA's administration of its HFE Program have derailed efforts to produce the HFE commissioned examiners that the Agency claimed to need. We questioned the $7.7 million in costs to develop, implement, and staff the HFE Program in light of the failure of that Program to yield the anticipated results.

Conservatorship Operations

Special Report on the Common Securitization Platform: FHFA Lacked Transparency and Exercised Inadequate Oversight Over a $2.13 Billion, Seven-Year Project (OIG-2019-005, issued March 29, 2019)

In 2012, FHFA directed the Enterprises to build a Common Securitization Platform (CSP or Platform) to replace their current separate "back-office" systems and to issue a single mortgage-backed security (single security). As originally envisioned, the CSP was intended to facilitate issuance of mortgage-backed securities (MBS) by multiple market participants in a future housing finance system. In May 2014, the then-FHFA Director decided to limit the current scope of the Platform to working "for the benefit of Fannie Mae and Freddie Mac" and committed to transparency in its development.

The first phase of CSP development, Release 1, was rolled out in November 2016. Release 1 allowed Freddie Mac to use the CSP to issue single-family fixed-rate MBS. Under the second phase, Release 2, both Enterprises will use the CSP to issue the new single security. Release 2 is now scheduled for completion by June 2019.

In December 2016, we reported that FHFA had not fully met its commitment to transparency around the development of the CSP. We found that the Agency publicly disclosed only the actual costs incurred to develop and test the CSP; represented to Congress that, as of the first quarter of 2016, the actual and projected costs to develop and test the CSP through 2018 totaled $696 million; and did not disclose to Congress or the public what it knew about the Enterprises' actual and projected integration costs. We also found that FHFA had not publicly disclosed the risks to successful development and implementation of the CSP.

During this reporting period, we conducted a review to determine whether (1) FHFA honored its commitment to transparency about the CSP by disclosing updated projections for the total cost (development and integration) of the CSP and its internal assessment of the risks of this project after December 2016; and (2) FHFA exercised adequate oversight of the CSP project. We found that: (1) FHFA was not transparent; and (2) its oversight of the CSP project was inadequate.

FHFA issued a public update in March 2017, in which it projected a total of $1.12 billion in CSP development costs. However, FHFA did not disclose the projected $955 million cost to integrate the Enterprises' IT systems into the CSP. Because it had conducted a thorough review of the program in late 2016, FHFA was aware that the CSP development was "off track" with a significant risk of untimely completion and additional costs. However, it disclosed no known issues or risks in its March 2017 update. It announced that Release 1 had been implemented but reported that Release 2 would be delayed by six months, until the second quarter of 2019.

Since March 2017, FHFA has provided no further cost information in public updates. Our review of internal FHFA documents found that, as of February 2019, FHFA projected that Platform development costs and Enterprise integration costs through Release 2 will total $2.13 billion by June 30, 2019. Although the Agency has asserted that the Platform was developed using standard industry technology and interfaces, it acknowledged to us that it has yet to develop plans, establish a timetable, and determine the costs for use of the Platform by any third party.

FHFA's Approval of Senior Executive Succession Planning at Freddie Mac Acted to Circumvent the Congressionally Mandated Cap on CEO Compensation (EVL-2019-002, issued March 26, 2019) and FHFA's Approval of Senior Executive Succession Planning at Fannie Mae Acted to Circumvent the Congressionally Mandated Cap on CEO Compensation (EVL-2019-001, issued March 26, 2019)

During this reporting period, we issued two reports that evaluated FHFA oversight of the Enterprises' boards of directors' succession planning efforts.

Under HERA, FHFA is empowered to operate the Enterprises "with all the powers of the shareholders, the directors, and the officers" while the Enterprises remain in conservatorship. FHFA delegated responsibility to the respective boards of directors to develop a succession plan for the CEO and President positions and select candidates for vacant CEO and President positions, and the selections are subject to review by FHFA as conservator. According to FHFA, it has, as a practical matter, chosen to approve such selections after review. FHFA has retained the responsibility to approve compensation actions for senior executive officers.

FHFA reported to us that the then-FHFA Director raised the need for succession planning with the Fannie Mae Board Chair in 2018, following the CEO's notice of his likely departure. In June 2018, the Board Chair submitted the Board's written proposed transition plan for directors and senior executive leadership (Board Transition Plan) to FHFA for approval. The Fannie Mae Board Transition Plan represented that the statutory cap of $600,000 on compensation for Enterprise CEOs imposed by the Equity in Government Compensation Act of 2015 created challenges to recruit internal and external qualified candidates for the CEO position.

To address these challenges, the Board Transition Plan recommended a change to Fannie Mae's management structure by filling the positions of President and CEO with separate individuals. (Since 2008, those positions had been held by one individual.) Under the Fannie Mae Board Transition Plan, certain responsibilities previously executed by the individual holding the CEO and President positions would be assigned to the position of President. The Fannie Mae Board proposed that the annual compensation for the President position should be no less than Fannie Mae's

most highly compensated Fannie Mae officer, which was then $3.25 million. The then-FHFA Director approved the Board Transition Plan in July 2018.

We found that FHFA's approval of the Fannie Mae Board Transition Plan acted to circumvent the congressionally mandated cap of $600,000 on CEO compensation. By authorizing Fannie Mae to fill the positions of CEO and President with two separate individuals and transfer substantial responsibilities from the CEO and President to the President position, FHFA permitted Fannie Mae to compensate its President at a level more than five times greater than the statutory cap. After the current President had served in the position for less than seven weeks, the Board approved an 11% increase in the President's target compensation, raising it to $3.6 million per year, which FHFA approved in October 2018. Fannie Mae is now compensating its interim CEO and President a total of $4.2 million to execute the same responsibilities for which it had previously paid $600,000.

In addition, we found that the then-FHFA Director overrode internal controls for processing, tracking, and monitoring requests for conservator approval, which he was authorized to do, when he determined to review the Fannie Mae Board Transition Plan directly, without any staff analysis or recommendation. The decision by the then-FHFA Director to override established FHFA internal controls for conservator review and approval of an Enterprise request created an information vacuum within the Division of Conservatorship (DOC) and rendered it unable to execute its responsibilities.

To address these shortcomings, we recommended that FHFA (1) re-assess the appropriateness of the annual compensation award of $3.6 million to the Fannie Mae President; and (2) establish a process for maintaining and monitoring sensitive conservator requests in its tracking system. FHFA disagreed with our first recommendation and agreed with our second recommendation.

In a companion report, we focused on FHFA oversight of the Freddie Mac Board of Directors. FHFA reported that Freddie Mac's CEO, who has served as CEO since May 2012, advised the Freddie Mac Board that he intends to retire during the second half of 2019. In May 2018, the Freddie Mac Board Chairman provided the then-FHFA Director with a Board Transition Plan that included recommendations to address this transition. The Freddie Mac Board Transition Plan stated that the statutory cap on the compensation of Enterprise CEOs of $600,000 created challenges to Freddie Mac's ability to recruit qualified external candidates and an external search could be disruptive to existing internal leadership. The then-FHFA Director responded in writing to the Board Transition Plan, advising the Freddie Mac Board that the plan "strikes us as being very reasonable" and concurred with the Board's request to forego an external search. Over the following months, the Freddie Mac Board Transition Plan was refined to include: designation of the senior executive who would succeed the CEO after his retirement; creation of a "Deputy CEO" position to be filled by this designated senior executive for one year; mentorship of the Deputy CEO by the CEO until his retirement; and a proposed compensation package for the Deputy CEO position at a level no less than the highest paid executive who reported to the CEO (then $3.25 million).

Acting upon a written staff recommendation, the then-FHFA Director approved this executive compensation package of $3.25 million for the Deputy CEO position on August 15, 2018. Despite FHFA's earlier response to Freddie Mac that the Board Transition Plan was reasonable, FHFA notified Freddie Mac after August 15, 2018, that the Enterprise would need to conduct an external search for a CEO and title the new position "President," rather than Deputy CEO. FHFA approved creation of the position of President with the understanding that the individual in that position would serve as the "understudy" to the CEO and execute only those responsibilities previously executed by the CEO and now delegated to him over a one-year period.

We found that FHFA's approval of a $3.25 million compensation package for the Deputy CEO position (which was never created) and subsequent approval of the same compensation for the President position, acted to circumvent the congressionally mandated cap of $600,000 on CEO compensation. As a result of FHFA's approval, Freddie Mac provided a total of $3.85 million in compensation for the same set of CEO responsibilities for which it previously paid $600,000. We recommended that FHFA re-assess the appropriateness of the Freddie Mac President's $3.25 million compensation. FHFA disagreed with our recommendation.

Fannie Mae Purchased Single-Family Mortgages, Including those Purchased through Master Agreements, in Accordance with Selected Credit Terms Set Forth in its Selling Guide for 2015 – 2017 (AUD-2019-006, issued March 27, 2019)

Fannie Mae manages the quality of its mortgage purchases by requiring mortgage sellers to comply with its Selling Guide. The Selling Guide sets forth Fannie Mae's underwriting standards and eligibility guidelines, as well as its policies and procedures related to sales of single-family mortgages to it. Fannie Mae's underwriting standards are developed, in part, based on risk-based criteria which enables it to evaluate a borrower's willingness and capacity to repay a mortgage and the value of the property to ensure that it provides adequate collateral for the mortgage. Risk-based criteria relating to a borrower's willingness and capacity include the debt-to-income (DTI) ratio, loan-to-value (LTV) ratio, and credit score while collateral value is assessed through property valuation. None of these criteria are considered in a vacuum but are considered together to build a snapshot of the potential risk level of the mortgage.

Historically, many mortgage sellers sought to sell mortgages to Fannie Mae that did not meet the underwriting standards and/or eligibility requirements in the Selling Guide. Fannie Mae captured these negotiated terms, referred to as variances, with its mortgage sellers in a document called a "master agreement." Each master agreement supplemented the general requirements of the Selling Guide and set forth the additional negotiated terms under which Fannie Mae agreed to purchase mortgages from the mortgage seller.

We completed an audit in which we sought to assess FHFA's oversight of Fannie Mae's master agreements with its single-family mortgage sellers from 2015 through 2017 (review period). As part of the audit, we analyzed master agreements for Fannie Mae's top three single-family mortgage sellers and found no variation between the terms in the master agreements for DTI ratio, LTV ratio, credit score, and property valuation method from the terms for the same element set forth in the Selling Guide.

We also obtained information from FHFA and Fannie Mae and analyzed loan-level data in FHFA's Mortgage Loan Integrated System (MLIS) for all single-family mortgage sellers to determine whether the credit terms for DTI ratio, LTV ratio, credit score, and property valuation methods for the mortgages purchased by Fannie Mae differed from those credit terms in the governing Selling Guide. For the single-family mortgages purchased by Fannie Mae during the review period (nearly 6.46 million mortgages with a total unpaid principal balance of $1.49 trillion), through our analysis, we identified some differences with these credit terms, but those differences were not material (less than one-tenth of one percent of the mortgages purchased by Fannie Mae during the review period).

We did, however, identify issues with the reliability of certain data fields in MLIS. Specifically, we found instances where data fields for our selected credit terms were either missing information or were shown as "unknown." particularly with respect to the data field for property valuation method. FHFA agreed with our recommendation to address this MLIS data field.

Information Technology Security

External Penetration Test of FHFA's Network and Systems During 2018 **(AUD-2019-003, issued February 11, 2019)**

To support our ongoing oversight of FHFA's implementation of the Federal Information Security Modernization Act of 2014 (FISMA), we completed an audit during this period to determine whether FHFA's security controls were effective to protect its network and systems against external threats.

We found that FHFA's security controls successfully prevented us from gaining unauthorized access to its systems via the internet, wireless access points, or phishing email. Through a vulnerability scan of the Internet Protocol addresses registered to FHFA, we identified two medium severity vulnerabilities related to an outdated encryption protocol and web cookies; however, we were not able to exploit these vulnerabilities to gain unauthorized access to FHFA's systems. Upon receiving our vulnerability scan reports, FHFA management reported that a plan was underway to replace systems with an outdated encryption protocol and FHFA took action to address the web cookie vulnerability.

We also performed a test that revealed FHFA employees were susceptible to email phishing. FHFA agreed with our three recommendations to address these matters.

Counterparties and Third Parties

FHFA Should Re-evaluate and Revise Fraud Reporting by the Enterprises to Enhance its Utility **(EVL-2018-004, issued September 24, 2018)**

HERA requires the Enterprises to establish and maintain procedures designed to discover and report instances of fraud and possible fraud. In 2010, FHFA promulgated a regulation to implement HERA's fraud reporting requirements. This regulation requires each Enterprise to report to the FHFA Director instances of fraud and possible fraud relating to the purchase or sale of fraudulent loans or financial instruments. In addition, FHFA Advisory Bulletin 2015-02, Enterprise Fraud Reporting, directs the Enterprises to submit monthly and quarterly fraud status reports. FHFA provided standardized templates for specifying the information the Enterprises should include in their monthly and quarterly reports. Similarly, under the Bank Secrecy Act, the Enterprises are required to report fraud and other suspicious activities to the Financial Crimes Enforcement Network, a Treasury bureau.

FHFA is responsible for examining and monitoring the Enterprises' fraud risk management practices and overseeing the Enterprises' compliance with FHFA fraud reporting requirements. FHFA recognizes that timely fraud reporting to the Agency is essential to maintain the Enterprises' safe and sound condition.

We reviewed the applicable requirements and guidance governing the Enterprises' obligations to detect and report fraud, the Enterprises' fraud detection and reporting practices, and FHFA's use of the Enterprises' fraud reports. We found that FHFA does not make any documented, systematic use of the content of the Enterprises' fraud reports. FHFA advised us that it recently began to analyze trends of the information in the Enterprises' fraud reports. While FHFA has considered using that information for risk analysis, it has not developed any framework in which to assess that information.

Because Congress required the Enterprises to prepare fraud reports and FHFA has directed them to submit detailed monthly and quarterly reports to meet this statutory requirement, we recommended that FHFA re-evaluate the fraud information it requires from the Enterprises and revise, as appropriate, its existing reporting requirements to enhance the utility of these reports with the goal of using these reports to inform its supervisory activities with respect to the risk that fraud poses to the Enterprises. FHFA agreed with our recommendation.

Examples of OIG Investigative Accomplishments

OIG is vested with statutory law enforcement authority that is exercised by its Office of Investigations (OI). OI conducts criminal and civil investigations into those, whether inside or outside of government, who waste, steal, or abuse in connection with the programs and operations of the Agency and the regulated entities. OI is staffed with special agents (SAs), investigative counsel, analysts, and attorney advisors who work in field offices across the nation. OI has offices located within several federal judicial districts that lead the nation in reported instances of mortgage fraud: the Southern District of Florida; the Northern District of Illinois; the District of New Jersey; and the Central District of California.

OI specializes in deterring and detecting fraud perpetrated against the Enterprises. OI's focus on fraud committed against the Enterprises is essential to the well-being of the secondary mortgage market. Collectively, Fannie Mae and Freddie Mac hold more than $5 trillion worth of mortgages on their balance sheets. Each year the Enterprises acquire millions of mortgages worth several hundreds of billions of dollars. The potential for fraud in these circumstances is significant.

Civil Cases

OI continued to participate in residential mortgage backed securities (RMBS) investigations and other civil investigations by working closely with U.S. Attorneys' offices to investigate allegations of fraud committed by financial institutions and individuals.

The Royal Bank of Scotland Agrees to Pay $4.9 Billion for Financial Crisis-Era Misconduct

In August 2018, the Department of Justice (DOJ) announced a $4.9 billion settlement with The Royal Bank of Scotland Group plc (RBS Group) resolving federal civil claims that RBS Group's subsidiaries in the United States (RBS) misled investors in the underwriting and issuing of RMBS between 2005 and 2008. The penalty is the largest imposed by DOJ for financial crisis-era misconduct at a single entity.

Using recordings of contemporaneous calls and emails of RBS executives, the settlement includes a statement of facts alleged by DOJ (but not admitted or agreed to by RBS) that details how RBS routinely made misrepresentations to investors about significant risks it failed to disclose about its RMBS.

For example, RBS's reviews of loans backing its RMBS (known as "due diligence") confirmed that loan originators had failed to follow their own underwriting procedures, and that their procedures were ineffective at preventing risky loans from being made. As a result, RBS routinely found that borrowers for the loans in its RMBS did not have the ability to repay and that appraisals for the properties guaranteeing the loans had materially inflated the property values RBS's RMBS contained, as its Chief Credit Officer put it, "total [expletive deleted] garbage" loans with "random" and "rampant" fraud that was "all disguised to, you know look okay kind of . . . in a data file." RBS never disclosed that these material risks both existed and increased the likelihood that loans in its RMBS would default.

RBS's due diligence practices did not remove fraudulent and high-risk loans from its RMBS. In fact, RBS executives internally discussed how RBS's due diligence process was "just a bunch of [expletive deleted]."

To develop and maintain business relations with originators, RBS agreed to limit the number of loans it could review (due diligence caps) and/or limit the number of materially defective loans it could remove from an RMBS (kick-out caps). As a result, RBS securitized tens of thousands of loans that it determined or suspected were fraudulent or had material problems without disclosing the nature of the loans to investors.

Through its scheme, RBS earned hundreds of millions of dollars, while simultaneously ensuring that it received repayment of billions of dollars it had lent to originators to fund the faulty loans underlying the RMBS. RBS used RMBS to push the risk of the loans, and tens of billions of dollars in subsequent losses, onto unsuspecting investors across the world, including non-profits, retirement funds, and federally-insured financial institutions. As losses mounted, and after many mortgage lenders who originated those loans had gone out of business, RBS executives showed little regard for this misconduct and made light of it. For example, after RBS's Head Trader received an e-mail from a friend stating "[I'm] sure your parents never imagine[d] they'd raise a son who [would] destroy the housing market in the richest nation on the planet," the Head Trader answered, "I take exception to the word 'destroy.' I am more comfortable with 'severely damage.'"

According to OIG's Associate Inspector General Jennifer Byrne: "The actions of RBS resulted in significant losses to investors, including Fannie Mae and Freddie Mac, which purchased the Residential Mortgage-Backed Securities backed by defective loans."

Criminal Cases

11 Individuals and 3 Businesses Charged in National Foreclosure Relief Scheme, Ohio

In March 2019, 11 people from across the country and three businesses were indicted for their roles in a scheme to defraud distressed homeowners by falsely representing that they could help the victims save their homes.

According to the 26-count indictment, the co-conspirators took advantage of homeowners' desperation to save their homes and used money from homeowner victims to personally enrich themselves. It is alleged that co-conspirators were involved in a multilevel marketing scheme, which promised affiliates commissions by recruiting distressed homeowners to companies they controlled, including MVP Home Solutions, LLC, Bolden Pinnacle Group Corp., and Silverstein & Wolf Corp. They used multiple ways to recruit affiliates, including conference calls and direct mailings. For example, some co-conspirators hosted weekly conference calls where participants from across the country dialed in to hear details of the scheme and share sales strategies. During the calls, co-conspirators encouraged affiliates to recruit homeowners to their companies on the promise of easy money.

Some co-conspirators also allegedly promoted, organized, and attended conferences in which affiliates came to hear details of the scheme in person. For example, some co-conspirators organized and participated in a national conference in Columbus, Ohio, in April 2015 in which they provided "deep impact training" and techniques for affiliates to convince homeowners to enroll in Bolden Pinnacle Group Corp. and Silverstein & Wolf Corp. programs.

Affiliates were encouraged to be aggressive in recruiting homeowners. Affiliates used online databases and court records to identify vulnerable, financially distressed homeowners who had recently received notice of foreclosure on their home.

According to the indictment, some co-conspirators mailed more than 22,000 postcards promising that they could "stop foreclosure" or "stop the sheriff sale" for a fixed fee. Co-conspirators also reached out to homeowners using Craigslist ads, websites, emails, and social media platforms.

On the promise of reducing or eliminating mortgage obligations in exchange for a fee, initial recruiters would collect payments from homeowners and refer the victims to the co-conspirator's companies.

Among other things, the referral programs promised to negotiate with mortgage lenders on the homeowners' behalf for the purchase of the mortgage notes at a discount, negotiate the sale of their home and release of their mortgage loans through a short sale and/or deed in lieu of foreclosure sale, stop an imminent foreclosure sale, remove the mortgage lien via a tender offer, and achieve short sale prices at a fraction of the value of the outstanding lien/note.

Further, co-conspirators represented that they had "proprietary" methods or "legal tactics" to help homeowners stall or completely avoid foreclosure. In actuality, the indictment says co-conspirators persuaded homeowners to file chapter 13 bankruptcies in order to delay foreclosure actions.

Co-conspirators allegedly filed skeletal bankruptcy petitions that they called "pump fakes." These petitions intentionally failed to disclose the co-conspirators as preparers and named the homeowners as filing pro se. Any relief from foreclosure delay was temporary until the bankruptcy court dismissed the proceeding.

In 2014 alone, one co-conspirator allegedly prepared and filed petitions for 30 homeowners without their knowledge.

The Enterprises suffered losses because of this scheme.

Vice President of Real Estate Management Company and Managing Director of Commercial Real Estate Financing Firm Pled Guilty in Multi-Million Dollar Mortgage Fraud Scheme, New York

Between December 2018 and March 2019, Kevin Morgan and Patrick Ogiony were charged by information and pled guilty to conspiracy to commit bank fraud.

According to court documents, Kevin Morgan and Ogiony, along with co-defendants Todd Morgan, Frank Giacobbe, and others, conspired to defraud financial institutions and the Enterprises. Kevin Morgan was employed as a Vice President at Morgan Management, LLC, a real estate management company that managed more than 200 multi-family properties. Todd Morgan also was employed by Morgan Management as a Project Manager. Kevin and Todd Morgan worked with Frank Giacobbe, who owned and operated Aurora Capital Advisors, LLC, a mortgage

brokerage company, and Patrick Ogiony, an Aurora employee, to secure financing for properties managed by Morgan Management or certain principals of Morgan Management.

Kevin Morgan, Ogiony, and others created and provided false information to lenders, the Enterprises, and servicers, including reporting inflated revenues and reduced expenses for the properties managed by Morgan Management. This resulted in the financial institutions issuing loans for larger amounts than they would have authorized had they been provided with truthful information.

The co-defendants misled the financial institutions regarding the occupancy of properties. For example, Kevin Morgan and Ogiony conspired to provide false rent rolls to lenders and appraisers on a variety of dates, overstating either the number of renters in a property and/or the rent paid by occupants; conspired to provide false and inflated income statements for the properties; and worked with others to deceive inspectors into believing that unoccupied apartments were, in fact, occupied.

In one such instance, Kevin Morgan, Ogiony, and others provided false information to Berkadia Commercial Mortgage LLC and Freddie Mac, in connection with Rochester Village Apartments at Park Place, a multi-family residential community owned by certain Morgan Management principals. The false information included inflated income derived from storage unit rentals, parking revenue, and apartment leases. Additionally, during the construction phase, apartments were reported to lenders as "occupied" prior to the issuance of the certificates of occupancy. At another property, radon testing procedures were falsified to secure financing.

In addition, Kevin Morgan, Ogiony, and others made misrepresentations to the lending institutions to conceal the unauthorized use of loan proceeds by Morgan Management and its principals. Loan funding was used to maintain or improve other properties managed by Morgan Management, and to satisfy debts associated with other properties managed by Morgan Management. For example, the defendants included a fictitious $2.5 million debt in a loan application, purportedly owed to a Morgan Management controlled entity and created a fabricated payoff letter for that debt to increase the amount of the loan in connection with a property known as Autumn Ridge.

Charges are pending against Giacobbe and Todd Morgan. The investigation revealed fraud in at least 23 loans issued for over $500 million, secured by at least 21 different properties.

Loss calculations are ongoing. Some loans involved in this scheme were purchased or securitized by the Enterprises.

Ex-Fannie Mae Employee Found Guilty and Fannie Mae Real Estate Owned (REO) Broker Pled Guilty in Multi-Million Dollar Scheme Involving Property Listings and Approval of Below-Market Sales, California

In February 2019, Shirene Hernandez was found guilty at trial on charges of wire fraud and deprivation of honest services involving a scheme where she received bribes and kickbacks from brokers in exchange for Fannie Mae real estate listings and for approving the discounted sales of Fannie Mae-owned properties.

According to the evidence presented at a five-day trial, Hernandez was a sales representative at Fannie Mae. As part of its operations, Fannie Mae acquires properties through foreclosures and other methods, and then it manages and sells those properties for Fannie Mae's benefit. Since at least 2012, Fannie Mae's profits have gone to the U.S. Treasury for the benefit of U.S. taxpayers.

As a sales representative, Hernandez assigned Fannie Mae-owned properties to real estate brokers and approved sales of the properties based on offers the brokers submitted. In violation of Fannie Mae rules and federal law, Hernandez approved sales of Fannie Mae-owned properties at discounted prices to herself and to the brokers who paid her kickbacks. She also received bribes – mostly in cash payments – in return for listing opportunities and commissions that brokers earned on real estate sales.

Hernandez also assigned listings to family members who earned nearly $2 million in commissions in less than three years. Other brokers who paid kickbacks earned millions more. For her part in the scheme, Hernandez received

more than $1 million in benefits, including the cash kickbacks that she received, and the value of a property that she obtained with kickback money.

As part of the scheme, Hernandez purchased a Fannie Mae-owned property in Sonoma, California, that she was responsible for selling, and she rejected higher, market-priced offers in favor of her own below-market price. Hernandez purchased the Sonoma property through intermediaries and affiliates that she controlled, selling it first to a company affiliated with a broker who was bribing her, then directing the broker to transfer the property to her sister-in-law, who paid for the property with a duffel bag filled with $286,450 in cash from Hernandez – far below the market price. The Sonoma property was rented out and Hernandez received the rent proceeds.

In a related case, in January 2019, Peter Michno, a broker, was charged and pled guilty to conspiracy to commit wire fraud involving deprivation of honest services for his role in this scheme.

According to the plea agreement, Michno was a Fannie Mae-approved REO broker entitled to receive a commission from the sale of REO properties as compensation for his services. Michno was not authorized to purchase Fannie Mae REO properties for himself or for his friends, relatives, and associates or permitted to pay referral fees, bribes, or kickbacks to Fannie Mae employees.

Michno paid co-conspirators, employed by Fannie Mae, cash bribes and kickbacks in exchange for the assignment of listings and the approval of below-market sales of Fannie Mae REO properties to him and his affiliates. Michno then transferred some of these properties to his co-conspirators as a kickback for the performance of their official duties.

Former Business Owner Convicted in Federal Court for Over $49 Million Bank Fraud, Maryland

In August 2018, Mark Gaver was convicted by a federal jury on charges of bank fraud and money laundering arising from a scheme in which he obtained over $49 million in bank financing for his company Gaver Technologies, Inc. (GTI), using false and fraudulent financial statements, balance sheets, and certifications of outstanding accounts receivable.

According to the evidence presented at his seven-day trial, Gaver formed GTI, an information technology company based in Frederick, Maryland. Gaver submitted materially false financial documents to Santander Bank, a federally insured bank, including fraudulent audit reports and contract status reports, to establish and obtain successive increases in the line of credit from the lender for GTI. Based upon the false documentation submitted by Gaver, the lender ultimately extended $50 million in financing to GTI.

The evidence showed that some of the funds obtained from the lender were used by Gaver to cover regular business expenses and thereby keep GTI open, but Gaver also diverted half of the loan proceeds—approximately $15 million—to his own personal use. For example, Gaver used loan proceeds to pay rental fees of private planes that he used for non-business purposes, as well as to pay for personal pleasure trips to France, Germany, Mexico, Jamaica, and the Bahamas. Gaver also used the funds to purchase vacation homes, including a 4,000-square foot condominium with a view of the Gulf of Mexico in Bonita Springs, Florida, a 2012 Maserati Gran Turismo, a 2011 Mercedes Benz SL Roadster, and a private membership at an exclusive golf club.

Gaver obtained a home equity line of credit that was pledged to the FHLBank of Pittsburgh. The estimated loss to Santander, a member bank of the FHLBank of Pittsburgh, is $49 million.

In December 2018, Gaver was sentenced to 17 years in prison, 3 years of supervised release, and ordered to pay $48,774,308 in restitution and $49,215,606 in forfeiture.

Office of Inspector General
U.S. Department of Housing and Urban Development

The HUD OIG conducts independent audits, evaluations, investigations, and other reviews of HUD operations and programs to promote economy, efficiency, and effectiveness, and protect HUD and its component entities from fraud, waste, and abuse.

Background

While organizationally located within HUD, the OIG operates independently with separate budget authority. Its independence allows for clear and objective reporting to HUD's Secretary and Congress. HUD's mission is to create strong, sustainable, inclusive communities and quality affordable homes for all. HUD is working to strengthen the housing market to bolster the economy and protect consumers, meet the need for quality affordable rental homes, and use housing as a platform for improving quality of life. Its programs are funded through more than $50 billion in annual congressional appropriations.

Within HUD are two entities that have major impact on the Nation's financial system: the Federal Housing Administration (FHA) and Government National Mortgage Association (Ginnie Mae). FHA provides mortgage insurance for single-family homes, multifamily properties, nursing homes, and hospitals. FHA is the largest insurer of mortgages in the world, having insured more than 47.5 million loans since its inception in 1934. FHA mortgage insurance provides lenders with protection against losses as the result of homeowners defaulting on their mortgage loans. In fiscal year 2018, FHA generated more than $1.3 trillion in insured loans. FHA receives limited congressional funding and is primarily self-funded through mortgage insurance premiums.

Ginnie Mae is a self-financing, wholly owned U.S. Government corporation within HUD. It is focused on providing investors a guarantee backed by the full faith and credit of the United States for the timely payment of principal and interest on mortgage-backed securities (MBS) secured by pools of government home loans, which are insured or guaranteed by FHA, HUD's Office of Public and Indian Housing, the U.S. Department of Veterans Affairs (VA), and the U.S. Department of Agriculture (USDA). The purchasing, packaging, and reselling of mortgages in a security form frees up funds that lenders use to provide more loans.

Ginnie Mae has an outstanding portfolio of MBS securities valued at more than $2 trillion. A majority of the MBS securities consist of FHA-insured mortgages. Ginnie Mae offers the only MBS securities carrying the full faith and credit guaranty of the U.S. Government, which means that its investors are guaranteed payment of principal and interest in full and on time. If an issuer of MBS securities fails to make the required pass-through payment of principal and interest to investors, Ginnie Mae is required to assume responsibility for it by defaulting the issuer and assuming control of the issuer's MBS securities pools and the servicing of the loans in those pools.

HUD's Top Management Challenges

OIG continually looks for ways to meet the needs of HUD's beneficiaries and to protect taxpayer dollars. OIG's oversight efforts focus on identifying and addressing HUD's most serious management challenges, several of which relate to financial oversight:

- Ensuring the Availability of Affordable Housing that is Decent, Safe, Sanitary, and in Good Repair
- Protecting the FHA Mortgage Insurance Fund
- Administering Disaster Recovery Assistance
- Instituting Sound Financial Management

Identifying these challenges helps HUD and Congress mitigate the primary risks that hinder HUD in meeting its mission and being able to put taxpayer dollars to the best use. OIG uses these challenges to target its oversight efforts, as demonstrated in the following summaries.

Ensuring the Availability of Affordable Housing that is Decent, Safe, Sanitary, and in Good Repair

Part of HUD's mission is to create quality, affordable homes for all. The housing that HUD insures and funds must be decent, safe, sanitary, and in good repair. Economic and demographic factors, as well as aging housing stock, have created an extreme shortage of housing that is affordable and safe. HUD's challenge is to adapt existing programs to address ever-increasing housing pressures on the Nation's lowest income residents.

One of HUD's financial strategies to address affordable housing is to encourage public housing agencies (PHAs) to transition public housing units to a private-public partnership model. HUD developed its Rental Assistance Demonstration Program (RAD) to give PHAs a tool to preserve and improve public housing properties and address the $26 billion nationwide backlog of deferred maintenance. For fiscal year 2018, Congress increased to 455,000 the number of public housing units that may participate in RAD. OIG audited a number of PHAs in fiscal year 2018 to assess their conversion to the RAD program, and is continuing to conduct PHA RAD audits nationwide in fiscal year 2019. For example:

The Housing Authority of the City of Evansville, IN, Did Not Follow HUD's and Its Own Requirements for Units Converted Under the Rental Assistance Demonstration

The Authority of the City of Evansville, IN, did not follow HUD's and its own requirements for the units converted under RAD. Specifically, it (1) did not ensure that units complied with HUD's housing quality standards before it entered into a housing assistance payments contract, (2) failed to obtain the services of a HUD-approved independent third party to perform housing quality standards inspections for units owned by entities it substantially controlled, and (3) did not apply the correct contract rents for the converted units. As a result, the Authority could not support the eligibility of more than $1 million in housing assistance payments to the entities and more than $10,000 in program funds paid to a contractor for housing quality standards inspection services. Further, the application of incorrect rents led to the underpayment of housing assistance to the entities, so these funds were not available for the administration of the Authority's Project-Based Voucher Program. OIG made multiple recommendations to correct the identified deficiencies. (Audit Report: 2018-CH-1003)

Protecting the FHA Mortgage Insurance Fund

HUD is challenged in protecting the FHA mortgage insurance fund, which insures approximately 25 percent of all mortgages in the United States. Through the Mutual Mortgage Insurance (MMI) fund,[5] FHA insures participating lenders against losses when borrowers default on loans, which allows lenders to make loans to higher risk borrowers. From April 2017 through March 2018, the MMI fund paid out almost $14 billion in reimbursements for defaulted loans. For those claims for which the lender conveyed the property to HUD and HUD resold the property, HUD recovered only about 54 percent of the funds paid out.

Without sufficient controls, oversight, and effective rules, FHA's MMI fund is at risk of unnecessary losses. Further, if insurance fees collected from borrowers cannot support the fund, additional funding from the U.S. Department of the Treasury is required, as authorized for Federal credit programs.

In protecting the FHA and Ginnie Mae programs, HUD is confronted with

- a lack of sufficient safeguards in FHA's mortgage insurance program,
- large losses to the insurance fund due to home equity conversion mortgages,
- an increase in Ginnie Mae's nonbank issuers, and
- potential emerging risks related to a market shift toward an entirely digital mortgage life cycle.

For more than a decade, OIG has reported the need for more safeguards to protect the FHA insurance program, and fiscal year 2018 was no exception. For example:

FHA Insured $1.9 Billion in Loans to Borrowers Barred by Federal Requirements

OIG audited FHA insured loans from calendar year 2016 to determine whether FHA insured loans to borrowers with delinquent Federal debt or who were subject to Federal administrative offset for delinquent child support. FHA insured an estimated 9,507 loans, worth more than $1.9 billion, which were not eligible for insurance because they were made to borrowers with delinquent Federal debt or who were subject to Federal administrative offset for delinquent child support. OIG recommended that FHA put more than $1.9 billion to better use by developing a method for using the U.S. Treasury Do Not Pay portal to identify delinquent Federal debt and delinquent child support to prevent future FHA insured loans to ineligible borrowers. (Audit Report: 2018-KC-0001)

HUD Paid an Estimated $413 Million for Unnecessary Preforeclosure Claim Interest and Other Costs Due to Lender Servicing Delays

OIG audited FHA's preforeclosure sale claim process to determine the amount of unnecessary preforeclosure claim interest and other costs that resulted from lender noncompliance with HUD's loan-servicing timeframe requirements. HUD paid more than $413 million in unnecessary interest and other costs for 27,634 preforeclosure claims because lenders failed to complete servicing actions for defaulted loans within established timeframes. Although the unnecessary amounts were caused by lenders' inaction, HUD reimbursed lenders for these added costs through FHA insurance claims. As a result, the FHA insurance fund incurred unnecessary and unreasonable costs, and fewer funds were available to pay other claims or apply toward reducing FHA borrower mortgage insurance premiums. OIG recommended that HUD implement a change to regulations at 24 CFR (Code of Federal Regulations) Part 203 to require curtailment of preforeclosure interest and other costs caused by lender servicing delays, resulting in more than $413 million in funds to be put to better use. (Audit Report: 2018-LA-0007)

5 The MMI fund is a Federal fund that insures mortgages guaranteed by FHA. The MMI fund supports both FHA mortgages used to buy homes and reverse mortgages used by seniors to extract equity from their homes.

HUD Failed to Enforce the Terms of a Settlement Agreement With Fifth Third Bank Because It Did Not Record Indemnified Loans in Its Tracking System

OIG worked with HUD to resolve outstanding matters related to two September 2015 agreements with Fifth Third Bank (FTB) and its principal subsidiary, Fifth Third Bancorp, a bank holding company. HUD had failed to properly record required indemnifications in its FHA Connection system; therefore, it did not hold FTB accountable to the terms of the settlement agreements. OIG recommended that HUD require FTB to reimburse HUD nearly $312,000 for two loans, for which HUD incurred losses when it sold the properties, and 15 loans for which FHA insurance had been terminated and HUD had paid loss mitigation claims to FTB. OIG also recommended that HUD record in FHA Connection the remaining indemnified loans, avoiding more than $47 million in estimated losses, and that HUD develop and implement controls to ensure that indemnification agreements that result from legal settlements have been properly recorded in FHA Connection. Finally, OIG recommended that HUD take appropriate administrative action against FTB for violations of the settlement agreement. (Memorandum: 2018-CF-0802)

OIG also conducted a civil fraud review of a professional services firm that provides auditing services to clients throughout the United States.

Deloitte & Touche, LLP, Settled Allegations That It Failed To Conduct Taylor, Bean & Whitaker Mortgage Corporation's Audits in Conformance With Generally Accepted Auditing Standards

OIG and the U.S. Attorney's Office conducted a civil fraud review of Deloitte & Touche, LLP, a professional services firm that provides auditing services to clients throughout the United States. Deloitte provided auditing services to its client, Taylor, Bean & Whitaker Mortgage Corporation (TBW). TBW was an FHA-approved direct endorsement lender and as such, was required to submit to HUD annual audited financial statements to maintain its status as a direct endorsement lender. Deloitte served as TBW's independent outside auditor and submitted audit reports on TBW's financial statements for its fiscal years ending April 30, 2002, through April 30, 2008. Deloitte stated in its reports that it had conducted its audits of TBW in accordance with generally accepted auditing standards.

Deloitte & Touche, LLP, entered into a settlement agreement with the Federal Government, agreeing to pay $149.5 million, of which $115 million was to be paid to HUD. Deloitte denied but settled allegations of alleged conduct in connection with its role as TBW's independent outside auditor for fiscal years that ended April 30, 2002, through April 30, 2008. The settlement agreement was neither an admission of liability by Deloitte nor a concession by the United States that its claims were not well founded. (Memorandum: 2018-FO-1802)

OIG has several planned and ongoing audits focused on protecting the FHA mortgage insurance fund. For example, one ongoing audit has the objective of determining whether FHA insured loans made to borrowers that were ineligible due to delinquent Federal tax debt. OIG expects to issue this report in fiscal year 2019. Another audit that recently began focuses on whether FHA insured loans that did not meet the underwriting requirements for special flood hazard areas. OIG expects to issue this report in fiscal year 2020.

In addition, OIG continues to pursue resolution to concerns reported in previous years. OIG reported one of its highest concerns in October 2016, which was that OIG projected that HUD paid claims for nearly 239,000 properties that servicers did not foreclose upon or convey on time. As a result, HUD paid an estimated $2.23 billion in unreasonable and unnecessary holding costs over a 5-year period. These excessive costs were allowed to occur because HUD regulations do not establish a maximum period for filing a claim and do not place limitations on holding costs when servicers do not meet all deadlines. OIG recommended HUD make regulatory changes to establish a maximum claim filing period and sufficient limitation on holding costs after services missed deadlines. To date, HUD has not completed the regulatory changes and our recommendation remains open. These significant, excessive costs will continue to negatively affect the MMI fund until the regulatory changes are completed.

OIG also fears continued large losses to the FHA insurance fund due to home equity conversion mortgages (HECM). HECM is a reverse mortgage program that enables eligible homeowners age 62 and older to borrow funds using the equity in their homes. FHA's fiscal years 2015 through 2018 annual reports on the status of the MMI fund showed an

overall trend of large fluctuations in the value of the HECM portfolio and consistently negative net cash flows ranging from negative $1.6 billion to negative $4.5 billion. In total, the HECM program consumed $13 billion in MMI fund assets and $7 billion in General Insurance fund[6] assets over the 4-year period of fiscal years 2015 through 2018.

OIG is currently conducting an audit with an objective to determine whether HUD designed the HECM program to control the risk of loss related to assignment claims and ensure program viability. Our subobjectives are to (1) identify the full cost of the HECM program and determine whether HUD reported that cost, (2) identify inherent program risks and existing or potential controls to mitigate risks and control costs, and (3) determine whether the HECM program can function as a stand-alone program without a Federal subsidy. OIG expects to issue this report in fiscal year 2019.

HUD is also challenged by the significant increase in the number of nonbanks issuing MBS pools that Ginnie Mae guarantees. In fiscal year 2018, nonbank issuers accounted for 78 percent of Ginnie Mae's single-family MBS issuance volume for the year, up from 51 percent in June 2014 and from 18 percent in fiscal year 2010. As OIG and Ginnie Mae have reported, the increase in the number of nonbank issuers and their complexity continues to present an unmitigated challenge for monitoring efforts. As Ginnie Mae wrote in its 2018 Annual Report, "[a]s more non-banks issue Ginnie Mae's securities, the cost and complexity of monitoring increases as the majority of these institutions involve more third parties in their transactions, making oversight more complicated. In contrast to traditional bank issuers, non-banks rely more on credit lines, securitization involving multiple players, and more frequent trading of [mortgage servicing rights]."

In addition, the mortgage industry is moving toward an entirely electronic loan process. FHA and Ginnie Mae intend to do the same. However, HUD, particularly FHA, has well-known technology challenges. Risks include information security, data transfers and platform integration, and system functionality, all of which could lead to fraudulent activities.

OIG continues to have concerns that an increase in demand on the FHA and VA programs will have collateral implications for the integrity of the Ginnie Mae MBS program, including the potential for increased fraud. Of particular concern is VA loan churning, in which lenders encourage veterans to repeatedly refinance their loans, which can result in the borrower incurring ever increasing fees on their loan. If the fees get too high, the veteran could lose his or her home. The churning produces profits for the lenders at the expense of the veterans, which means that lenders, at times, use deceptive practices to encourage repeated refinances. Since September 2017, the Ginnie Mae – VA Loan Churn Task Force has been working to address these concerns. Ginnie Mae has notified issuers that are outliers among market participants to develop corrective action plans. The action plans are aimed to prevent a few bad actors from raising the cost of homeownership for millions of Americans. A Ginnie Mae executive said "We expect issuers receiving these notices to respond quickly, produce a corrective action plan and come into compliance with our program."

OIG also helps protect the FHA insurance fund by conducting investigations of alleged fraud against the fund, and securing recoveries to the fund. OIG completed 126 single-family investigations of fraud against the FHA insurance fund in fiscal year 2018. A majority of the investigations focused on loan origination fraud, for both forward and reverse mortgages. Recoveries from these cases totaled nearly $500 million. For example:

- The co-owner of a mortgage company was sentenced in U.S. District Court in connection with a guilty plea to 24 counts of wire fraud, 6 counts of bank fraud, and 3 counts of filing a false tax return. The defendant was sentenced to 60 months incarceration, followed by 5 years of probation, and ordered to pay $12.7 million in restitution. The co-owner and three other defendants defrauded numerous lenders into purchasing refinanced FHA and refinanced conventional mortgages that the mortgage company originated, for which the first mortgages were not paid off at the time of closing. The defendants used the closing escrow funds

6 The General Insurance fund (GI) provides a large number of specialized mortgage insurance activities, including insurance of loans for property improvements, cooperatives, condominiums, housing for the elderly, land development, group practice medical facilities, nonprofit hospitals, and reverse mortgages. To comply with the FHA Modernization Act of 2008, activities related to most single-family programs, including HECM, endorsed in fiscal year 2009 and going forward, are in the MMI fund. The single-family activities in the GI fund from fiscal year 2008 and prior remain in the GI fund.

for their personal benefit. OIG, the U.S. Attorney's Office, the Federal Bureau of Investigation (FBI), and the Internal Revenue Service Criminal Investigation division conducted the investigation.

- A former accountant for a Ginnie Mae-approved loan servicing company was sentenced in U.S. District Court in connection with a guilty plea to an Information charging the defendant with reporting false transactions to HUD. The Court sentenced the former accountant to one year of supervised release and ordered her to pay HUD more than $108,000 in restitution. Over a period of about 18 months, the defendant helped the former owner of the loan servicing company divert millions of dollars in mortgage payments to an account that the former owner used for other business and personal expenses. The payments should have been made to Ginnie Mae investors. The former accountant and former company owner then falsely reported to Ginnie Mae that the defrauded borrowers had not made those mortgage payments. Given the shortfall in payments to investors, as well as tax and insurance payments that were supposed to have been escrowed for borrowers but were not, Ginnie Mae was forced to reimburse investors and borrowers, resulting in an approximate $2.8 million loss to HUD. OIG, the U.S. Attorney's Office, the USDA OIG, the VA OIG, and the FBI conducted this investigation.

Administering Disaster Recovery Assistance

HUD has taken on significant leadership responsibilities in the area of disaster recovery assistance. Congress has appropriated more than $84 billion in supplemental funding to HUD for disaster recovery since 2001. This amount includes $35.8 billion appropriated by Congress in supplemental appropriations to HUD in 2017 and 2018 for recovery from Hurricanes Harvey in Texas; Irma in Florida, Georgia, South Carolina, and the U.S. Virgin Islands; Maria in Puerto Rico and the Virgin Islands; and Nate in Mississippi. These disasters resulted in the loss of many human lives and massive property destruction. Further, as the Federal Emergency Management Agency noted, economic recovery is a critical and integral part of disaster recovery. Disasters not only damage property, but also entire markets for goods and services. Considerable Federal funds are contributed to State, local, and Tribal economic recovery as well as to other areas of recovery that necessarily strengthen the economy.

The nature of disaster recovery is inherently risky and susceptible to fraud, given the complexity and range of challenges experienced when recovering from disasters. Disaster recovery appropriation funds may take decades to spend, as their purpose is for long-term recovery, which includes rebuilding homes and communities. HUD awards grants to States and units of local government for disaster recovery efforts. Over the years, HUD has gained more experience and made progress in assisting communities recovering from disasters, but it continues to face these challenges in administering and overseeing these grants:

- codifying the Community Development Block Grant - Disaster Recovery (CDBG-DR) program,
- ensuring that expenditures are eligible and supported,
- ensuring and certifying that grantees are following Federal procurement regulations,
- addressing concerns that citizens encounter when seeking disaster recovery assistance, and
- preventing fraud in disaster recovery assistance.

OIG reported on these areas in recent years, including fiscal year 2018. For example:

HUD's Office of Block Grant Assistance Had Not Codified the Community Development Block Grant Disaster Recovery Program

OIG audited HUD's disaster recovery program to determine whether HUD should codify the CDBG-DR funding as a program in the CFR. Although HUD had managed billions in CDBG-DR funds since 2002, it has not codified the program because it believed it did not have the authority under the Robert T. Stafford Disaster Relief and Emergency Assistance Act and had not determined whether it had the authority under the Housing and Community

Development Act of 1974, as amended. It also believed a Presidential Executive order presented a barrier to codification, as it required HUD to identify two rules to eliminate before creating a new codified rule. OIG believes HUD has the authority under the Housing Act of 1974 and it should codify the program. HUD's use of multiple Federal Register notices to operate the CDBG-DR program presented challenges to the grantees. For example, 59 grantees with 112 active CDBG-DR grants, which totaled more than $47.4 billion as of September 2017, had to follow requirements contained in 61 different Federal Register notices to manage the program. Further, codifying the CDBG-DR program would (1) ensure that a permanent framework is in place for future disasters, (2) reduce the volume of Federal Register notices, (3) standardize the rules for all grantees, and (4) ensure that grants are closed in a timely manner. OIG recommended that HUD work with its Office of General Counsel to codify the CDBG-DR program. (Audit Report: 2018-FW-0002)

The City of New York, NY, Did Not Always Use Disaster Recovery Funds Under Its Program for Eligible and Supported Costs

OIG audited the City of New York, NY's Infrastructure Rehabilitation and Reconstruction of Public Facilities Program to determine whether the City used CDBG-DR funds under its program for eligible and supported costs. The City did not always use CDBG-DR funds under its program for eligible and supported costs. Specifically, for one of two projects reviewed, the City did not (1) have sufficient documentation to show that the use of salary multipliers for overhead and profit, resulting in more than $594,000 in additional costs, was supported and eligible; (2) maintain adequate documentation to show compliance with requirements of the Davis-Bacon Act and related acts; and (3) identify billing and payroll errors made by subcontractors. As a result, HUD did not have assurance that the City used nearly $598,000 in CDBG-DR funds as intended for matching requirements for other federally funded infrastructure projects, and HUD could not be assured that funds were disbursed for only eligible and supported costs that complied with applicable Federal requirements. OIG recommended that HUD require the City to adequately support identified expenditures or reimburse its program from non-Federal funds, and strengthen its controls to ensure compliance with applicable expenditure requirements. (Audit Report: 2018-NY-1007)

Grantees carry out the disaster recovery activities supported by CDBG-DR funding. The ability of these grantees to accomplish recovery from disasters and do so in an efficient and effective manner is critical to the recovery of the affected communities. To help HUD ensure that grantees have this ability, OIG conducts capacity reviews to determine whether these entities have the capability to administer their CDBG-DR grants in accordance with applicable regulations and requirements, particularly with regard to financial management, procurement, monitoring, and reporting. In fiscal year 2018, OIG conducted capacity reviews of the State of Florida's Department of Economic Opportunity (2018-AT-1010) and the State of Texas' General Land Office (2018-FW-1003). In fiscal year 2019, OIG has planned and ongoing capacity reviews and compliance audits of Puerto Rico's Department of Housing, the U.S. Virgin Island's Housing Authority, and the State of Texas' General Land Office, among others. OIG expects to begin reporting on these audits starting in fiscal year 2019.

OIG is also currently conducting an audit of HUD to determine whether it is adequately prepared to respond to upcoming natural and man-made disasters. The audit focuses on disaster policies and procedures regarding interaction with external partners and disaster survivors, as well as for receiving and distributing disaster funds. OIG is coordinating this audit with several other Federal agencies and expects to issue a report in fiscal year 2019 or 2020.

Instituting Sound Financial Management

Over the last several years, HUD's financial management has been operating at "inadequate" or "basic" levels of maturity[7] due to (1) a weak governance structure, including the lack of a confirmed Chief Financial Officer for a number of years; (2) ineffective internal controls; and (3) an antiquated financial management system consisting of legacy systems and manual processes that have precluded HUD from producing reliable and timely financial reports.

7 U.S. Department of the Treasury, Bureau of the Fiscal Service, Federal Financial Management Maturity Model. The Maturity Model is a business tool that helps a CFO self-assess his or her organization's level of financial management discipline, effectiveness, and efficiency. A copy of the model can be found at *https://www.fiscal.treasury.gov/fsservices/gov/fit/MaturityModelHandout2017-05-10.pdf*.

As a result, HUD has been unable to achieve an unmodified audit opinion[8] on its financial statements for the last 6 years and has received a disclaimer of opinion for the last 5 years.

One of HUD's component entities, Ginnie Mae, has also been unable to achieve an unmodified opinion and has received a disclaimer of opinion for the last 5 years due to poor governance and a weak internal control framework. Ginnie Mae has been unable to appropriately account for and support several financial statement line items in accordance with generally accepted accounting principles, including its nonpooled loan asset portfolio, which totaled as much as $6 billion at one point. HUD's unstable financial management environment weakens public confidence in the government programs HUD administers and prevents HUD's stakeholders from being able to rely on HUD's financial position.

8 Codification of Statements on Auditing Standards, AU-C Section 700.11, "The opinion expressed by the auditor when the auditor concludes that the financial statements are presented fairly, in all material respects, in accordance with the applicable financial reporting framework."

Office of Inspector General
National Credit Union Administration

The NCUA OIG promotes the economy, efficiency, and effectiveness of NCUA programs and operations and detects and deters fraud, waste and abuse, thereby supporting the NCUA's mission of providing, through regulation and supervision, a safe and sound credit union system that promotes confidence in the national system of cooperative credit.

Agency Overview

The National Credit Union Administration (NCUA) is responsible for chartering, insuring, and supervising Federal credit unions and administering the National Credit Union Share Insurance Fund (Share Insurance Fund). The agency also manages the Operating Fund,[9] the Community Development Revolving Loan Fund,[10] and the Central Liquidity Facility.[11]

Credit unions are member-owned, not-for-profit cooperative financial institutions formed to permit members to save, borrow, and obtain related financial services. NCUA charters and supervises federal credit unions, and insures accounts in federal and most state-chartered credit unions across the country through the Share Insurance Fund, a federal fund backed by the full faith and credit of the United States government.

The NCUA's mission is to provide through regulation and supervision, a safe and sound credit union system that promotes confidence in the national system of cooperative credit and its vision is to protect consumer rights and member deposits. NCUA further states that it is dedicated to upholding the integrity, objectivity, and independence of credit union oversight. The agency implements initiatives designed to meet these goals.

Major NCUA Programs

Supervision

NCUA supervises credit unions through annual examinations, regulatory enforcement, providing guidance in regulations and letters, and taking supervisory and administrative actions as necessary.

The agency's Office of National Examinations and Supervision (ONES) oversees examination and supervision issues related to consumer credit unions with assets greater than $10 billion and all corporate credit unions, which provide services to consumer credit unions (also known as natural person credit unions). Due to the relative size of their

9 The Operating Fund was created by the Federal Credit Union Act of 1934. It was established as a revolving fund in the United States Treasury under the management of the NCUA Board for the purpose of providing administration and service to the federal credit union system. A significant majority of the Operating Fund's revenue is comprised of operating fees paid by federal credit unions. Each federal credit union is required to pay this fee based on its prior year asset balances and rates set by the NCUA Board.

10 The NCUA's Community Development Revolving Loan Fund, which was established by Congress, makes loans and Technical Assistance Grants to low-income designated credit unions.

11 The Central Liquidity Facility is a mixed-ownership government corporation the purpose of which is to supply emergency loans to member credit unions.

insured share base, they are deemed systemically important to the Share Insurance Fund. In addition, the Dodd-Frank Act gave the Consumer Financial Protection Bureau (CFPB) the authority to examine compliance with certain consumer laws and regulations by credit unions with assets over $10 billion.

Insurance

NCUA administers the Share Insurance Fund, which is capitalized by credit unions and provides insurance for deposits held at federallyinsured credit unions nationwide. The insurance limit is $250,000 per depositor.

Credit Union Resources and Expansion

NCUA's Office of Credit Union Resources and Expansion (CURE) supports credit union growth and development, including providing support to low-income, minority, and any credit union seeking assistance with chartering, charter conversions, by-law amendments, field of membership expansion requests, and low-income designations. CURE also provides access to online training and resources, grants and loans, and a program for preserving and growing minority institutions.

Consumer Protection

NCUA's Office of Consumer Financial Protection (OCFP) is responsible for consumer protection in the areas of fair lending examinations, member complaints, and financial literacy. OCFP consults with the CFPB, which has supervisory authority over credit unions with assets of $10 billion or more. CFPB also can request to accompany NCUA on examinations of other credit unions. In addition to consolidating consumer protection examination functions within the agency, OCFP responds to inquiries from credit unions, their members, and consumers involving consumer protection and share insurance matters. Additionally, the office processes member complaints filed against federal credit unions.

Asset Management

NCUA's Asset Management and Assistance Center (AMAC) conducts credit union liquidations and performs management and recovery of assets. AMAC assists agency regional offices with the review of large complex loan portfolios and actual or potential bond claims. AMAC also participates extensively in the operational phases of conservatorships and records reconstruction. AMAC's purpose is to minimize costs to the Share Insurance Fund and to credit union members.

Office of Minority and Women Inclusion

NCUA formed the Office of Minority and Women Inclusion in January 2011, in accordance with the Dodd-Frank Act. The office is responsible for all matters relating to measuring, monitoring, and establishing policies for diversity in the agency's management, employment, and business activities, and with respect to the agency's regulated entities, excluding the enforcement of statutes, regulations, and executive orders pertaining to civil rights.

Office of Continuity and Security Management

The Office of Continuity and Security Management evaluates and manages security and continuity programs across NCUA and its regional offices. The office is responsible for continuity of operations, emergency planning and response, critical infrastructure and resource protection, cyber threat and intelligence analysis, insider threats and counterintelligence, facility security, and personnel security.

The NCUA Office of Inspector General

The 1988 amendments to the Inspector General Act of 1978 (IG Act) established IGs in 33 designated federal entities (DFEs), including the NCUA.[12] The NCUA Inspector General (IG) is appointed by, reports to, and is under the general supervision of a three-member presidentially appointed Board. OIG staff consists of ten employees: the IG, the Deputy IG/Assistant IG for Audit, the Counsel to the IG/Assistant IG for Investigations, the Director of Investigations, five auditors, and an office manager. OIG promotes the economy, efficiency, and effectiveness of agency programs and operations, and detects and deters fraud, waste, and abuse, thereby supporting the NCUA's mission of facilitating the availability of credit union services to all eligible consumers through a regulatory environment that fosters a safe and sound credit union system. OIG supports this mission by conducting independent audits, investigations, and other activities, and by keeping the NCUA Board and the Congress fully and currently informed of its work.

Recent Work

We coordinated with our counterparts in CIGFO on issues of mutual interest, including on the *Top Management and Performance Challenges Facing Financial Regulatory Organizations* report that CIGFO issued in September 2018. This report noted that cybersecurity was the most frequently identified cross-cutting challenge among CIGFO members and included our observation that the NCUA must continue to strengthen the resiliency of the credit union system to cyber threats.

In that regard, we currently are conducting an audit of the NCUA's Information Systems and Technology Examination Program to determine whether the NCUA provides adequate oversight of the cybersecurity programs of federal credit unions with assets of $10 billion or more and all corporate credit unions. This audit follows our September 2017 audit focusing on the NCUA's oversight of cybersecurity programs of credit unions with assets between $250 and $10 billion. Both of these audits could be instructive for the broader financial sector.

12 5 U.S.C. app. § 8G.

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

The U.S. Securities and Exchange Commission (SEC or agency) Office of Inspector General (OIG) promotes the integrity, efficiency, and effectiveness of the critical programs and operations of the SEC and operates independently of the agency to help prevent and detect fraud, waste, and abuse in those programs and operations, through audits, evaluations, investigations, and other reviews.

Background

The SEC's mission is to protect investors; maintain fair, orderly, and efficient markets; and facilitate capital formation. The SEC strives to promote capital markets that inspire public confidence and provide a diverse array of financial opportunities to retail and institutional investors, entrepreneurs, public companies, and other market participants. Its core values consist of integrity, excellence, accountability, teamwork, fairness, and effectiveness. The SEC's goals are focusing on the long-term interests of Main Street investors; recognizing significant developments and trends in evolving capital markets and adjusting agency efforts to ensure the SEC is effectively allocating its resources; and elevating the SEC's performance by enhancing its analytical capabilities and human capital development.

The SEC is responsible for overseeing the nation's securities markets and certain primary participants, including broker-dealers, investment companies, investment advisers, clearing agencies, transfer agents, credit rating agencies, and securities exchanges, as well as organizations such as the Financial Industry Regulatory Authority, Municipal Securities Rulemaking Board, Public Company Accounting Oversight Board, Securities Investor Protection Corporation, and the Financial Accounting Standard Board. Under the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (Dodd-Frank Act), the agency's jurisdiction was expanded to include certain participants in the derivatives markets, private fund advisers, and municipal advisors.

The SEC's headquarters are in Washington, DC, and the agency has 11 regional offices located throughout the country. The agency's functional responsibilities are organized into 5 divisions and 25 offices, and the regional offices are primarily responsible for investigating and litigating potential violations of the securities laws. The regional offices also have examination staff to inspect regulated entities such as investment advisers, investment companies, and broker-dealers. In fiscal year 2018, the SEC employed 4,483 full-time equivalents.

The SEC OIG was established as an independent office within the SEC in 1989 under the Inspector General Act of 1978, as amended (IG Act). The SEC OIG's mission is to promote the integrity, efficiency, and effectiveness of the SEC's critical programs and operations. The SEC OIG prevents and detects fraud, waste, and abuse through audits, evaluations, investigations, and other reviews related to SEC programs and operations.

The SEC OIG Office of Audits conducts, coordinates, and supervises independent audits and evaluations of the SEC's programs and operations at its headquarters and 11 regional offices. These audits and evaluations are based on risk and materiality, known or perceived vulnerabilities and inefficiencies, and information received from the Congress, SEC staff, the U.S. Government Accountability Office, and the public.

The SEC OIG Office of Investigations performs investigations into allegations of criminal, civil, and administrative violations involving SEC programs and operations by SEC employees, contractors, and outside entities. These investigations may result in criminal prosecutions, fines, civil penalties, administrative sanctions, and personnel actions. The Office of Investigations also identifies vulnerabilities, deficiencies, and wrongdoing that could negatively impact the SEC's programs and operations.

In addition to the responsibilities set forth in the IG Act, Section 966 of the Dodd-Frank Act required the SEC OIG to establish a suggestion program for SEC employees. The SEC OIG established its SEC Employee Suggestion Program in September 2010. Under this program, the OIG receives, reviews and considers, and recommends appropriate action with respect to such suggestions or allegations from agency employees for improvements in the SEC's work efficiency, effectiveness, and productivity, and use of its resources, as well as allegations by employees of waste, abuse, misconduct, or mismanagement within the SEC.

SEC OIG Work Related to the Broader Financial Sector

In accordance with Section 989E(a)(2)(B)(i) of the Dodd-Frank Act, below is a discussion of the SEC OIG's completed and ongoing work, focusing on issues that may apply to the broader financial sector.

Completed Work

Evaluation of the EDGAR System's Governance and Incident Handling Processes, Report No. 550, September 21, 2018

On September 20, 2017, the Chairman of the SEC publicly disclosed that an incident—specifically, a software vulnerability in a component of the agency's Electronic Data Gathering, Analysis, and Retrieval (EDGAR) system—previously detected in 2016, resulted in unauthorized access to non-public information. On September 23, 2017, the Chairman, who began his service in May 2017 and was notified of the incident in August 2017, requested that the OIG review the agency's handling of, and response to, the 2016 incident. In response, the OIG initiated an evaluation. In July 2018, the OIG presented the Chairman and other SEC Commissioners with the non-public results of its evaluation relative to the 2016 EDGAR intrusion. Report No. 550 presents the OIG's findings related to the information security practices applicable to the EDGAR system between fiscal years (FYs) 2015 and 2017.

EDGAR is at the heart of the agency's mission of protecting investors; maintaining fair, orderly, and efficient markets; and facilitating capital formation. The availability of accurate, complete, and timely information from EDGAR is essential to the SEC's mission and the investing public. Without adequate controls to ensure the SEC identifies, handles, and responds to EDGAR system incidents in a timely manner, threat actors could gain unauthorized access to the system, which could lead to illicit trading, negative impacts to the economy and public access to filings, and loss of public confidence in the SEC.

We determined that, between FYs 2015 and 2017, the EDGAR system lacked adequate governance commensurate with the system's importance to the SEC's mission. In addition, we determined that certain preventive controls did not exist or did not operate as designed. Moreover, between September 2015 and September 2016, the SEC wasted at least $83,000 on a tool for which the SEC derived little, if any, benefit. Finally, we found that the SEC lacked an effective incident handling process. These weaknesses potentially increased the risk of EDGAR security incidents, and impeded the SEC's response efforts. The SEC has since strengthened EDGAR's system security posture, including the handling of and response to vulnerabilities. Among other actions, in August 2017, the agency established a Cyber Initiative Working Group to oversee and lead a number of priority cyber initiatives such as an EDGAR security uplift. As this and other work continues, opportunities for further improvement exist.

We issued our final report on September 21, 2018, and made 14 recommendations to improve the SEC's EDGAR system governance, security practices, and incident handling processes. We also noted that open recommendations from prior OIG work should address some of our observations, and we encouraged management to implement

agreed-to corrective actions. Management concurred with the recommendations, which will be closed upon completion and verification of corrective action.

Because the underlying report contains sensitive information about the SEC's information security program, we prepared this summary with information releasable to the public. An executive summary is also available on our website at *https://www.sec.gov/files/Eval-of-the-EDGAR-Systems-Governance-and-Incident-Handling-Processes.pdf*.

TCP Established Method to Effectively Oversee Entity Compliance With Regulation SCI but Could Improve Aspects of Program Management, Report No. 551, September 24, 2018

In recent years, several factors, including a significant number of systems issues at exchanges and other trading venues, increased concerns over "single points of failure" in U.S. securities markets. These concerns contributed to the SEC's decision to address technological vulnerabilities and improve agency oversight of the core technology of key U.S. securities markets entities. In November 2014, the SEC adopted Regulation Systems Compliance and Integrity (SCI), under which the agency monitors the security and capabilities of U.S. securities markets' technological infrastructure. The SEC's Office of Compliance Inspections and Examinations' (OCIE) Technology Controls Program (TCP) is responsible for ensuring entities comply with Regulation SCI and for evaluating whether entities have established, maintained, and enforced written policies and procedures reasonably designed to ensure the capacity, integrity, resiliency, availability, and security of their Regulation SCI systems. We initiated an evaluation to assess OCIE's TCP and determine whether the program provided effective oversight of entities' compliance with Regulation SCI.

TCP has an established method to effectively oversee entity compliance with Regulation SCI. The program assesses compliance through its CyberWatch program and through TCP examinations. However, we identified opportunities to improve aspects of TCP program management. Specifically, we found that TCP's examination manuals in effect at the outset of our evaluation were outdated, management had not identified or documented TCP risks and control activities in OCIE's internal risk and control matrix, and TCPs' development of the Technology Risk-Assurance, Compliance, and Examination Report (TRACER) system—the program's system of record—was not well-planned or documented.

- *Examination Manuals*. The TCP Examination Manual and draft TRACER Examination User Manual in effect at the outset of our evaluation were outdated and did not align with TCP examination practices. Management was in the process of revising the TCP Examination Manual and, on June 25, 2018, released an updated version.

- *Risks and Control Activities*. TCP management had not identified or documented the program's risks and corresponding control activities in OCIE's risk and control matrix. Although TCP examinations appear to have similar risks and controls as other OCIE examinations, documentation we reviewed did not clearly identify comparable documented control activities specific to TCP examination processes for all identified risks.

- *TRACER Development*. Between September 2015 and January 2018, TCP continued development of the SEC's TRACER system at a cost of nearly $780,000. As the system's business owner during that time, TCP oversaw frequent (sometimes weekly) system updates, but did not properly plan or document its development efforts. TRACER's purpose and functions evolved over time as TCP was considering continued development of the system or migration to an existing OCIE system known as the Tracking and Reporting Examinations National Documentation System (TRENDS). Certain planned system capabilities were not realized and it is unclear, based on a lack of documentation, how TCP assessed or managed system requirements. On May 4, 2018, TCP management decided to discontinue developing TRACER and transition its examination program to TRENDS, which is expected to yield operational and cost savings benefits.

We also identified two other matters of interest for management's consideration. First, a majority of TCP staff who responded to a survey we administered indicated that they either did not receive adequate training or only sometimes received adequate training. TCP management has completed a 3-year training plan. We encouraged management to continue to review TCP staff training to ensure staff members have the knowledge and skills

necessary to perform TCP examinations. Secondly, we identified a gap in the Office of Acquisitions' process for reviewing CORs' files. We suggest that Acquisitions consider establishing follow-up procedures to address this gap.

At the outset of our evaluation, TCP management identified ongoing improvement initiatives and began implementing changes. We issued our final report on September 24, 2018, and, to further improve TCP program management, we recommended that OCIE: (1) ensure TCP management updates the TCP Examination Manual in a timely manner following TCPs' transition to TRENDS; (2) identify and document the risks and controls related to TCP operations, and update OCIE's risk and control matrix accordingly; and (3) ensure TCP management properly plans and documents TCP's transition to TRENDS, and retains all relevant materials in a central location. Management concurred with the recommendations, which will be closed upon completion and verification of corrective action.

Because the underlying report contains non-public information, we prepared this summary with information releasable to the public. Also, a redacted public version is available on our website at *https://www.sec.gov/files/TCP-Established-Method-to-Effectively-Oversee-Entity-Compliance-with-Reg-SCI--But-Could-Improve.pdf*.

Although Highly Valued by End Users, DERA Could Improve Its Analytics Support by Formally Measuring Impact, Where Possible, Report No. 553, April 29, 2019

The SEC increasingly relies on data and analytics to guide its strategic and operational activities and to make more informed, effective decisions. Based on FY 2017 budget information, the SEC spends about $120 million annually on data management and about $20 million annually on analytics. Furthermore, the SEC's Strategic Plan for FY 2018 through FY 2022 and FY 2020 Annual Performance Plan emphasize the agency's goal of enhancing and expanding its use of analytics.

The SEC's Division of Economic and Risk Analysis (DERA) assists the agency in executing its mission by integrating sophisticated, data-driven analytics and economic analysis into the work of the SEC. Analytics provided by DERA's Office of Risk Assessment (ORA) and Office of Research and Data Services (ORDS) support exam planning and other agency oversight programs related to issuers, broker-dealers, investment advisers, exchanges, and other trading platforms. To assess DERA's controls over integration of data analytics into the core mission of the SEC, we initiated an evaluation.

We determined that, although end users highly valued DERA's analytics support and believed such analytics were indispensable for risk scoping, investor protection, detecting illegal conduct, allocating resources more efficiently, and helping the SEC achieve its mission, ORA and ORDS management generally did not formally measure the quantitative or qualitative impact of either office's analytics support. Management noted that it tracked end user requests for analytics support, considered repeat customers as evidence analytics are valued, and identified potential metrics for measuring impact (such as efficiency gains and end user satisfaction); however, management had not formalized such metrics.

DERA management and end users of DERA's analytics acknowledged that it might be difficult to devise meaningful impact measurement metrics for some analytics projects. For example, even though ORA analytics identified outliers that led to at least one Division of Enforcement investigation, not all analytics produce such directly measurable outcomes. Management was also apprehensive about burdening end users with requests for feedback regarding analytics' impact. However, by not measuring, where possible, the impact of ORA's and ORDS' analytics support, DERA risks limiting its ability to assess its organizational performance, increase awareness of its analytics capabilities (including through outreach efforts), and fully integrate analytics into the work of the SEC in accordance with the agency's strategic goals and objectives.

In addition, we reviewed available usage data for two analytics tools that incorporated ORA analytics and found that end users used and valued both tools. Although DERA did not regularly review the usage data for one tool and usage data for the other tool was incomplete, we determined that DERA's review of such data would not significantly help the Division meet agency goals and objectives.

We also assessed DERA's interactions with the SEC's other divisions and offices, including its coordination and outreach efforts, and determined that staff in other divisions and offices generally viewed interactions with DERA favorably; duplicative analytics work across the SEC was not apparent; and DERA proactively engaged in outreach. However, a majority of respondents to a question in a survey we administered (22 of 37, or almost 60 percent) expressed an interest in further DERA outreach. Respondents believed that promoting the nature and benefits (that is, impact) of DERA analytics and systems could be useful to the SEC's other divisions and offices.

Finally, we identified one other matter of interest related to data management. Although we did not assess the SEC's data management practices and are not making any recommendations regarding data management at this time, we noted that data management is the foundation of analytics. Therefore, it is important to verify completion of the SEC's plans to improve in this area. We will continue to monitor the agency's plans and progress related to data management.

We issued our final report on April 29, 2019, and to improve its ability to assess its organizational performance, increase awareness of its analytics capabilities, and fully integrate analytics into the work of the SEC in accordance with the agency's strategic goals and objectives, we recommend that DERA (1) work with end users of its analytics projects to develop metrics, where possible, for formally measuring analytics support impact; (2) modify existing internal tracking processes to include, where possible, analytics impact measurement; and (3) incorporate the results of analytics impact measurements in the Division's outreach efforts. Management concurred with the recommendations, which will be closed upon completion and verification of corrective action.

This report is available on our website at *https://www.sec.gov/files/Although-Highly-Valued-by-End-Users-DERA-Could-Improve-Report-No-553_0.pdf*.

Final Management Letter: Update on the SEC's Progress Toward Redesigning the EDGAR System

In September 2017, we reported observations about controls over the SEC's EDGAR system enhancements and redesign efforts.[13] We noted that the SEC's EDGAR Redesign (ERD) program is a multi-year, cross-agency initiative and, since 2014, the SEC had taken steps to develop and implement a new electronic disclosure system that meets agency needs, including spending about $10.6 million on related contracts. Since issuing our September 2017 report, we have continued to monitor the SEC's progress toward redesigning the EDGAR system. We did not conduct an audit or evaluation in conformance with generally accepted government auditing standards or the Council of the Inspectors General on Integrity and Efficiency's Quality Standards for Inspection and Evaluation. However, based on the work performed, on May 23, 2019, we reported concerns that warrant management's attention. Specifically, we determined that:

- The agency's approach to redesigning the EDGAR system is unclear;
- ERD program cost and schedule estimates presented to agency decision makers and senior officials were not based on best practices; and
- The EDGAR Business Office (EBO) created a Grand Functional Requirements Document (Grand FRD) for the redesigned EDGAR system, but did not include sufficient detail about the system's security requirements.

On May 7, 2019, we provided SEC management with a draft of our management letter for review and comment. In its May 17, 2019, response, management concurred with our overall observations and stated that it remains committed to modernizing and improving the security, functionality, and maintainability of the EDGAR system. Although management did not use cost and schedule estimates based on best practices for its deliberations about the appropriate high-level strategy for the EDGAR system, management anticipates preparing more detailed estimates, based on best practices, later in the process. Also, although the Grand FRD did not describe in detail security

13 U.S. Securities and Exchange Commission, Office of Inspector General, *Audit of the SEC's Progress in Enhancing and Redesigning the Electronic Data Gathering, Analysis, and Retrieval System*, Report No. 544; September 28, 2017.

requirements for redesigning EDGAR, management anticipates it will obtain detailed security requirements in a future phase of the project. Finally, management expects that completed and ongoing work will modernize much of the EDGAR system, achieve many of the goals of the original EDGAR redesign project, and position the system for further modernization.

To help us determine whether further action by the OIG is warranted, we requested that, no later than June 6, 2019, management provide to the OIG the SEC's approach to redesigning the EDGAR system and its planned or ongoing actions to (a) manage the ERD program using reliable cost and schedule estimates based on established methods and valid data; (b) integrate "functional requirements" with "non-functional requirements," including those for security, recoverability, testability, and maintainability, with sufficient detail that future offerors can propose viable solutions and designs as part of a future competitive procurement; and (c) further manage the existing EDGAR system.

The final management letter contains non-public information about the agency's efforts to redesign the EDGAR system. We redacted the non-public information to create this public summary. Our public version of the letter is also available on our website at *https://www.sec.gov/files/Final-Mgmt-Ltr-Update-on-the-SECs-Progress-Toward-Redesigning-EDGAR.pdf*.

Ongoing Work

Evaluation of the Division of Trading and Markets' Office of Broker-Dealer Finances

The SEC prescribes broker-dealer net capital and risk assessment reporting requirements through various rules, overseen by the Division of Trading and Markets' Office of Broker-Dealer Finances (OBDF). On June 10, 2019, we initiated an evaluation of OBDF's efficiency and effectiveness. Specifically, we will determine whether OBDF (1) ensures efficient use of government resources to help achieve organizational goals and objectives, and (2) provides effective oversight of broker-dealer compliance with capital and risk reporting requirements, in accordance with applicable rules and guidance. We expect to issue a report summarizing our findings during 2020.

Evaluation of the SEC's Delinquent Filer Program

In 2004, the SEC initiated the delinquent filer program, administered jointly by the Division of Enforcement and the Division of Corporation Finance, to bring administrative proceedings under Exchange Act Section 12(j) to revoke the Exchange Act registrations of securities of issuers that are more than 1-year delinquent in their Exchange Act reports and have been unresponsive to SEC requests for compliance.[14] At the same time, the Division of Enforcement seeks Commission approval for trading suspensions under Section 12(k) to suspend trading of the securities of the non-filing issuers under certain circumstances. On June 10, 2019, we initiated an evaluation of the SEC's delinquent filer program to assess the SEC's process for identifying, tracking, and notifying delinquent filers and issuing related revocation orders and/or trading suspensions in accordance with applicable laws, rules, and regulations. As part of the evaluation, we will also review the Division of Enforcement's efforts to decentralize the delinquent filer process. We expect to issue a report summarizing our findings during 2020.

14 According to a 2004 advice memo, an enhanced delinquent filings program for issuers was needed because publicly traded companies that are delinquent in filing Exchange Act reports deprive investors of accurate financial information upon which to make informed investment decisions. Further, these entities are often vehicles for fraudulent stock manipulation schemes.

Special Inspector General for the Troubled Asset Relief Program

The Special Inspector General for the Troubled Asset Relief Program (SIGTARP) has the duty, among other things, to conduct, supervise, and coordinate audits and investigations of the purchase, management, and sale of assets under the Troubled Asset Relief Program (TARP) or as deemed appropriate by the Special Inspector General.

Background

SIGTARP is primarily a Federal law enforcement agency protecting the interests of the American people by investigating crime at financial institutions that received TARP funds or at other TARP recipients in housing programs. All TARP programs are intended to promote financial stability.

When first created, SIGTARP found that financial institution fraud had evolved from the insider self-dealing fraud that marked the savings and loan crisis, to escape detection from traditional fraud identification methods of self-reporting and regulator referrals. SIGTARP created an intelligence-driven approach and leveraged technological solutions to discover insider crimes at banks that previously went undetected. Now, as a result of SIGTARP investigations, 105 bankers have been criminally charged and 74 have been sentenced to prison with more bankers awaiting trial and sentencing.

SIGTARP is applying its intelligence-driven approach to search for crime in TARP housing and foreclosure prevention programs. TARP recipients include large mortgage servicers in the Making Home Affordable (MHA) Program, like Wells Fargo, Bank of America, and JPMorgan Chase.

SIGTARP assesses that the top threat in TARP today is unlawful conduct by any of the 152 banks and other financial institutions that received $20.1 billion or will continue to receive $3.7 billion for foreclosure prevention in TARP's MHA Program. With an uptick in enforcement actions against financial institutions in MHA, SIGTARP has shifted resources to counter this threat.

The Most Serious Management and Performance Challenges & Threats of Fraud, Waste, & Abuse Facing the Government in TARP

SIGTARP identifies the most serious management and performance challenges and threats facing the Government in TARP. Our selection is based on the significance and duration of the challenge/threat to the mission of TARP and to Government interests; the risk of fraud or other crimes, waste or abuse; the impact on agencies in addition to Treasury; and Treasury's progress in mitigating the challenge/threat.

Risk of Fraud, Waste, and Abuse by Large Banks and Others in the Making Home Affordable Program (Until Sep. 2023)

Unlawful conduct by any of the 152 banks or institutions that received $20.1 billion or will continue to receive $3.7 billion in TARP's MHA program is the top threat in TARP. Treasury will pay up to $3.1 billion to Ocwen, Wells Fargo, JPMorgan Chase, Bank of America, Nationstar, Select Portfolio Servicing, CitiMortgage, OneWest/CIT, Bayview Loan Servicing, and Specialized Loan Servicing along with 131 institutions. These TARP payments require compliance with the law and Treasury's rules for the institutions assisting the 834,206 consumers in all 50 states. Wells Fargo recently disclosed in two SEC filings its wrongful denial of homeowners for admission to the program. Despite enforcement actions and other wrongdoing by many of these financial institutions, Treasury has significantly scaled back its compliance reviews. The risk of fraud, waste, and abuse also jeopardizes the GSEs, FHA, and Veterans Affairs that participate in MHA.

Risk of Waste and Misuse of TARP Dollars by State Agencies for Their Own Administrative Expenses in the Hardest Hit Fund (Until Dec. 2021)

Treasury has budgeted $1.1 billion in TARP dollars for administrative expenses of 19 state agencies to distribute HHF assistance. In March 2019, SIGTARP issued an audit that found state agencies violated federal cost regulations by charging more than $400,000 in prohibited travel and conference costs to the Hardest Hit Fund. SIGTARP found waste, a lack of internal controls at state agencies, and lack of effective oversight by Treasury. State agencies did not have the documentation required by Federal regulations to charge the travel and conferences to HHF. The audit also identified outright waste, including TARP funds spent on luxury hotels, conferences and extravagant dinners and receptions. In 2016 and 2017, SIGTARP identified $11 million in wasteful and unnecessary spending by state housing agencies, including, for example, catered barbeques, parties, country club events, leasing a Mercedes, cash bonuses, gym memberships, gifts, free parking, settlements and legal fees in discrimination cases, other costs not associated with HHF, and more. In 2018, SIGTARP issued an audit that found that while Treasury anticipates millions of dollars in spending on lawyers, accountants, auditors, consultants, information technology, communications, risk management, training, and marketing, there is no Federal requirements for competition.

Risk of Corruption, Anticompetitive Actions, and Fraud in the Hardest Hit Fund Blight Elimination Program (Until Dec. 2021)

There is a risk of corruption, anticompetitive acts, and fraud as TARP funds the demolitions of abandoned homes and apartments. The number of municipalities in the program increased to 378 cities or counties. There have already been criminal indictments for corruption in HHF.

Risk of Asbestos Exposure, Contaminated Soil, and Illegal Dumping in the Hardest Hit Fund Blight Elimination Program (Until Dec. 2021)

In November 2017, based on the U.S. Army Corps of Engineers' findings, SIGTARP warned that the standard protections in demolition are not present in the TARP program. The Army Corps found missing industry standard safeguards that protect against the risk of asbestos exposure, illegal dumping of debris, and contaminated material filling the hole. Treasury did not implement SIGTARP's recommendations, even to require basic documentation of proper asbestos abatement, certain inspections, landfill receipts for dumping, and receipts showing the purchase of clean dirt. SIGTARP's investigation into a demolition contractor for illegal dumping of contaminated soil in Fort Wayne, Indiana was resolved for over $800,000 through remediation and a settlement by DOJ under the False Claims Act.

TARP may expand even further in this area: The Economic Growth, Regulatory Relief, and Consumer Protection Act authorizes Treasury to use TARP dollars to remediate lead and asbestos hazards in residential properties.

No Complete List or Data Identifying All Contractors and Others Doing Work in the Hardest Hit Fund Blight Subprogram and What They Were Paid

Treasury and the state agencies do not know, and cannot provide to SIGTARP a complete list of contractors receiving TARP dollars in the program. SIGTARP and Treasury cannot conduct oversight over contractors and other entities that are unknown. Treasury rejected SIGTARP's 2015 recommendation to maintain a list and accounting of payments in HHF. SIGTARP's proactive analysis has identified 2,210 land banks or other partners, contractors, or subcontractors that have done or are contracted to do work in the program—but given the missing data, we believe the actual numbers may be much higher. State agency data is incomplete. The data provided by state agencies to SIGTARP also provides limited detail about the $510.5 million that has been spent in the Blight Elimination Program beyond the first-level recipient. As a result, there may be hundreds, or perhaps thousands, of additional unknown subcontractors doing work in the program. Without complete records and accounting, the program and taxpayers are vulnerable.

Risk of Waste from Weakened Oversight by Treasury of State Agencies in the Hardest Hit Fund

Starting in October 2018, Treasury has allowed state agencies to shift HHF dollars between programs and removed caps on administrative expenses (by the greater of five percent or $50,000). Treasury also decreased oversight in the HHF program in 2018 by reducing OFS personnel charged with providing oversight of the HHF program by 30%. These Treasury changes increase risk of fraud, waste and abuse because state agencies can move more TARP money to higher risk subprograms. These changes also have weakened Treasury oversight of state administrative spending after SIGTARP has proven waste and misuse of TARP dollars by state agencies. Additionally, GAO found in a December 2018 study that "Treasury is missing an opportunity to ensure that HFAs are appropriately assessing their risk."

SIGTARP's Investigations Approach

SIGTARP gained expertise in investigating large institutions which resulted in significant DOJ enforcement actions against Goldman Sachs, Bank of America, JPMorgan Chase, Morgan Stanley, Ally Financial, Wilmington Trust, Sun Trust Bank, Fifth Third Bank, Jefferies & Co., and RBS Securities.

SIGTARP's law enforcement counters threats to public safety and Government interests by investigating criminal actors and working with the Justice Department to prosecute those criminal actors. With 278 people sentenced to prison resulting from a SIGTARP investigation, at an average prison sentence of nearly five years, the threat these crimes pose is significant. SIGTARP's ongoing criminal investigations of recipients of TARP dollars in TARP housing programs promote free and fair trade by improving the overall condition for competition, and counter threats to public safety and Government interests, including financial institution fraud, public corruption, antitrust (unfair competition), contract fraud, and organized crime. Recent DOJ charges, pleas and false claim settlements continue to demonstrate that these threats are current and real.

Financial Institution Fraud: SIGTARP's highest priority is investigating banks and other financial institutions receiving TARP dollars in the Making Home Affordable Program. Our investigations into TARP banks have already resulted in 104 bankers criminally charged and 73 sentenced to prison. Many await trial. Our remaining investigative work in this area focuses on supporting the Justice Department in its efforts to prosecute TARP bankers. SIGTARP's work on financial institution fraud supports Justice Department prosecutions of individuals investigated by SIGTARP, such as international money laundering charges related to a TARP bank, that help identify and reduce vulnerabilities in the financial system while stopping abuses by illicit actors.

Public Corruption: The corruption of local officials threatens public safety and fair competition. State and local officials award contracts under the more than $760 million Hardest Hit Fund blight demolition program.

Antitrust Violations: Unfair competitive practices in TARP housing programs including contract steering, bid rigging and price fixing, threatens the quality of work, harms public safety, threatens fair competition, and results in higher costs.

Contract Fraud, False Claims/Theft or Bribery in TARP Programs: Demolition contractors and State agencies play key roles in administering HHF programs. Fraud in any of these risk areas harm Government interests and fair competition.

Organized Crime: Organized crime in the over $760 million blight demolition program or in TARP banks threatens public safety, fair competition and harms Government interests.

Selected SIGTARP's Investigations Results (April 1, 2018 to March 31, 2019)

Wilmington Trust Corporation

In December 2018 and January 2019, a federal court sentenced seven former Wilmington Trust bankers to prison terms of up to six years. As a result of a SIGTARP investigation, the bank's former president, chief financial officer, chief credit officer and controller were convicted of securities fraud after a trial. Wilmington Trust Bank received a $330 million TARP bailout. As the conspiracy was ongoing and while in TARP, the bank collapsed and was acquired by M&T Bank at a discount of approximately 46% from the bank's share price the prior trading day.

SIGTARP's investigation uncovered a scheme by bank insiders to conceal the total quantity of past due loans on its books from the Federal Reserve, the Securities and Exchange Commission and the investing public. After the trial, a jury convicted former president Robert Harra, former chief financial officer David Gibson, former chief credit officer William North, and former controller Kevyn Rakowski of hiding more than $300 million in loans that were 90 days past due.

At their sentencing, U.S. District Judge Richard G. Andrews said the investigation uncovered the "the biggest financial crime in Delaware, at least in the past 35 years." The court sentenced former president Harra and former chief financial officer Gibson to six years in prison and ordered them to pay $300,000 each. The court sentenced former chief credit officer North to four and half years in prison and ordered him to pay $100,000 and former controller Rakowski to three years in prison. The court separately sentenced three other Wilmington Trust officers: former head of commercial real estate Delaware Brian Baily to two and half years, former vice president for commercial real estate for Delaware Joseph Terranova to one year and nine months and former commercial real estate relationship manager for Delaware Peter Hayes to one year and three months.

In October 2017, as part of a criminal investigation Wilmington Trust admitted wrongdoing and agreed to pay $60 million. Wilmington Trust was the only TARP bank indicted by the Justice Department.

SIGTARP was joined in the investigation by the Federal Bureau of Investigation, the Internal Revenue Service-Criminal Investigation, and the Federal Reserve Bank-Office of Inspector General. The U.S. Attorney's Office for the District of Delaware prosecuted the case.

Sonoma Valley Bank of California

In August 2018, a federal court sentenced both the Sonoma Valley Bank CEO Sean Cutting and Chief Loan Officer Brian Melland to eight years and four months in prison, and the attorney of a bank borrower to six years and eight months in prison. SIGTARP's investigation uncovered that leading up to and during the time Sonoma Valley Bank was in TARP, the bank officers conspired to commit fraud that would contribute to the failure of the bank and a complete loss to TARP of $8.6 million. They made millions in illegal bank loans to "straw" borrowers, knowing the proceeds would go to one bank borrower who was a real estate developer. They then tried to cover up the scheme by falsifying the bank's books and lying to the bank's regulators.

During the fraud, the bank applied for TARP, with the CEO describing TARP as a "cookie jar" and saying it only made sense for the bank to take some. After a Federal jury trial in December 18, 2017, the jury found Cutting and Melland guilty of conspiracy, bank fraud, wire fraud, attempted obstruction of justice, and other offenses. The real estate developer was indicted but died prior to the trial when his car drove over a cliff on Highway 1. The court ordered $19 million in restitution and forfeiture of a condominium complex involved in the fraud.

SIGTARP was joined in the investigation by the Federal Housing Finance Agency Office of Inspector General, the Federal Deposit Insurance Corporation Office of Inspector General, the Marin County Sheriff's Office, the Sonoma County Sheriff's Office, and the Santa Rosa Police Department. The U.S. Attorney's Office for the Northern District of California prosecuted the case.

Southern Bancorp

As a result of a SIGTARP investigation, in February 2019, a federal court sentenced bank officer Michael J. Erickson to two years in prison after he was convicted of embezzling funds from Southern Bancorp. The court ordered Erickson to pay $1.4 million to Southern Bancorp. Taxpayers lost $2.3 million on the investment; the bank received a $33.8 million bailout from TARP.

In its investigation, SIGTARP uncovered a scheme where Erickson stole thousands of dollars for his own personal enrichment from a commercial loan he managed. SIGTARP was joined in the investigation by the Federal Bureau of Investigation. The U.S. Attorney's Office for the Northern District of Mississippi prosecuted the case.

Saigon National Bank

In February 2019, a federal court sentenced Vivian Tat to two years in federal prison for laundering tens of thousands of dollars in cash. This case is the result of Operation "Phantom Bank," targeting TARP recipient Saigon National Bank, which resulted in six indictments that charge a total of 25 defendants. SIGTARP was joined in the investigation by the FBI and the IRS Criminal Investigation. The U.S. Attorney's Office for the Central District of California prosecuted the case.

First Legacy Community Credit Union of North Carolina

In March 2019, President and CEO of First Legacy Community Credit Union (FLCCU) Saundra Torrence was sentenced to six months in prison and ordered to pay $187,066 in restitution for making or causing false entries. SIGTARP's investigation uncovered that Scales falsified the credit union's books, misapplied and stole funds from the credit union, and fraudulently used the identity of at least one third party victim to obtain a loan from FLCCU. Torrence's wrongdoing caused significant losses to the credit union. The fraudulent entries she made to conceal her wrongdoing caused the credit union's reported financial results to be inaccurate.

SIGTARP was joined in the investigation by the FBI. The U.S. Attorney's Office for the Western District of North Carolina prosecuted the case.

First State Bank

In October 2018, former First State Bank CEO Joseph Natale, financier Albert Gasparro, and business owner Gary Ketchum were indicted for their roles in a scheme to defraud the now defunct First State Bank, which attempted to obtain TARP funds.

The defendants are charged with conspiracy to mislead the FDIC and First State Bank, conspiracy to commit bank fraud and bank fraud. Former First State Bank legal counsel Donna Conroy, a conspirator, pleaded guilty in May 2017 and is awaiting sentencing. SIGTARP was joined in the investigation by the FBI and the FDIC Office of Inspector General. The U.S. Attorney's Office for New Jersey is prosecuting the case.

Lone Star Bank

Following a SIGTARP investigation, in September 2018, a Federal court sentenced Lone Star Bank loan officer Ricky Hajdik to 20 months in prison and sentenced co-conspirator Hugo Lafuente to 25 months in prison for a conspiracy to defraud the bank out of $1.3 million in loans. Hajdik knew that Lafuente's income would not qualify for a construction loan. Hajdik conveyed to loan broker Leonard Tyson an inflated and untrue income number that LaFuente needed to qualify for the construction loan. Lafuente then directed Mark Zylker to prepare fraudulent income tax returns that inflated his income, which Hajdik used for the bank to make the loan. When Lafuente defaulted on this loan and a Small Business Administration Loan, the bank suffered losses $735,758. TARP suffered a $1.2 million loss on the bank and the bank missed dividend payments of $2.2 million.

SIGTARP was joined in the investigation by the Federal Deposit Insurance Corporation Office of Inspector General. The U.S. Attorney's Office for the Southern District of Texas prosecuted the case.

SIGTARP's Audit Approach

SIGTARP conducts audits over TARP housing programs, helping promote financial stewardship by the Government. Much of SIGTARP's audit work is at the request of members of Congress. SIGTARP specializes in forensic audits that follow the money, analyzing general ledgers, credit card statements, invoices, and receipts.

SIGTARP assists Treasury in these efforts by auditing and evaluating housing programs to determine whether the Government is receiving fair value for its money and that recipients are spending TARP funds appropriately to accomplish the stated goals. To promote financial stewardship, SIGTARP reports on fraud, waste, and abuse and makes recommendations to Treasury (which has oversight of all TARP programs) to recover wasteful spending and prevent future fraud, waste, and abuse.

Travel and Conference Charges to the Hardest Hit Fund that Violated Federal Regulations

In a March 2019 audit, SIGTARP uncovered that state agencies violated federal cost regulations by charging HHF $411,658 in prohibited travel and conference costs. Remarking on the findings, Special Inspector General Goldsmith Romero said, "Flying around the country, staying at luxury hotels, attending conferences beachside and at other vacation destinations are not 'must have' costs for a local foreclosure prevention program."

SIGTARP's Recoveries from Audits and Investigations

SIGTARP continues to assess current and future operations to fulfill its mission and reduce spending, while supporting financial stewardship by providing recoveries to assist in funding the Government at the least cost over time. SIGTARP's investigations and audits have recovered $10 billion. Fiscal Year 2018 recoveries of more than $314 million, including more than $294 million recovered for the government, are a 9 times return on investment from the Fiscal Year 2018 appropriated budget. Already in Fiscal Year 2019, SIGTARP has recovered $804 million, including more than $336 million paid to the government, a 35 times annual return on investment from the Fiscal Year 2019 appropriated budget.

Office of Inspector General Department of the Treasury

The Department of the Treasury Office of Inspector General performs independent, objective reviews of specific Treasury programs and operations with oversight responsibility for one federal banking agency – the Office of the Comptroller of the Currency. That federal banking agency supervises approximately 1,260 financial institutions.

Introduction

The Department of the Treasury (Treasury) Office of Inspector General (OIG) was established pursuant to the 1988 amendments to the Inspector General Act of 1978. The Treasury Inspector General is appointed by the President, with the advice and consent of the Senate. Treasury OIG performs independent, objective reviews of Treasury programs and operations, except for those of the Internal Revenue Service (IRS) and the Troubled Asset Relief Program (TARP), and keeps the Secretary of the Treasury and Congress fully informed. Treasury OIG is comprised of four divisions: (1) Office of Audit, (2) Office of Investigations, (3) Office of Counsel, and (4) Office of Management. Treasury OIG is headquartered in Washington, DC, and has an audit office in Boston, Massachusetts, and investigative offices in Greensboro, North Carolina; Houston, Texas; and Jacksonville, Florida.

Treasury OIG has oversight responsibility for the Office of the Comptroller of the Currency (OCC). OCC is responsible for approximately 891 national banks, 316 federal savings associations, and 57 federal branches of foreign banks. The total assets under supervision are $12.5 trillion. Treasury OIG also oversees four offices created by the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank) which are (1) the Office of Financial Research (OFR), (2) the Federal Insurance Office, (3) the Office of Minority and Women Inclusion within Treasury's Departmental Offices (DO), and (4) the Office of Minority and Women Inclusion within OCC. Additionally, Treasury OIG oversees Treasury's role related to the financial solvency of the Federal National Mortgage Association (Fannie Mae) and the Federal Home Loan Mortgage Corporation (Freddie Mac) under the Housing and Economic Recovery Act of 2008 (HERA), to include Treasury's Senior Preferred Stock Purchase Agreements established for the purpose of maintaining the positive net worth of both entities.

Treasury Management and Performance Challenges Related to Financial Regulation and Economic Recovery

In accordance with the Reports Consolidation Act of 2000, the Treasury Inspector General annually provides the Secretary of the Treasury with his perspective on the most serious management and performance challenges facing the Department. In a memorandum to the Secretary dated October 15, 2018, the Inspector General reported three management and performance challenges that were directed towards financial regulation and economic recovery.

Those challenges are: Operating in an Uncertain Environment, Cyber Threats, and Anti-Money Laundering and Terrorist Financing/Bank Secrecy Act Enforcement.[15]

Operating in an Uncertain Environment

The proposed budget cuts and new requirements imposed by Executive Order (EO) 13781, *Comprehensive Plan for Reorganizing the Executive Branch* (March 13, 2017) create an uncertain environment that affect Treasury's operations. In its implementation of EO 13781 the Office of Management and Budget (OMB) required agencies to submit Agency Reform Plans to OMB, which included long-term workforce plans that are in alignment with their strategic plans. These plans were to include proposals in four categories: eliminate activities; restructure or merge; improve organizational efficiency and effectiveness; and workforce management. In June 2018, after consideration of all Agency Reform Plans, OMB developed it comprehensive "Government-wide Reform Plan and Reorganization Recommendations" (Government-wide Reform Plan) to reorganize the Executive Branch.

The Government-wide Reform Plan includes a recommendation to transfer alcohol and tobacco responsibilities from the Bureau of Alcohol, Tobacco, Firearms and Explosives within the Department of Justice to Treasury's Alcohol and Tobacco Tax and Trade Bureau (TTB) in order to leverage the expertise of TTB. Other potential impacts on Treasury include OMB recommendations to increase coordination and avoid duplication of agency's roles in the areas of small business programs, the housing finance market, and financial literacy and education. Until OMB and agencies begin discussions with Congress to prioritize and refine the proposals in the Government-wide Reform Plan, there is looming uncertainty as to the plan's impact. Nonetheless, the Department must plan for the potential long-term restricting of certain functions or offices/bureaus and expected budget cuts.

Cyber Threats

Cybersecurity continues to be a long-standing and serious challenge facing the Nation today. A reliable critical infrastructure, including information systems and networks, is vital to our national security and economic stability. Cyber threats are a persistent concern as Treasury's information systems are critical to the core functions of government and the Nation's financial infrastructure. As cyber threats continue to evolve and become more sophisticated and subtle, they pose an ongoing challenge for Treasury to fortify and safeguard its internal systems and operations and the financial sector it oversees.

Attempted cyber attacks against Federal agencies, including Treasury, and financial institutions are increasing in frequency and severity, in addition to continuously evolving. Such attacks include distributed denial of service attacks, phishing or whaling attacks, fraudulent wire payments, malicious spam (malspam), and ransomware. Organized hacking groups leverage published and unpublished vulnerabilities and vary their methods to make attacks hard to detect and even harder to prevent. Criminal groups and nation-states are constantly seeking to steal information; commit fraud; and disrupt, degrade, or deny access to information systems.

Effective public-private coordination continues to be required to address the cyber threat against the Nation's critical infrastructure. In this regard, Treasury is looked upon to provide effective leadership to financial institutions in particular, and the financial sector in general, to strengthen awareness and preparedness against cyber threats.

Anti-Money Laundering and Terrorist Financing/Bank Secrecy Act Enforcement

Identifying, disrupting, and dismantling the financial networks that support terrorists, organized transnational crime, weapons of mass destruction proliferators, and other threats to international security continue to be a challenge. Treasury's Office of Terrorism and Financial Intelligence (TFI) is dedicated to countering the ability of terrorist organizations to support such activities through intelligence analysis, sanctions, and international private-sector cooperation that identify donors, financiers, and facilitators funding terrorist organizations.

15 The Treasury Inspector General's memorandum included one other challenge not directly related to financial regulation and economic recovery: Efforts to Promote Spending Transparency and to Prevent and Detect Improper Payments. The memorandum also discussed concerns about two matters: currency and coin production and excise tax reform.

Disrupting terrorist financing depends on a whole-of-government approach and requires collaboration and coordination within Treasury and with other Federal agencies. Effective coordination and collaboration and TFI's ability to effectively gather and analyze intelligence information on financial crimes and terrorism requires a stable cadre of staff. TFI filled long standing vacancies such as the Assistant Secretary of Intelligence and Analysis, which is a key leadership position that had been vacant for approximately 2 years. Stability, experienced leadership, and coordination within TFI is imperative to enhance information gathering and intelligence analysis and increase efficiency.

Completed and In-Progress Work on Financial Oversight

OFR's Procurement Activities – Contracts

We initiated an audit of OFR's procurement activities. We reported that OFR effectively and efficiently acquired goods and services to accomplish its mission and those acquisitions were made in compliance with applicable procurement regulations. We did not make any recommendations as a result of our audit; however, in light of OFR's recent workforce restructuring efforts, we encouraged the Acting Director to ensure the files of OFR's contracting officer representatives are maintained and accessible in the event of any changes in contracting officer representatives' responsibilities.

OCC's Supervision of Federal Branches of Foreign Banks (In Progress)

We initiated an audit of OCC's supervision of federal branches of foreign banks. The objective of this audit is to assess OCC's supervision of federal branches and agencies of foreign banking organizations operating in the United States.

OCC's Supervision of Wells Fargo Bank (In Progress)

We initiated an audit of OCC's supervision of Wells Fargo Bank's sales practices. The objectives of this audit are to assess (1) OCC's supervision of incentive-based compensation structures within Wells Fargo and (2) the timeliness and adequacy of OCC's supervisory and other actions taken related to Wells Fargo sales practices, including the opening of accounts.

OCC's Supervision Related to De-risking by Banks (In Progress)

We initiated an audit of OCC's supervisory impact on the practice of de-risking[16] by banks. The objectives of this audit are to determine (1) whether supervisory, examination, or other staff of the OCC have indirectly or directly caused banks to exit a line of business or to terminate a customer or correspondent account, and (2) under what authority OCC plans to limit, through guidance, the ability of banks to open or close correspondent or customer accounts, including a review of laws that govern account closings and OCC's authority to regulate account closings.

OFR's Hiring Practices (In Progress)

We initiated an audit of OFR's hiring practices. The objective for this audit is to determine whether OFR's hiring practices are in accordance with Office of Personnel Management, Treasury, OFR, and other Federal requirements.

OCC's Controls over Purchase Cards (In Progress)

We initiated an audit of OCC's controls over purchase cards. The objective for this audit is to assess the controls in place over OCC's purchase card use and identify any potential illegal, improper, or erroneous transactions.

16 The Financial Action Task Force defines de-risking as the termination or restriction, by financial institutions, of business relationships with categories of customers.

OCC Human Capital Policies and Planning (In Progress)

We initiated an audit of OCC's human capital policies and resource planning. The objective for this audit is to determine whether OCC's human capital policies and planning align with its mission and strategic goals.

Failed Bank Reviews

In 1991, Congress enacted the Federal Deposit Insurance Corporation Improvement Act (FDICIA) amending the Federal Deposit Insurance Act (FDIA). The amendments require that banking regulators take specified supervisory actions when they identify unsafe or unsound practices or conditions. Also added was a requirement that the Inspector General for the primary federal regulator of a failed financial institution conduct a material loss review when the estimated loss to the Deposit Insurance Fund is "material." FDIA, as amended by Dodd-Frank, defines the loss threshold amount to the Deposit Insurance Fund triggering a material loss review as a loss that exceeds $50 million for 2014 and thereafter (with a provision to temporarily raise the threshold to $75 million in certain circumstances). The act also requires a review of all bank failures with losses under these threshold amounts for the purposes of (1) ascertaining the grounds for appointing Federal Deposit Insurance Corporation (FDIC) as receiver and (2) determining whether any unusual circumstances exist that might warrant a more in-depth review of the loss. As part of the material loss review, OIG auditors determine the causes of the failure and assess the supervision of the institution, including the implementation of the prompt corrective action provisions of the act.[17] As appropriate, OIG auditors also make recommendations for preventing any such loss in the future.

From 2007 through March 2019, FDIC and other banking regulators closed 538 banks and federal savings associations. One hundred and forty-two (142) of these were Treasury-regulated financial institutions; in total, the estimated loss to FDIC's Deposit Insurance Fund for these failures was $36.4 billion. Of the 142 failures, 58 resulted in a material loss to the Deposit Insurance Fund, and our office performed the required reviews of these failures.

During the period covered by this annual report, we completed a material loss review of Washington Federal Bank for Savings (Washington Federal) located in Chicago, Illinois, whose failure in December 2017 resulted in a loss to the Deposit Insurance Fund estimated at $82.6 million. We determined that Washington Federal failed because of fraud[18] in the bank's loan activity perpetrated by bank employees. The fraudulent activity depleted the bank's capital, with the result that the bank was insolvent and in an extremely unsafe or unsound condition to transact business. Regarding supervision, we found that OCC generally performed examinations of Washington Federal in accordance with laws, regulations and guidance; however, we identified weaknesses in the execution of OCC's supervision of the bank that led to missed opportunities for timely enforcement actions related to the bank's loan portfolio. Specifically, we identified the following supervisory weaknesses: (1) the Supervisory Office and Examiners-in-Charge (EIC) did not provide sufficient supervision of examination staff comprised mainly of first-time Assistant Examiners-in-Charge (AEIC) and examiners with limited experience; (2) examiner conclusions were contradicted by documentation in the OCC work papers; (3) examiners did not act promptly to address significant weaknesses in the loan portfolio reporting capability of the bank's management information system; (4) examiners missed red flags related to Washington Federal's loan portfolio and resultantly did not timely expand the core assessment minimum procedures; (5) examiners did not identify and did not report unsafe or unsound practices that were contrary to agency guidance and bank policy related to the appraisal program; and (6) examiners did not identify a lack of independence in the bank's lending or loan review function.

We recommended the Comptroller of the Currency: (1) assess the need for additional guidance related to the supervision of non-commissioned examiners by the EIC and the Supervisory Office including the need to require

17 Prompt corrective action is a framework of supervisory actions for insured institutions that are not adequately capitalized. It was intended to ensure that action is taken when an institution becomes financially troubled in order to prevent a failure or minimize the resulting losses. These actions become increasingly severe as the institution falls into lower capital categories. The capital categories are well-capitalized, adequately capitalized, undercapitalized, significantly undercapitalized, and critically undercapitalized.

18 The use of this term "fraud" comes from OCC's finding in its Supervisory Memorandum. As of the date of the issuance of this material loss review report (November 7, 2018), no criminal or civil judicial finding of fraud has been made and applied to the bank's activities.

that supervision be documented; (2) revise examination guidance to clarify the roles and responsibilities of an EIC in supervising an examination team, with an emphasis on reviewing work papers and confirming that conclusions in work papers are supported by the documentation; (3) reinforce to examiners and provide training where necessary to ensure they understand: (a) the requirements of OCC Bulletin 2000-20 and the importance of the bank maintaining sufficient loan portfolio reporting for extensions, deferrals, renewals, and rewrites of closed-end loans; (b) that bank assurances made to examiners regarding deficiencies being resolved should be viewed with skepticism unless support for the assurances is provided and the examiner validates the effectiveness of the bank's corrective actions, especially when the deficiencies result in noncompliance with regulation or law; (c) that expanded procedures are recommended when an examination team is comprised of examiners in training positions and those with limited experience, including AEICs; (d) that expanded procedures are recommended for banks, or examination areas, that are consistently considered low risk; (e) the need to identify and report appraisal exceptions as required by the *Interagency Appraisal and Evaluation Guidelines*; and (f) the need to identify and address issues of independence in small banks where employees or board members are participating in more than one function or committee.

SEPTEMBER 2018

Top Management and Performance Challenges Facing Financial Regulatory Organizations

Approved September 13, 2018

EXECUTIVE SUMMARY

Purpose

The purpose of this report is to consolidate and provide insight into cross-cutting management and performance challenges facing financial-sector regulatory organizations as identified by members of CIGFO.

Approach

Following a review of 10 TMPC reports issued by CIGFO members, we integrated the primary areas of concern facing financial regulatory organizations. We sought to identify common insights within the financial sector.

CIGFO Members

- Department of the Treasury (Chair)
- Federal Deposit Insurance Corporation
- Federal Housing Finance Agency
- Commodity Futures Trading Commission
- Department of Housing and Urban Development
- Board of Governors of the Federal Reserve System and the Bureau of Consumer Financial Protection
- National Credit Union Administration
- Securities and Exchange Commission
- Special Inspector General for the Troubled Asset Relief Program

The Dodd-Frank Wall Street Reform and Consumer Protection Act established the Council of Inspectors General on Financial Oversight (CIGFO) to oversee the Financial Stability Oversight Council (FSOC) and suggest measures to improve financial oversight. FSOC has a statutory mandate that established collective accountability for identifying risks and responding to emerging threats to U.S. financial stability.

The Inspectors General within CIGFO report annually on the Top Management and Performance Challenges (TMPC) affecting their respective organizations. This report reflects the collective input from the Inspectors General in CIGFO and identifies cross-cutting Challenges facing multiple financial-sector regulatory organizations:

- Enhancing Oversight of Financial Institution Cybersecurity
- Managing and Securing Information Technology at Regulatory Organizations
- Sharing Threat Information
- Readiness for Crises
- Strengthening Agency Governance
- Managing Human Capital

These Challenges highlight the importance of Government-wide coordination and information sharing for a particular sector – such as the financial sector – in a whole-of-government approach, as distinct from considering the issues on an agency-by-agency basis. It is important to address these Challenges in a coordinated and cohesive fashion, because the financial sector is one of 16 critical infrastructure sectors that are vital to public confidence and the nation's safety, prosperity, and well-being (as designated by Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience*). Moreover, the financial sector has changed considerably since the last financial crisis. It is more diverse, technology dependent, and interconnected. Further, the speed of technological advances in the financial sector and increased targeting of the financial system by malicious actors highlight the need for financial regulators to address the Challenges identified in this report.

CIGFO initiated this project to provide useful information to the leaders of financial-sector regulatory organizations as they look to develop strategies to improve efficiency, economy, effectiveness, and accountability at their agencies, consistent with Executive Order 13781, *Comprehensive Plan for Reorganizing the Executive Branch*. By consolidating and reporting these Challenges, CIGFO aims to inform regulatory organizations, FSOC, the Congress, and the American public as to the assessments by CIGFO members.

TABLE OF CONTENTS

BACKGROUND AND OBSERVATIONS

The Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act), established CIGFO to oversee FSOC and suggest measures to improve financial oversight. FSOC has a statutory mandate that established collective accountability for identifying risks and responding to emerging threats to U.S. financial stability.

CIGFO meets regularly to facilitate the sharing of information among Inspectors General, with a focus on concerns that affect the financial sector and ways to improve financial oversight. CIGFO publishes an annual report that describes the concerns and recommendations of each Inspector General and a discussion of ongoing and completed work. Additionally, CIGFO is authorized to convene a working group to evaluate FSOC's effectiveness and internal operations.

CIGFO members include the Inspectors General of the Department of the Treasury, the Federal Deposit Insurance Corporation, the Commodity Futures Trading Commission, the Department of Housing and Urban Development, the Board of Governors of the Federal Reserve System and the Bureau of Consumer Financial Protection, the Federal Housing Finance Agency, the National Credit Union Administration, the Securities and Exchange Commission, and the Special Inspector General for the Troubled Asset Relief Program. CIGFO members oversee one or more financial-sector regulatory organizations as shown in Table 1.

Table 1 - CIGFO Membership & Oversight

CIGFO MEMBERSHIP	OVERSIGHT OF FINANCIAL- SECTOR REGULATORY ORGANIZATIONS
Department of the Treasury (Chair)	▪ Department of the Treasury ▪ Office of the Comptroller of the Currency
Federal Deposit Insurance Corporation	Federal Deposit Insurance Corporation
Commodity Futures Trading Commission	Commodity Futures Trading Commission
Department of Housing and Urban Development	Department of Housing and Urban Development
Board of Governors of the Federal Reserve System and Bureau of Consumer Financial Protection	▪ Board of Governors of the Federal Reserve System ▪ Bureau of Consumer Financial Protection
Federal Housing Finance Agency	Federal Housing Finance Agency
National Credit Union Administration	National Credit Union Administration
Securities and Exchange Commission	Securities and Exchange Commission
Special Inspector General for the Troubled Asset Relief Program	Department of the Treasury's Troubled Asset Relief Program

The Inspectors General within CIGFO, as well as the Inspectors General of other agencies, publish annually reports of what they consider to be the TMPCs facing their agency.

On June 14, 2018, CIGFO approved a motion to compile a report identifying the top Challenges facing financial-sector regulatory organizations. The Federal Deposit Insurance Corporation (FDIC) Office of Inspector General (OIG) led the working group to conduct this analysis and compile this report.

This CIGFO report reflects the collective input from the Inspectors General and identifies cross-cutting Challenges facing multiple financial-sector regulatory organizations:

- Enhancing Oversight of Financial Institution Cybersecurity
- Managing and Securing Information Technology at Regulatory Organizations
- Sharing Threat Information
- Readiness for Crises
- Strengthening Agency Governance
- Managing Human Capital

Cybersecurity was the most frequently identified cross-cutting Challenge among CIGFO members. The Challenge relating to cybersecurity encompassed risks to the security of information technology (IT) systems and information at financial institutions, those institutions' third-party service providers, and financial regulatory organizations. This report recognizes the significance of the interconnection among the information systems of financial sector private and public participants and the possibility of contagion where a security incident for one participant may affect the entire financial sector.

Another significant Challenge is effective sharing of threat information among government agencies and throughout the entire financial sector. Actionable threat information assists regulators, financial institutions, and third-party service providers in understanding threats and taking action to mitigate their impact. Financial-sector regulatory organizations also face Challenges in the current environment of limited government spending to stand ready to address crises in the financial sector.

In addition, Federal regulators face Challenges governing risk management and internal control processes to fulfill their missions and provide stewardship of public resources. Further, many financial-sector regulatory organizations face Challenges in managing limited staff and preparing for the departure of institutional knowledge because of significant near-term retirements of experienced staff.

This report emphasizes the importance of government-wide coordination and information sharing for a particular sector – such as the financial sector – in a whole-of-government approach, as distinct from considering the issues on an agency-by-agency basis. Financial regulators may require this approach to coordinate and share information to support combating cybersecurity threats, take action when a crisis occurs, identify and address emerging risks and threats through strong governance, and ensure appropriate numbers of trained staff to recognize and mitigate financial system risks.

Addressing these Challenges in a coordinated and cohesive fashion is important, because the financial sector is one of 16 critical infrastructure[1] sectors that are vital to public confidence and the nation's safety, prosperity, and well-being. Moreover, the financial sector has changed considerably since the

[1] The term "critical infrastructure" is defined in the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act) as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact in security, national economic security, national public health or safety, or any combination of those matters." 42 U.S.C. §5195c(e).

last financial crisis. It is more diverse, technology dependent, and interconnected, spanning from Federal, state and local government regulators, to the largest institutions and the smallest community banks and credit unions, as well as those institutions' associated service providers. According to the Department of the Treasury (Treasury Department), from 2010 to 2017, more than 3,300 financial service technology-based firms were founded, and those firms represent 36 percent of all U.S. personal loans, an increase from 1 percent in 2010. Also, in 2018, 50 percent of people with bank accounts use mobile devices to access their information, compared to 20 percent in 2011. Further, the speed of technological advances in the financial sector and increased targeting of the financial system by malicious actors highlight the need for financial regulators to address the Challenges identified in this report.

CIGFO initiated this project to provide useful information to the leaders of financial-sector regulatory organizations as they look to develop strategies to improve efficiency, economy, effectiveness, and accountability at their agencies, consistent with Executive Order 13781, *Comprehensive Plan for Reorganizing the Executive Branch*. By consolidating and reporting these Challenges, CIGFO aims to inform regulatory organizations, FSOC, the Congress, and the American public as to the assessments by these Inspectors General.

CHALLENGE 1 ENHANCING OVERSIGHT OF FINANCIAL INSTITUTION CYBERSECURITY

Cybersecurity is "the process of protecting information by preventing, detecting and responding to attacks."[2] This Challenge centers on ensuring rigorous and relevant supervisory cybersecurity examination procedures to identify institution and sector weakness, and identify and address vulnerabilities with interconnections among financial institutions and third-party service providers.

The financial sector is diverse and interconnected and spans from the largest institutions (assets greater than $2 trillion) to the smallest community banks and credit unions. Financial institutions enter into a network of trusted interconnection agreements with other financial institutions; third-party service providers; Federal, state and local agencies; and the public to conduct their business. Those interconnections provide opportunities for contagion where a cybersecurity incident at a single point of entry may impact the entire financial system. Such IT security issues are particularly significant as the financial sector is recognized in Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience*,[3] as one of 16 critical infrastructure sectors[4] vital to public confidence and the nation's safety, prosperity, and well-being. As recognized in the Financial Services Sector-Specific Plan compiled by the Departments of Treasury and Homeland Security and the Financial Services Sector Coordinating Council,[5] "organizations that make up the Financial Services Sector form the backbone of the Nation's financial system and are a vital component of the global economy. These organizations are tied together through a network of electronic systems with innumerable entry points. An incident, whether manmade or natural, impacting these financial systems could have detrimental effects on the entire economy."[6]

The President's National Infrastructure Advisory Council[7] highlighted the significant cybersecurity risks to the financial services sector and concluded that the country had "a narrow and fleeting window of opportunity before a watershed, 9/11-level cyber attack to organize effectively and take bold action."[8] FSOC also underscored cybersecurity risks to the banking sector in its Annual Report for 2017 stating that, "[i]f severe enough, a cybersecurity failure could have systemic implications for the financial sector and the U.S. economy more broadly." The International Monetary Fund Working Paper, *Cyber Risk, Market Failures, and Financial Stability* (2017) recognized that the financial sector experienced the most cybersecurity incidents – by a substantial margin— across all industries with confirmed data losses in

[2] NIST Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (April 16, 2018).
[3] Presidential Policy Directive 21, Critical Infrastructure Security and Resilience (February 12, 2013).
[4] The 16 critical infrastructure sectors are (1) Chemical, (2) Commercial Facilities, (3) Communication, (4) Critical Manufacturing, (5) Dams, (6) Defense Industrial Base, (7) Emergency Services, (8) Energy, (9) Financial Services, (10) Food and Agriculture, (11) Government Facilities, (12) Healthcare and Public Health, (13) Information Technology, (14) Nuclear Reactors, Materials, and Waste, (15) Transportation Systems, and (16) Water and Wastewater Systems.
[5] The Financial Services Sector Coordinating Council is comprised of 70 members that include financial trade associations, financial utilities, and critical financial firms.
[6] Financial Services Sector-Specific Plan 2015.
[7] The President's National Infrastructure Advisory Council was established on October 16, 2001 and advises the President, through the Secretary of Homeland Security, on security and resilience of the Nation's critical infrastructure sectors and their functional systems, physical assets, and cyber networks.
[8] The President's National Infrastructure Advisory Council, Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure (August 2017).

2015. In recent testimony, the U.S. Government Accountability Office (GAO) recognized that technological developments such as artificial intelligence and the internet-of-things[9] makes the cybersecurity "threat landscape even more complex and can introduce security, privacy and safety issues that were previously unknown."[10]

Cybersecurity Examinations

Given the significance of the cybersecurity of U.S. financial institutions to depositors and the financial sector, IT examinations are an important tool to identify weaknesses and vulnerabilities. Financial regulators' IT examinations assess the management of IT risks, including cybersecurity at supervised institutions. When examinations identify undue risks and weak management practices at institutions, financial regulators may use formal and informal enforcement procedures to address those risks and practices as well as risks from deteriorating financial conditions, or violations of laws or regulations. In addition, as noted by GAO, IT examinations provide a means to analyze trends in specific security problems across institutions as well as assess cybersecurity across the entire financial sector.[11]

CIGFO members identified challenges regarding new IT examination programs which are designed and implemented to uncover IT weaknesses and vulnerabilities at financial institutions and across the financial sector. The Federal Housing Finance Agency (FHFA) OIG noted that FHFA will be challenged to ensure that newly developed cybersecurity examination guidance remains current and that it provides written guidance and training to examiners to aid them in their supervision of IT issues. The FDIC OIG also recognized challenges with the implementation of a new Information Technology Risk Examination program designed to enhance identification, assessment, and validation of IT and operations risks. In this regard, the FDIC OIG noted that the FDIC needed to continue building its capabilities to assess IT risks and trends and deploy IT examination staff commensurate with risks at FDIC-supervised institutions. Further, the FDIC OIG noted that a GAO study found that financial regulators did not routinely aggregate and analyze data on IT deficiencies found in individual financial institutions in order to analyze trends in specific security problems across institutions.[12]

Additionally, the National Credit Union Administration (NCUA) OIG noted the NCUA must continue to strengthen the resiliency of the entire credit union system because: cyber threats continue to pose significant dangers to the stability and soundness of the credit union industry; and credit unions and other small financial institutions are increasingly the target of cyberattacks. The Treasury Department OIG also recognized the Treasury Department's challenge in providing effective leadership to the financial sector and strengthening preparedness against cyber threats.

[9] U.S. Government Accountability Office defines the "internet-of-things" as technologies and devices that sense information and communicate it to the Internet or other networks and, in some cases, act on that information. U.S. Government Accountability Office, High Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation, GAO-18-645T (July 25, 2018).

[10] U.S. Government Accountability Office, High Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation, GAO-18-645T (July 25, 2018).

[11] U.S. Government Accountability Office, Cybersecurity: Banks and Other Depository Regulators Need Better Data Analytics and Depository Institutions Want More Useable Threat Information, Report No. GAO-15-509 (July 2015).

[12] U.S. Government Accountability Office, Cybersecurity: Banks and Other Depository Regulators Need Better Data Analytics and Depository Institutions Want More Useable Threat Information, Report No. GAO-15-509 (July 2015).

In *Critical Infrastructure Protection: Additional Actions Are Essential for Assessing Cybersecurity Framework Adoption*,[13] GAO assessed the extent to which the 16 critical infrastructure sectors, including the financial sector, have adopted the National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*[14] (NIST Framework) to manage their cyber risk. The NIST Framework is a set of industry standards and best practices to help organizations manage their cyber risk and includes five functional areas: (1) identify, (2) protect, (3) detect, (4) respond, and (5) recover. GAO found that 12 of 16 critical infrastructure sectors developed guidance to facilitate their respective sector's framework adoption. GAO found no formal financial sector-specific guidance for the NIST framework; however, GAO did note that the Financial Services Sector Coordinating Council developed an Automated Cybersecurity Assessment Tool to provide a means for financial institutions to assess cybersecurity and provide advice. In response to GAO's report, the financial sector leader, the Treasury Department, stated that it lacked legal authority to compel financial institutions to report their adoption of the NIST framework. Specifically, the Treasury Department was not authorized to receive any adoption information reported by financial institutions to their independent Federal and state regulators. Therefore, the Treasury Department does not have authority to obtain information from regulators to understand adoption of cybersecurity measures or cybersecurity weaknesses of the financial sector it leads.

Another challenge associated with IT examinations is ensuring that regulators have the right number of examiners with the appropriate skill sets to carry out examinations commensurate with an institution's IT complexity. As recognized by the Office of the Comptroller of the Currency (OCC) in its Semiannual Risk Perspective (Fall 2017 and Spring 2018), the speed and sophistication of cybersecurity threats are increasing and evolving; therefore examiners' skill sets and processes must keep pace with that threat. The OIG for the Board of Governors of the Federal Reserve System (Federal Reserve Board) and the Bureau of Consumer Financial Protection (BCFP) noted that the Federal Reserve Board must improve recruitment and retention as well as succession planning of cybersecurity resources to ensure an agile, diverse, and highly qualified cybersecurity workforce. Similarly, both the FDIC and FHFA OIGs noted the importance of recruiting and retaining a sufficient complement of examiners with experience needed to conduct examinations of IT systems.

Vulnerabilities in Interconnections with Third-Party Service Providers

Many financial institutions maintain contracts with third-party service providers (TSPs) to outsource certain bank functions such as IT operations or business product lines. As described by the Federal Financial Institutions Examination Council (FFIEC),[15] the term TSP, "generally includes independent third parties, joint venture/limited liability corporations, and bank and credit union service corporations that provide processing services to financial institutions."[16] The OCC recognized in its Semiannual Risk Perspectives (Spring 2017 and 2018) that TSPs are increasingly targets for cybercrime and espionage, and when compromised, may provide avenues to exploit bank operations through the supply of IT products and services that allow remote access and management of bank operations or applications. In

[13] U.S. Government Accountability Office, Critical Infrastructure Protection: Additional Actions Are Essential for Assessing Cybersecurity Framework Adoption, Report No. GAO-18-211 (February 2018).
[14] Available from NIST at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
[15] The FFIEC was established on March 10, 1979, pursuant to Title X of the Financial Institutions Regulatory and Interest Rate Control Act of 1978 (FIRA), Public Law 95-630. The FFIEC members include the Federal Reserve Board, the FDIC, the NCUA, the OCC, the State Liaison Committee, and the Bureau of Consumer Financial Protection.
[16] Supervision of Technology Service Providers, FFIEC IT Examination Handbook InfoBase.

addition, the OCC identified concerns with large numbers of banks relying on services from a small number of TSPs. Such concentration increases cybersecurity risks as an incident or compromise at a TSP may significantly impact a large segment of the banking industry. The Federal Reserve Board, FDIC, and OCC have statutory authority to supervise TSPs that enter into contractual arrangements with their regulated financial institutions; however, the NCUA does not have such authority.[17] The FFIEC coordinates TSP supervision and examination of TSPs.

The OIGs for the FDIC and the Federal Reserve Board and BCFP recognized challenges overseeing TSPs. The Federal Reserve Board and BCFP OIG noted a need to enhance oversight by implementing an improved governance structure and providing additional guidance to examination teams on the supervisory expectations for TSPs. The FDIC OIG highlighted work assessing 49 TSP contracts with 19 institutions showing that most FDIC-supervised institutions did not fully consider and assess the potential impact that a TSP may have on the institutions' cybersecurity.

Cybersecurity is a significant risk in the financial sector. Oversight and mitigation of financial institution cybersecurity risk may necessitate consideration of a whole-of-government, rather than an agency-by-agency, approach to eliminate barriers to information sharing and protect the financial sector infrastructure.

[17] 12 U.S.C. 1464(d)(7), 1867(c)(1). The Bureau of Consumer Financial Protection has authority as described in 12 U.S.C. 5514(e), 5515(d), and 5516(e). See CFPB Bulletin 2012-03 (Apr. 13, 2012), available at CFPB Bulletin. The NCUA does not have independent regulatory authority over TSPs.

CHALLENGE 2 MANAGING AND SECURING INFORMATION TECHNOLOGY AT REGULATORY ORGANIZATIONS

The Challenge on IT management and security incorporates the protection of financial-sector regulatory organizations' IT systems from individuals and groups with malicious intentions who can intrude and use their access to obtain sensitive information, commit fraud and identify theft, disrupt operations, or launch attacks against other computer systems and networks. The interconnection among private sector institutions and Federal, state and local government regulators form the ecosystem of the U.S. financial sector. A cybersecurity incident at any point in the systems may impact the entire financial system.[18]

Without proper safeguards, the information generated and collected on financial-sector regulatory organizations' IT systems – commercially valuable and market sensitive information, and significant amounts of personally identifiable information (PII)[19] for bank officials, depositors, and borrowers – remains vulnerable. For example, the FDIC highlighted eight data breaches where departing employees took sensitive information before leaving the FDIC. Those incidents affected 121,633 individual bank customers from approximately 380 financial institutions. The OIG also noted that the FDIC's Failed Bank Data System contained more than 2,500 terabytes of sensitive information for over 500 banks. Also, the OIG of the Department of Housing and Urban Development (HUD) reported concerns about the security of HUD data that included in excess of 300 million records for recipients of HUD-sponsored housing assistance, public housing, and Federal Housing Administration-insured mortgages.

According to the United States Computer Emergency Readiness Team, Federal government agencies reported more than 177,000 cybersecurity incidents from 2004 through 2016.[20] As recognized by GAO, IT security has been a high risk across all government agencies over the past 20 years.[21] In recent testimony on July 25, 2018, GAO recognized that the Federal Government needs to take urgent action to address cybersecurity challenges and that agencies have not implemented 1,000 of the 3,000 cybersecurity recommendations GAO made.[22]

[18] Financial Services Sector-Specific Plan 2015 issued jointly among the Department of the Treasury, Department of Homeland Security, and the Financial Services Sector Coordinating Council.

[19] According to OMB Memorandum 07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, the term PII refers to information that can be used to distinguish or trace an individual's identity, such as their name, Social Security Number, biometric records, etc. alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

[20] US-CERT is an organization within the Department of Homeland Security responsible for "analyzing and reducing cyber threats and vulnerabilities, disseminating cyber threat warning information, and coordinating incident response activities."

[21] U.S. Government Accountability Office, High Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others, Report No. GAO-17-317 (February 2017).

[22] U.S. Government Accountability Office, Testimony Before the Subcommittees on Government Operations and Information Technology, Committee on Oversight and Government Reform, House of Representatives, High Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation, Report No. GAO-18-645T (July 25, 2018).

CIGFO members identified the security of financial sector regulatory organizations' IT systems as a Challenge due to IT security risk management, obsolete technology, and a shortage of IT security professionals.

IT Security Risk Management

CIGFO members identified challenges related to the overall governance of their IT security programs and the resulting shortcoming in implementing cybersecurity best practices. Under the Federal Information Security Modernization Act of 2014,[23] Federal agencies must develop, document, and implement department- and agency-wide information security programs to protect information and information systems. Additionally, on May 11, 2017, the President issued Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* that, among other things, requires that Federal agencies use the NIST Framework to manage their cyber risk.

The HUD OIG identified HUD's decentralized and fragmented approach to its risk management program to incorporate and prioritize IT risks according to enterprise mission and business objectives. As a result, HUD continues to face the same IT challenges year after year. Specifically, the HUD OIG reported weaknesses in IT risk management, lagging IT modernization efforts, key IT staffing vacancies, the lack of technical contractor oversight, and gaps in HUD's information security continuous monitoring program.

The U.S. Securities and Exchange Commission (SEC) OIG noted that although the SEC Chairman initiated an assessment of the agency's cybersecurity risk profile and approach to cybersecurity from a regulatory and oversight perspective and the agency took steps to improve key information security program areas, the SEC OIG continued to identify opportunities to improve the SEC's information security controls. Among other things, the SEC OIG found that the SEC did not have a mature and consistently implemented information security continuous monitoring program; and to further mature the agency's incident response program, the SEC must ensure activities are repeatable and metrics are used to measure and manage the implementation of the program, achieve situational awareness, and control ongoing risk. Further, the SEC did not annually test its system-specific contingency plans and disaster recovery plans and had not fully implemented processes to identify gaps in skills and training for users with additional security and privacy responsibilities.

The Federal Reserve Board and BCFP OIG found inconsistent implementation of the Federal Reserve Board's information security risk management processes related to security control assessments, security planning, and authorization for select systems that resulted from a decentralized IT structure and inconsistent oversight of the Federal Reserve Board's risk management program. The Federal Reserve Board and BCFP OIG also identified that the BCFP faces challenges in centralizing and automating processes to better manage insider risks; ensuring that the Bureau's security information event management tool captures automated feeds from all systems, including contractor-operated systems; and aligning its information security program, policies, and procedures with the agency's evolving enterprise risk program.

In discussing this Challenge, the FDIC OIG identified that significant turnover of the FDIC's Chief Information Officer hindered the FDIC's progress in establishing an IT governance framework, including an information security plan. The FDIC OIG identified a number of information security control

[23] Public Law No. 113-283.

weaknesses involving systems access. Further, the FDIC did not devote sufficient resources to review potential breaches, and too much time elapsed between the discovery of an incident and the determination that the incident involved a data breach. The FDIC's IT restoration capabilities were limited, and the agency had not taken timely action to address known limitations with respect to its ability to maintain or restore critical IT systems and applications during a disaster.

Obsolete IT

The use of obsolete software, platforms, and systems can increase the vulnerability of financial-sector regulatory organizations' IT systems. As noted by GAO, if a vendor no longer supports a system, it will not prepare a "patch", *i.e.*, software code to fix defects."[24] According to GAO, attackers can exploit known unpatched vulnerabilities thus enabling unauthorized access to systems or enabling users to have access to greater privileges than authorized.

The HUD OIG reported challenges with many legacy IT systems running more than 400 IT applications on unsupported platforms, which increased the risk of unknown and unpatchable vulnerabilities. Overall, funding constraints diminished HUD's ability to replace and deactivate legacy systems that are 15 to 30 years old. Those systems result in high operation and maintenance costs and increased susceptibility to breaches. Further, the HUD OIG noted that such legacy systems are difficult to, or unable to, migrate to cloud computing technology and comply with two-factor authentication[25] system requirements. Similarly, the FDIC OIG identified security risks associated with obsolete technology including the management of software patches. The OIG identified that software used in the FDIC's server operating technology was at the end of its useful life and the vendor no longer supported it.

Shortage of IT Security Professionals

Financial-sector regulatory organizations also face challenges in attracting and retaining a cybersecurity workforce. GAO recognized that a significant impediment for agencies in expanding the Federal cybersecurity workforce is a shortage of available cybersecurity professionals.[26] In addition, as noted by the Office of Management and Budget (OMB), strengthening cybersecurity is not possible without the appropriate talent.[27]

The Treasury Department OIG highlighted that its cybersecurity work in many bureaus indicated that many of its IT security findings related to a lack of resources or management oversight. Further, the HUD OIG identified significant staffing challenges in filling key IT vacancies. It identified that during 2016 and 2017, 16 of 36 (44 percent) key IT managerial and supervisory positions at HUD headquarters were either vacant (11) or filled by temporary personnel (5). Such continued turnover in IT leadership roles reduces HUD's chances of correcting short- and long-term security challenges. Similarly, the FDIC OIG

[24] U.S. Government Accountability Office, Information Security: SEC Improved Control of Financial Systems but Needs to Take Additional Actions, Report No. GAO-17-469 (July 2017).

[25] According to NIST, two-factor authentication, also referred to as multi-factor authentication is a security enhancement that allows a user to present two pieces of evidence known as credentials when logging into an account. NIST Trusted Identities Group, Back to basics.

[26] U.S. Government Accountability Office, Federal Information Security: Actions Needed to Address Challenges, GAO-16-885T (September 19, 2016).

[27] Office of Management and Budget, Cybersecurity Strategy and Implementation Plan for the Federal Civilian Government, M-6-04 (October 30, 2015).

identified that turnover in key leadership positions affected the management of the FDIC's cybersecurity and privacy programs. Between 2010 and 2017, the FDIC had seven acting or permanent Chief Information Officers who also held the role of Chief Privacy Officer. During this same period of time, the FDIC also had seven Chief Information Security Officers. These senior management changes impact the direction of an organization because turnover affects management strategy, planning, budgets, and staffing.

As global cyber intrusions continue to increase, it is important for financial-sector regulatory organizations to safeguard their systems and data. Improving IT security risk management governance, addressing obsolete technology, and enhancing security expertise minimizes the risks associated with breaches, including the compromise of sensitive data and PII.

CHALLENGE 3 SHARING THREAT INFORMATION

This Challenge relates to disclosing and sharing threat information among financial sector participants and government agencies to combat current and emerging cyber threats, terrorist financing, money laundering, and other threats to the financial sector. Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience* designated the financial sector as part of the critical infrastructure of the United States. Accordingly, Federal departments and agencies must collaborate with sector critical infrastructure owners and operators to ensure the infrastructure can withstand all hazards and rapidly recover from disasters. Under the leadership of the Departments of the Treasury and Homeland Security, sector-specific plans recognize the need for sharing timely and actionable information to manage risk.[28] This Challenge is of significant importance to the financial sector given the increasing speed and sophistication of cyber threats as well as the anonymity provided by innovative technology such as virtual currencies.[29] The two key threat information challenges identified by CIGFO members include providing timely and relevant threat information to financial institutions and examiners, and sharing information among regulatory organizations to combat terrorist financing and money laundering.

Sharing Threat Information with Financial Institutions and Examiners

The U.S. Government gathers threat information about domestic financial institutions and the financial system. In its report, *Cybersecurity: Banks and Other Depository Regulators Need Better Data Analytics and Depository Institutions Want More Usable Threat Information,* GAO identified numerous sources of threat information throughout the Federal government (see Figure 1).[30] In its Annual Report for 2017, FSOC called upon government agencies to "share information with the industry to enhance cybersecurity resilience… [and] continue efforts to declassify (or downgrade classification) to the extent practicable, consistent with national security needs."[31]

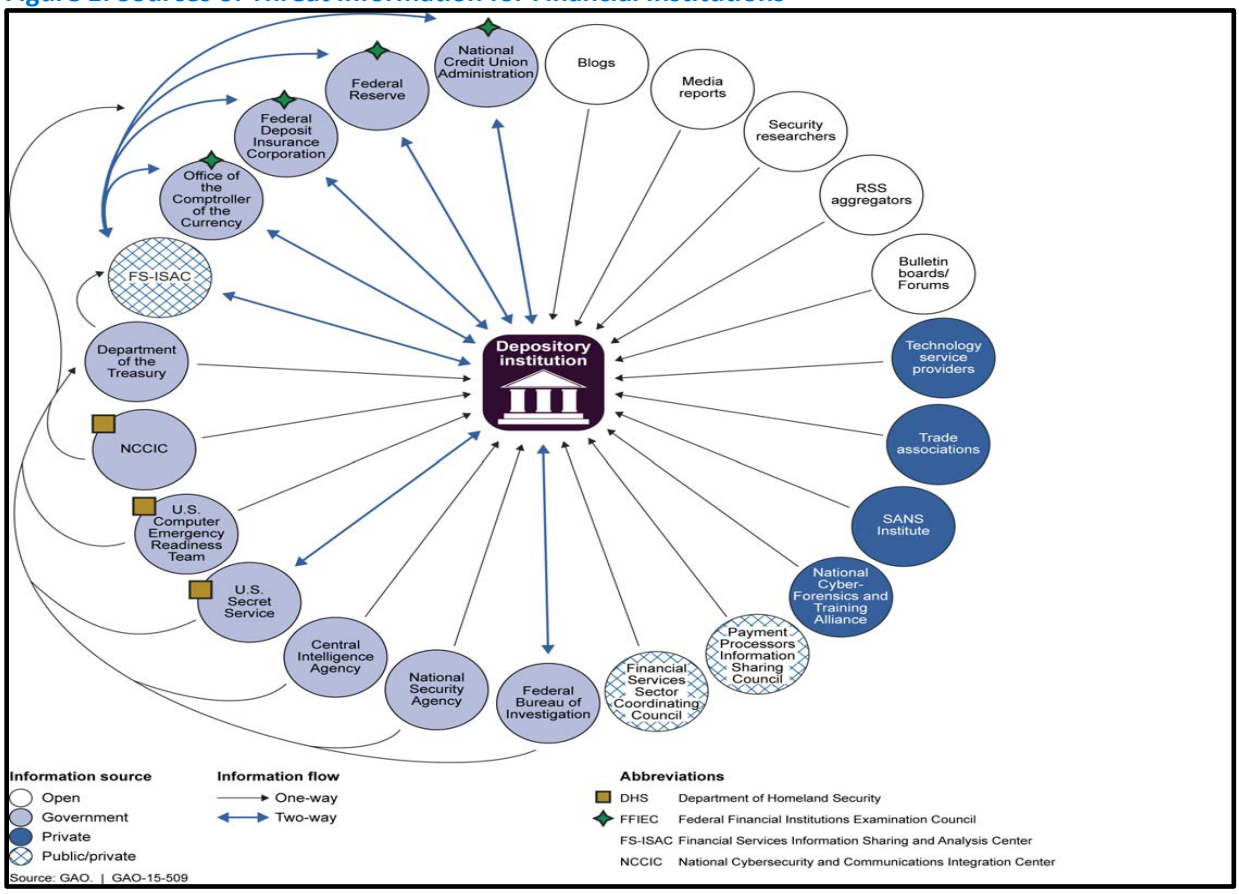
[28] In 2006, the Department of Homeland Security developed the National Infrastructure Protection Plan (NIPP); one portion of the NIPP relates to the financial sector – the *Banking and Finance Critical Infrastructure and Key Resources Sector-Specific Plan (Financial Sector-Specific Plan)*. The plans are updated periodically and the current versions of the plans are the 2013 NIPP and the 2015 Financial Sector-Specific Plan.

[29] Office of the Comptroller of the Currency (OCC) in its Semiannual Risk Perspective (Spring 2017), states that the speed and sophistication of cybersecurity threats are increasing, therefore, examiners' skill sets and processes must keep pace with that threat.

[30] U.S. Government Accountability Office, Cybersecurity: Banks and Other Depository Regulators Need Better Data Analytics and Depository Institutions Want More Usable Threat Information, Report No. GAO-15-509 (July 2015).

[31] FSOC 2017 Annual Report.

Figure 1: Sources of Threat Information for Financial Institutions



The Commodity Futures Trading Commission (CFTC) OIG identified the need for the CFTC to take a leadership position to increase automated risk analysis and information sharing to alert and educate CFTC registrants of incidents, threats, and defense measures in real time. The Federal Reserve Board and BCFP OIG recognized challenges to ensure that supervisory approaches keep pace with evolving cyber threats to financial institutions and the financial services sector. Further, the Federal Reserve Board and BCFP OIG recognized that the Federal Reserve Board must enhance its communication of critical IT and cybersecurity-related risks relevant to the Federal Reserve Board and supervisory personnel.

The Treasury Department OIG recognized that the Treasury Department must provide effective leadership to financial institutions and the financial sector to strengthen awareness of, and preparedness for, cyber threats. The FDIC OIG identified challenges with the FDIC ensuring that financial institutions and their service providers receive actionable intelligence in order to secure their systems and respond quickly to mitigate the impact of a breach. Further, the FDIC OIG noted that threat information held by the U.S. Government is critical to an examiner's understanding of current threat levels and types in order to focus examinations and prioritize areas for supervisory attention.

Sharing Information Among Regulators to Combat Terrorist Financing, Money Laundering, and Other Financial Crimes

Preventing terrorist financing requires massive amounts of data sharing while not compromising national security.[32] Federal Reserve Board Vice Chairman Randal Quarles noted that bank regulators have a bigger role to play in preventing cybercrime and should focus on connecting financial institutions with national security agencies.[33] The former Comptroller of the Currency, Thomas Curry also warned that "[w]e can't allow the Federal banking system to be compromised by hackers or used by criminals or terrorists."[34]

The Treasury Department OIG reported that identifying, disrupting, and dismantling financial networks that support terrorists, organized international crime, weapons of mass destruction proliferators, and other threats to international security continues to be a challenge. Specifically, the Treasury Department OIG noted that combating terrorism and other illicit financing depends on a whole-of-government approach that requires collaboration and coordination among Federal agencies, including regulators and law enforcement. As identified by the Treasury Department OIG, the Treasury Department's Financial Crimes Enforcement Network (FinCEN) continues to face challenges to collect, analyze, and report on national and international threats. FinCEN focuses on partnering with Federal banking regulators and law enforcement to enhance enforcement efforts and strengthen transparency by issuing rules and regulations requiring financial institutions to identify beneficial ownership of financial accounts.

The financial sector also faces terrorist financing, money laundering, and other financial crime threats posed by new virtual currencies. According to Forbes, there are more than 1,000 different virtual currencies.[35] As noted by GAO, virtual currencies lack the transparency and regulation underlying traditional payment systems.[36] Such currencies, therefore, may lend themselves to money laundering, financial and other crimes including cross-border criminal activities, and consumer protection issues related to the loss of funds on virtual exchanges. The FDIC OIG highlighted that the United States does not yet have a direct and comprehensive program to conduct oversight of the virtual currency markets.[37] The OIG also recognized the FDIC should continue to monitor issues surrounding virtual currencies, to ensure examiners and institutions are aware of the threats posed by these evolving technologies.

Threat information helps financial regulators understand and target their resources to combat cybersecurity risks, terrorist financing, money laundering and other financial crimes. The dissemination of threat information contained within databases and repositories of regulators and their government partners to financial-sector participants helps all parties more effectively take action to mitigate those threats.

---

[32] American Banker, Next stop on the reg relief train: reforming AML rules (May 3, 2018).
[33] American Banker, Regulators Have Bigger Role to Play in Cybersecurity (December 1, 2017).
[34] Office of the Comptroller of the Currency, Semiannual Risk Perspective (Fall 2015).
[35] 2018 Will See Many More Cryptocurrencies Double in Value (January 2, 2018).
[36] U.S. Government Accountability Office, GAO Virtual Currencies: Emerging Regulatory, Law Enforcement, and Consumer Protection Challenges, GAO-14-496 (2014).
[37] Some financial-sector regulators issued guidance on virtual currencies. FinCEN's Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime (FIN-2016-A005 October 25, 2016) and CFTC Backgrounder on Oversight of and Approach to Virtual Currency Futures Markets (January 4, 2018).

CHALLENGE 4 READINESS FOR CRISES

This Challenge reflects readiness to mitigate risks and, when necessary, resolve failed banks and credit unions in the event of a banking crisis or other disruption to the financial system, and the administration of programs directed towards victims of disasters. In its report of the causes of the financial crisis, the Financial Crisis Inquiry Commission concluded, among other things, that "widespread failures in financial regulation and supervision proved devastating to the stability of the nation's financial markets."[38] The report identified that nearly $11 trillion in household wealth vanished during the financial crisis that began in 2008. Nearly 4 million families lost their homes to foreclosure, while another 4-1/2 million either entered the foreclosure process or were seriously behind on mortgage payments, and 26 million Americans were out of work, could not find full-time jobs, or gave up looking for work.[39] As reported in the FDIC's *Crisis and Response, An FDIC History, 2008-2013*, the net cost of the crisis was up to "roughly 80 percent of an entire year's gross domestic product."[40] The financial crisis resulted in 489 bank failures from 2008 through 2013. These failures cost the Deposit Insurance Fund (DIF) approximately $72 billion, and the DIF fell to the lowest level in history, a negative $20.9 billion by the end of 2009.[41]

Financial regulatory authority and financial sector complexity have evolved significantly since the financial crisis. Notably, the Dodd-Frank Act was designed to prevent excessive risk taking that led to the financial crisis and, among other things, provided regulators with additional tools to shut down failing financial companies without precipitating panic or requiring taxpayer bailouts.[42] The financial sector has also become more complex and interconnected through the introduction of service providers and increased use of financial technology for banks products, services, and operations.[43] Such interconnections may increase the speed of future crises.

[38] The Financial Crisis Inquiry Commission was established by statute, Financial Enforcement and Recovery Act (2009), to "examine the causes of the current financial and economic crisis in the United States." The Commission was independent and composed of a 10-member panel of experienced financial experts knowledgeable in housing, economics, finance, market regulation, banking, and consumer protection. These members were selected by the leadership in Congress at the time. The Financial Crisis Inquiry Report, the Final Report of the National Commission on the Causes of the Financial and Economic Crisis in the United States (January 2011).

[39] The Commission and staff reviewed millions of pages of documents, interviewed more than 700 witnesses, and held 19 days of public hearings. See also, U.S. Government Accountability Office, Financial Regulatory Reform: Financial Crisis Losses and Potential Impact of the Dodd-Frank Act, GAO-13-180 (January 2013).

[40] The FDIC conducted a study of the financial crisis entitled Crisis and Response, An FDIC History, 2008-2013, published in December 2017.

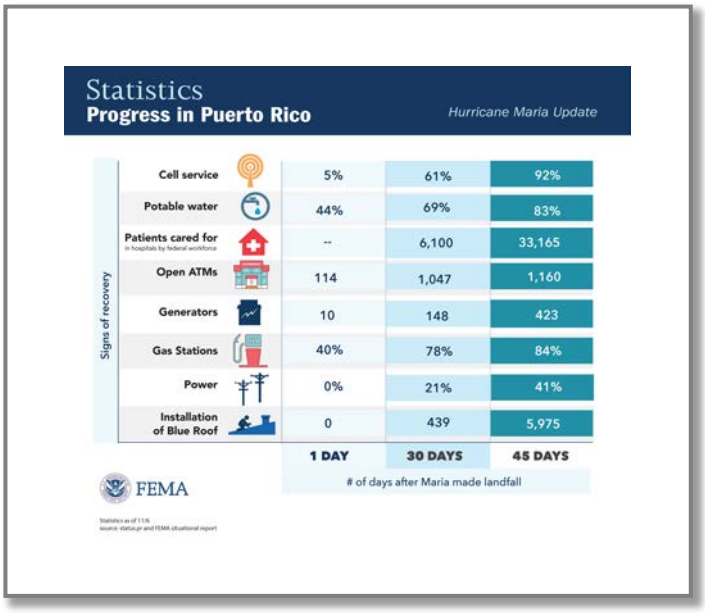
[41] Since the end of 2009, the DIF has grown every quarter and became positive in the second quarter of 2011. The DIF balance as of December 31, 2017 was $92.7 billion.

[42] Wall Street Reform: The Dodd-Frank Act, The White House summary.

[43] OCC Semiannual Risk Perspective (Spring 2018).

In addition to the banking crisis, Congress has appropriated more than $49.6 billion in supplemental funding to HUD since 1993 to address long-term recovery in the wake of the attacks of September 11, 2001; Hurricanes Katrina, Rita, and Wilma in 2005; Hurricanes Ike and Gustav and Midwest flooding in 2008; Hurricane Sandy in 2012; and the Louisiana flooding event and Hurricane Matthew in 2016. When disasters strike, there are disruptions in services that affect banks and their customers, and financial regulatory organizations. As noted by the Federal Emergency Management Agency (FEMA) statistics for Hurricane Maria in Puerto Rico in September 2017 (see Figure 2), cellular phone service, ATMs, gas stations, and power services were unavailable after the hurricane's landfall and were not fully restored even 45 days after the event. In Puerto Rico alone, FEMA obligated $2.7 billion for public assistance grants.[44]

Figure 2: FEMA Hurricane Maria Statistics



Readiness for Failures of Financial Institutions

Financial-sector regulatory organizations have supervisory responsibilities to identify and mitigate potential systemic problems in the financial sector. When supervisory mitigation cannot stem failures or economic events overtake such mitigation, the FDIC and the NCUA, in conjunction with other Federal and state regulators, resolve failed banks and credit unions. It has been 10 years since the financial crisis. As noted by former FDIC Chairman Martin J. Gruenberg, regulators "should guard against the temptation to become complacent about the risks facing the financial system."[45] Further, in those 10 years since the crisis, the financial system has changed significantly. The Office of Financial Research[46] in its Annual Report for 2017 identified that new vulnerabilities have emerged since the previous financial crisis and highlighted key threats to the financial system.[47] For example, the increased use of automated trading systems, increased speed of executing financial transactions, and a wider variety of trading venues and liquidity providers. As recognized by former FDIC Chairman Gruenberg, "the evolution of the global financial system towards greater interconnectedness and complexity may tend to increase the frequency, severity, and speed with which the financial crises occur."[48]

---

[44] Federal Emergency Management Agency Puerto Rico Hurricane Maria statistics.

[45] Remarks by Martin J. Gruenberg, Chairman, Federal Deposit Insurance Corporation on Financial Regulation: A Post Crisis Perspective; Brookings Institution, Washington, D.C. (November 14, 2017).

[46] The Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 established the Office of Financial Research within the Department of the Treasury to support the Financial Stability Oversight Council.

[47] Annual Report to Congress, Office of Financial Research (2017).

[48] According to FDIC analysis, failure rates increased much faster during the 2008–2013 crisis than during the 1980s and early 1990s banking and thrift crises. For example, by 2009 almost 2 percent of banks had failed—a rate that was not reached in the previous crisis until the eighth year.

The NCUA OIG noted that the NCUA faces several challenges that threaten the safety and soundness of the credit union system and the National Credit Union Share Insurance Fund.[49] The NCUA outlined risks with changes to the credit union market. These risks include: growing disparity in the performance of large and small credit unions specific to loan and net worth growth and membership; increasing competition in the financial services industry; and continuing consolidation among depository institutions The FDIC OIG identified challenges with the FDIC's continued readiness to fulfill its mission of insuring deposits and managing receiverships. Specifically, the FDIC will be challenged to ensure that plans are in place to react and respond quickly to a crisis, irrespective of their cause, nature, magnitude, or scope; ensure those plans are current and up-to-date; and incorporate lessons learned from past crises and the related bank failures.

Readiness for Disaster Aid

In response to Presidentially declared disasters, Congress may authorize additional funding to HUD for the Community Development Block Grant Program when there are significant unmet needs for long-term recovery.[50] HUD awards grants to state and local governments who, in turn, may grant money to state agencies, non-profit organizations, economic development agencies, citizens, and businesses. The State and local governments provide these funds for disaster relief, long-term recovery, restoration of infrastructure, housing, and economic revitalization.

The HUD OIG identified that HUD will have tremendous future challenges resulting from disaster relief efforts in response to Hurricanes Harvey in Texas, Irma in Florida, and Maria in Puerto Rico. The amount of HUD funding needed to assist in recovery efforts will be enormous, and HUD will be challenged to monitor grants to ensure that expenditures are eligible and supported. In 38 prior audits and 4 evaluations and investigations related to activities for grants for Hurricane Sandy and other disasters from 2011 through 2013, HUD OIG identified $119.6 million in ineligible or unnecessary costs, $465 million in unsupported costs, and $5.3 billion in funds put to better use. Historically, HUD has been challenged to have resources to appropriately monitor disaster grants according to established policies and procedures. The HUD OIG found that disaster recovery funds were not always used for eligible and supported items and state and local government grantees did not always follow Federal procurement standards when making purchases. The HUD OIG also identified challenges that citizens face in receiving timely disaster-related funding and the possibility of repaying disaster funds because of duplicate benefits from multiple Federal agencies.

Disruptions to the financial sector may come from many sources and at any time. Risk mitigation and crisis planning allows financial-sector regulatory organizations to stand ready to address these disruptions.

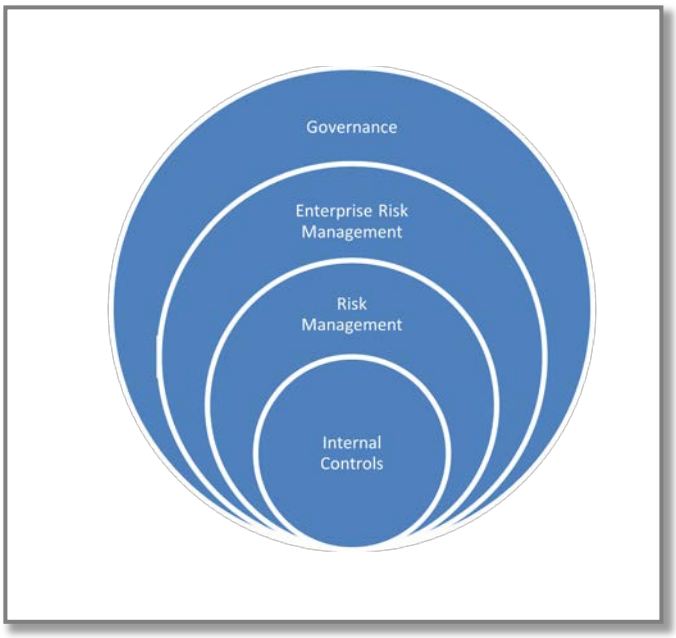
[49] Created by Congress in 1970, NCUA administers the Share Insurance Fund and insures individual credit union member accounts against losses up to $250,000 and a member's interest in all joint accounts combined up to $250,000. https://www.ncua.gov/services/Pages/share-insurance.aspx

[50] Community Development Block Grant Disaster Recovery Fact Sheet available at www.hudexchange.info/resources/documents/CDBG-DR-Fact-Sheet.pdf

CHALLENGE 5 STRENGTHENING AGENCY GOVERNANCE

This Challenge involves ensuring financial-sector regulatory organizations' governance processes – including enterprise risk management (ERM) and internal controls – are in place so that agencies can fulfill their missions and provide stewardship of public resources. As described in OMB Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control,* (OMB Circular A-123) "[f]ederal leaders and managers are responsible for establishing and achieving goals and objectives, seizing opportunities to improve effectiveness and efficiency of operations, providing reliable reporting, and maintaining compliance with relevant laws and regulations."[51] As reflected in OMB's concentric circle diagram (see Figure 3), Federal leaders and managers are responsible for establishing a governance structure to direct and oversee implementation of a risk management and internal control process. ERM and internal controls are components of this governance framework.

Figure 3: OMB Governance Model



Source: Office of Management and Budget

The governance of risk and internal controls plays an important role, given the March 13, 2017 Executive Order 13781, *Comprehensive Plan for Reorganizing the Executive Branch*. The Executive Order requires that OMB and Federal agencies propose plans to improve efficiency, effectiveness, and accountability of Federal agencies, including potential elimination or reorganization of redundant agencies.

Enhance Enterprise Risk Management

ERM is a discipline to identify, assess, and manage risks. OMB Circular A-123 encourages agencies to develop a risk management council and risk profiles that identify risks arising from mission and mission-support operations; and consider those risks as part of the annual strategic review process.

A number of CIGFO members identified challenges with the implementation of ERM. The Federal Reserve Board and BCFP OIG identified challenges to the Federal Reserve Board's complex governance approach. Specifically, the Federal Reserve Board's decentralized structure and lack of a single authority to manage agency-wide functions such as human capital, IT services, physical infrastructure, and internal controls and risk management resulted in redundancies and potentially higher costs in certain areas.

[51] Office of Management and Budget Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control (July 15, 2016).

The Federal Reserve Board has made limited progress in establishing internal control processes and an ERM system to manage the risks it faces as it works to achieve its strategic objectives or that arise from its activities and operations. Similarly, HUD OIG recognized that HUD lacked an ERM approach to monitoring risk and that, for the most part, each program office monitors risk, and program office approaches and results differ greatly. The FDIC OIG identified challenges in the FDIC's implementation of ERM. Staffing changes and a reorganization and re-alignment of the Chief Risk Officer organization slowed integration of ERM into the FDIC's culture. In 2011, the FDIC established a Chief Risk Officer who reported to the FDIC Chairman and managed an Office of Corporate Risk Management. This structure provided an organization within the FDIC to review risk with a system-wide perspective and instill risk governance as part of the FDIC's culture. In September 2017, however, the FDIC transferred the ERM function to the Division of Finance, and the Chief Risk Officer now reports to the Division Director and the Chief Financial Officer rather than directly to the Chairman.

The Special Inspector General for the Troubled Asset Relief Program (SIGTARP) identified the need for the Treasury Department to improve its governance and oversight of the Troubled Asset Relief Program (TARP). SIGTARP found that the Treasury Department has significantly scaled back its oversight of TARP's housing programs, which increases the risk of fraud, waste, and abuse by mortgage servicers and others receiving TARP funds, and jeopardizes the agencies who participate in TARP housing programs. SIGTARP also found waste and misuse of TARP dollars by state agencies that the Treasury Department relies on to manage TARP programs due to weaknesses in oversight and failures to impose or monitor appropriate Federal requirements.

Improve Internal Controls

OMB Circular A-123 emphasizes the need for agencies to coordinate risk management and strong and effective internal controls into existing business activities as an integral part of governing and managing an agency. Internal controls provide reasonable assurance that the objectives of the agency will be achieved.

The Federal Reserve Board and BCFP OIG found that the BCFP must strengthen its internal controls by documenting controls, transactions, and other significant events in a manner to ensure the effective design, implementation, and operation of an internal control system. The Federal Reserve Board and BCFP OIG noted specific internal control shortcomings with BCFP acquisitions, procedures for documenting examination results, and granting access rights to examination documentation and materials. The HUD OIG identified the need for HUD to establish a framework for operational risks and controls to ensure an effective system of internal control across HUD and within all programs.

ERM and internal controls assist financial sector regulatory organizations in anticipating, managing, and mitigating risks. When organizations capture and consider risks both vertically (*i.e.*, up and down an organization) and horizontally (*i.e.*, across organizational units), leaders have the information to improve the quality of their decision making as they execute their missions.

CHALLENGE 6 MANAGING HUMAN CAPITAL

Financial-sector regulatory organizations rely on skilled personnel to achieve their respective missions and personnel costs are their largest budget line item for many regulators. Bank and credit union examiners, economists, regulatory enforcement personnel, and policy makers help to ensure the safety and soundness of the U.S. financial system. Challenges include succession management for the wave of projected retirements and managing human capital in an environment of limited and uncertain budgets. Further, Executive Order 13781, *Comprehensive Plan for Reorganizing the Executive Branch,* requires agencies to submit Agency Reform Plans that include long-term workforce plans designed to align with agency strategic plans.

Succession Planning

GAO identified strategic human capital management as a high-risk area across all of government for 17 years and recognized that human capital risks "impede the Federal government from cost-effectively serving the public and achieving results."[52] According to estimates from the Office of Personnel Management, 34.3 percent of all Federal employees are eligible to retire by fiscal year 2020.[53] CIFGO members identified succession planning issues in line with GAO findings. The HUD OIG noted that 43 percent of HUD's career workforce on board as of September 20, 2014 was eligible to retire by 2019. Given that statistic, the HUD OIG noted that HUD will be challenged to fill critical skills gaps and ensure that it fulfills its mission. The FDIC OIG also recognized the challenge the FDIC faces as more than 25 percent of the FDIC's current permanent workforce is projected to retire over the next 10 years and many others are eligible to retire. To fulfill its mission, the FDIC must work to maintain a steady flow of new examiners to step into the roles currently filled by seasoned examiners. In addition, the FDIC must manage "knowledge transfer" from the more experienced personnel to the newer staff. The Federal Reserve Board and BCFP OIG identified that the BCFP will be challenged to implement its succession management program to ensure the continuity of knowledge and leadership across the organization. The Federal Reserve Board and BCFP OIG also noted that the expected rise in the number of Federal Reserve Board employees eligible for retirement may contribute to gaps in leadership and institutional knowledge.

Effective Human Capital Management

In addition to succession planning, CIGFO members noted challenges in managing the existing workforce and ensuring they have the appropriate number of personnel, with the right skill sets and appropriate use of technology to continue to fulfill their respective missions. The HUD OIG identified as a major challenge HUD's ability to manage its limited staff to accomplish its mission. Specifically, the HUD OIG noted that HUD lacks a valid basis for assessing its human resource needs and allocating staff within program offices. The FDIC OIG described the FDIC's challenge to determine the appropriate number of examination and support staff to support ongoing work as well as increase staffing during crisis periods.

[52] U.S. Government Accountability Office, High-Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others, Report number GAO-17-317 (February 2017).
[53] GAO analysis of Office of Personnel Management's Enterprise Human Resource Integration database, GAO-17-627T (May 18, 2017).

Further, the FDIC OIG noted the need for increased use of off-site monitoring technology to assess banks' safety and soundness in order to preserve examiner resources.

The Federal Reserve Board and BCFP OIG described the Federal Reserve's challenge to hire staff with appropriate skill sets given a highly competitive job market. The SEC OIG highlighted a 2016 GAO report on the SEC's personnel management that stated because the SEC had not identified skills gaps among its hiring specialists; its training of these staff was limited. GAO concluded that the SEC lacked the assurance that its hiring specialists will hire the most qualified applicants.

Other CIGFO members indicated challenges with vacancies in significant management positions and the expiration of acting positions. The Treasury Department OIG noted that several Presidentially appointed, Senate-confirmed leadership positions within the Treasury Department have been vacant since January 2017. Similarly, the HUD OIG indicated challenges with financial management governance due to the vacancy of the Chief Financial Officer and other senior positions. The FDIC OIG also noted that the FDIC's internal Board of Directors member position has been vacant since June 2015.

The management of human capital has a direct relationship to the achievement of financial-sector regulatory organizations' missions. Full alignment and focus on the life-cycle of human capital activities – workforce planning, recruitment, on-boarding, compensation, engagement, succession planning, and retirement programs – allows for effective achievement of an organization's mission.

CONCLUSION

CIGFO members developed this report to assist policy makers in determining how best to address the Challenges facing financial-sector regulators, including fostering consideration of a whole-of-government approach to coordination and information sharing. Consistent with the mission of IGs, the report helps inform the public by providing them with information about the important Challenges facing the financial sector to which most of the public is directly connected through bank or credit union accounts and mortgages. This report also informs CIGFO members in their identification of future Challenges and collaboration on reviews addressing cross-cutting Challenges facing the financial sector.

APPENDIX 1 ABBREVIATIONS AND ACRONYMS

Abbreviation and Acronym	Full Name
BCFP	Bureau of Consumer Financial Protection
CFTC	Commodity Futures Trading Commission
Challenges	The CIGFO Top Management and Performance Challenges identified in this report.
CIGFO	Council of Inspectors General on Financial Oversight
DIF	Deposit Insurance Fund
Dodd-Frank Act	The Dodd-Frank Wall Street Reform and Consumer Protection Act
ERM	Enterprise Risk Management
FDIC	Federal Deposit Insurance Corporation
Federal Reserve Board	Board of Governors of the Federal Reserve System
FEMA	Federal Emergency Management Agency
FFIEC	Federal Financial Institutions Examination Council
FHFA	Federal Housing Finance Agency
FinCEN	Financial Crimes Enforcement Network
FISMA	Federal Information Security Modernization Act of 2014
FSOC	Financial Stability Oversight Council
GAO	U.S. Government Accountability Office
HUD	Department of Housing and Urban Development
IT	Information Technology
NCUA	National Credit Union Administration
NIST	National Institute for Standards and Technology
NIST Framework	NIST Framework for Improving Critical Infrastructure Cybersecurity
OCC	Office of the Comptroller of the Currency
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	Personally Identifiable Information
SEC	Securities and Exchange Commission
SIGTARP	Special Inspector General for the Troubled Asset Relief Program
TMPC	Top Management and Performance Challenges
Treasury Department	Department of the Treasury
TSP	Third-party service provider

APPENDIX 2 METHODOLOGY

We reviewed nine TMPC reports issued by CIGFO members listed below that covered challenges identified in 2017.[54] Specifically, we reviewed every challenge reported in each TMPC report to identify common challenges reported by multiple CIGFO members. Through this process, we identified the most frequently reported challenges of CIGFO members by category, which resulted in six challenges being identified. Once we established these categories, we reviewed individual challenges to determine whether we could also identify any common themes or key areas of concern.

Department of the Treasury

Federal Deposit Insurance Corporation

Commodity Futures Trading Commission

Bureau of Consumer Financial Protection

Department of Housing and Urban Development (begins on page 125)

Board of Governors of the Federal Reserve System

Federal Housing Finance Agency

National Credit Union Administration (begins on page 81)

Securities and Exchange Commission

Special Inspector General for the Troubled Asset Relief Program Quarterly Reports to Congress

[54] The Special Inspector General for the Troubled Asset Relief Program does not issue a top management and performance challenges report to the Treasury Department. However, SIGTARP has published its assessment of the most serious management and performance challenges and threats facing the Government in TARP in its Quarterly Report to Congress since October 2017.

CIGFO Audit of the Financial Stability Oversight Council's **Monitoring of International Financial Regulatory Proposals and Developments**

May 2019

CIGFO-2019-01

Office of Inspector General
Board of Governors of the Federal Reserve System
Consumer Financial Protection Bureau

Table of Contents

Abbreviations

CIGFO	Council of Inspectors General on Financial Oversight
Dodd-Frank Act	Dodd-Frank Wall Street Reform and Consumer Protection Act
FSB	Financial Stability Board
FSOC or Council	Financial Stability Oversight Council
IOSCO	International Organization of Securities Commissions
LIBOR	London Interbank Offered Rate
RRC	Regulation and Resolution Committee
SRC	Systemic Risk Committee
Treasury	Department of the Treasury

Message from the Chair

Dear Mr. Chairman:

I am pleased to present you with the Council of Inspectors General on Financial Oversight (CIGFO) report titled, Audit of the Financial Stability Oversight Council's Monitoring of International Financial Regulatory Proposals and Developments.

One of the statutory duties of the Financial Stability Oversight Council (FSOC) is to monitor domestic and international financial regulatory proposals and developments, including insurance and accounting issues, and to advise Congress and make recommendations in such areas that will enhance the integrity, efficiency, competitiveness, and stability of the U.S. financial markets.

FSOC's monitoring of international financial regulatory proposals and developments is conducted in the context of FSOC's statutory purposes, which focuses on developments that could pose risks to the stability of the U.S. financial system.

CIGFO convened a Working Group to assess FSOC's monitoring of international financial regulatory proposals and developments. In this resulting audit report, we concluded that FSOC has a process for monitoring international financial regulatory proposals and developments. All FSOC members or member representatives who offered an opinion described FSOC's monitoring process as adequate. Although described as adequate, several FSOC members or representatives offered suggestions for enhancing the process. We encourage FSOC to consider incorporating into its process the suggestions made by its members to the extent the suggestions are consistent with FSOC's focus on identifying and addressing threats to the stability of U.S. financial system. We are not making any recommendations to FSOC as a result of this audit.

I would like to take this opportunity to thank the FSOC members for their support, especially those Department of the Treasury officials who assisted with this effort.

CIGFO looks forward to working with you on this and other issues. In accordance with the Dodd-Frank Wall Street Reform and Consumer Protection Act, CIGFO is also providing this report to Congress.

Sincerely,

/s/

Eric M. Thorson

Chair, Council of Inspectors General on Financial Oversight

This page is intentionally blank

Executive Summary

Why and How We Conducted this Audit

The Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act)[1] created regulatory and resolution frameworks designed to reduce the likelihood, and severe economic consequences, of financial instability. The Dodd-Frank Act established the Financial Stability Oversight Council (FSOC or Council) and charged it 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. Among other duties, Title I of the Dodd-Frank Act requires FSOC to monitor domestic and international financial regulatory proposals and developments, including insurance and accounting issues, and to advise Congress and make recommendations in such areas that will enhance the integrity, efficiency, competitiveness, and stability of the U.S. financial markets.

The Dodd-Frank Act also created the Council of Inspectors General on Financial Oversight (CIGFO), whose members include the Inspectors General with oversight authority for the majority of FSOC's member agencies. The Dodd-Frank Act authorizes CIGFO to convene a Working Group of its members to evaluate the effectiveness and internal operations of FSOC. In December 2017, CIGFO convened a Working Group to conduct an audit to assess FSOC's monitoring of international financial regulatory proposals and developments for the period of January 2016 to January 2018.[2] The Working Group was led by the Department of the Treasury's (Treasury) Office of Inspector General, whose Inspector General is the Chair of CIGFO.

To accomplish the audit objective, the Working Group reviewed the Dodd-Frank Act to determine FSOC's statutory purposes and duties. It reviewed FSOC's governance documents, annual reports, meeting minutes, and committee meeting agendas. It also interviewed staff from the FSOC Secretariat at Treasury as well as interviewed or received responses from FSOC members

1 Public Law No. 111-203, enacted July 21, 2010.
2 See Appendix IV for a listing of Working Group members.

and member agency representatives to develop a better understanding of FSOC's monitoring of international financial regulatory proposals and developments. The Working Group conducted fieldwork from February 2018 through June 2018. Appendix I provides additional details about the objective, scope, and methodology of this audit.

What We Learned

FSOC monitors international financial regulatory proposals and developments in several ways. First, FSOC develops and publishes an annual report, which describes important international financial regulatory proposals and developments, identifies emerging threats to U.S. financial stability, and can include recommendations related to these issues. FSOC also follows up on the issues, threats, and recommendations identified in its annual report. Second, FSOC members periodically discuss international topics at their meetings, and are given presentations by experts from relevant member agencies. Third, the staffs of FSOC member agencies share information on these topics in FSOC's staff-level committees, primarily the Systemic Risk Committee (SRC). Finally, some FSOC member agencies have their own international engagement, which can inform their participation in FSOC meetings.

FSOC members and FSOC member agency representatives expressed their overall satisfaction with FSOC's monitoring of international activities and proposals, and believed that the process was adequate. Several FSOC members offered suggestions for process enhancements which are included on pages 8 and 9 of this report. We encourage FSOC to consider incorporating the suggestions made by these members into its processes to the extent the suggestions are consistent with FSOC's purposes of identifying risks to U.S. financial stability, promoting market discipline, and responding to emerging threats to the stability of the U.S. financial system. We are not making any recommendations to FSOC as a result of our audit.

FSOC Response

In a written response, Treasury, on behalf of the FSOC Chairperson, acknowledged the findings and conclusions in this report. The response stated that the suggestions made by several FSOC members to further enhance the Council's work will be considered. The response is provided as Appendix III.

CIGFO Working Group Audit

This report presents the results of the CIGFO Working Group's audit of FSOC's monitoring of international financial regulatory proposals and developments. CIGFO is issuing this report to FSOC and Congress as part of CIGFO's responsibility to oversee FSOC under the Dodd-Frank Act. See Appendix II for a listing of previous CIGFO reports.

Background

The Dodd-Frank Act established FSOC 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 protecting financial stability would require the collective engagement of the entire financial regulatory community. As shown in Figure 1, the Council consists of 10 voting members and 5 non-voting members and brings together the expertise of federal financial regulators; state regulators; an insurance expert appointed by the President, by and with the advice and consent of the Senate; and others.[3] The voting members of FSOC provide a federal financial regulatory perspective as well as an independent insurance expert's view. The non-voting members offer different insights as state-level representatives from bank, securities, and insurance regulators or as the directors of offices within Treasury — the Office of Financial Research and the Federal Insurance Office, established in Titles I and V of the Dodd-Frank Act, respectively.

Within Treasury, a dedicated policy office of Treasury staff, led by a Deputy Assistant Secretary, functions as the FSOC Secretariat and assists in coordinating the work of the Council among its members and member agencies.

The statutory purposes of FSOC are to:

- 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;

3 12 U.S.C. 5321(b).

Figure 1: FSOC Council Membership

Federal and Independent Members	State Members
• Secretary of the Treasury, Chairperson (v) • Chairman of the Board of Governors of the Federal Reserve System (v) • Comptroller of the Currency (v) • Director of the Bureau of Consumer Financial Protection (v) • Chairman of the Securities and Exchange Commission (v) • Chairperson of the Federal Deposit Insurance Corporation (v) • Chairman 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 • Independent member with insurance expertise (v) (v) Indicates Voting Member	State Insurance Commissioner State Banking Supervisor State Securities Commissioner

- promote market discipline, by eliminating expectations on the part of shareholders, creditors, and counterparties of such companies that the Government will shield them from losses in the event of failure; and

- respond to emerging threats to the stability of the U.S. financial system.[4]

Each year, FSOC is to issue an annual report to Congress on the activities of the Council, significant financial market and regulatory developments, potential emerging threats, and its recommendations regarding various topics.

Audit Approach

Our audit objective was to assess FSOC's monitoring of international financial regulatory proposals and developments. Our audit scope focused on FSOC's efforts to monitor international activities over a 2-year period, January 2016 through January 2018. To accomplish our objective, participating Offices of Inspector General collected information from FSOC members and/or FSOC member representatives, through interviews or self-reporting guided by a questionnaire developed by the CIGFO Working Group, regarding their perspectives on FSOC's efforts to monitor international financial regulatory proposals

4 12 U.S.C. 5322(a)(1).

and developments. In addition, we interviewed officials of the FSOC Secretariat and reviewed FSOC annual reports and laws applicable to FSOC's authority to monitor international financial regulatory proposals and developments. We conducted our audit fieldwork from February 2018 through June 2018.

FSOC's Activities To Monitor International Financial Regulatory Proposals And Developments

The Dodd-Frank Act provides that FSOC has the duty to monitor international financial regulatory proposals and developments, including insurance and accounting issues, and to advise Congress and make recommendations in such areas that will enhance the integrity, efficiency, competitiveness, and stability of the U.S. financial markets. FSOC's monitoring of international financial regulatory proposals and developments is conducted in the context of FSOC's statutory purposes, which focuses on developments that could pose risks to the stability of the U.S. financial system.

The Dodd-Frank Act does not establish specific guidelines or expectations for how FSOC is to fulfill its duty to monitor international financial regulatory proposals and developments. Accordingly, the CIGFO Working Group developed a methodology for reviewing FSOC's activities in this regard. Through our interviews with the FSOC Secretariat and FSOC members and/or representatives and their responses to the questionnaire developed by the CIGFO Working Group, we learned that FSOC monitors these activities in several ways: (1) periodic discussion of international topics at the FSOC principals'[5] meetings, including presentations by experts from relevant member agencies; (2) information sharing at FSOC committee-level meetings; and (3) the development and publishing of its annual reports, which describe important international proposals and developments, identify potential emerging threats to U.S. financial stability, and may include recommendations related to these issues. In addition, some member agencies have their own international engagement, which can inform their participation in FSOC meetings.

FSOC Principals and FSOC Committee Meetings

FSOC has a statutory duty to facilitate information sharing and coordination among its member agencies and other Federal and State agencies.[6] Through this role, FSOC works to address gaps and weaknesses within the regulatory structure that could pose risks to U.S. financial stability, and to promote a safer and more stable financial system. FSOC exercises its convening authority both through meetings of FSOC members and through its staff-level committee structure. We noted that the principals held 17 meetings during the audit period and international topics were discussed at 10 of those meetings.

5 Principals are FSOC members, most of whom are heads of federal or state financial regulatory agencies.
6 12 U.S.C. 5322(a)(2)(E).

FSOC operates under a committee structure to promote shared responsibility among its members and member agencies and to leverage the expertise that already exists at each agency. These committees consist of senior or staff level representatives from each of the FSOC members. We identified two primary committees that support the Council's monitoring of international activities, FSOC's Regulation and Resolution Committee (RRC) and FSOC's SRC. The RRC is tasked with identifying potential gaps in regulation that could pose risks to U.S. financial stability, and the SRC is tasked with identifying risks and responding to emerging threats to the stability of the U.S. financial system. During the audit period, the RRC held nine meetings to discuss topics that were regulatory in nature. We were told by an FSOC Secretariat official that most of the topics had international aspects. Additionally, the SRC held 10 meetings during the audit period to receive briefings from FSOC member agencies on a range of international topics that had a bearing or potential bearing on financial stability and to discuss the issues raised.

Topics discussed during SRC and RRC meetings included: European political and market developments, the United Kingdom referendum to leave the European Union (known as Brexit), Basel standards, the European banking sector (including Greece), China's economy and potential spillover risks, virtual currency, the London Interbank Offered Rate (LIBOR), central counterparty supervisory stress tests, and qualified financial contracts. We determined that many topics discussed at the committee meetings were raised with the Council and were included, as appropriate, in FSOC's annual report.

Most FSOC members and/or representatives that we interviewed or coordinated with noted that the SRC is FSOC's primary mechanism to monitor international financial regulatory proposals and developments. The SRC serves as a forum for FSOC members and member agencies to identify, discuss, and analyze potential risks to U.S. financial stability, which may extend beyond the jurisdiction of a single agency.

Representatives from one member agency stated that proposals and developments monitored by these committees are shared with the Deputies Committee,[7] sometimes as part of a committee meeting readout, and sometimes as a standalone presentation. Representatives from another member agency stated that when there is an international financial regulatory proposal or development of concern from a financial stability perspective, the Deputies Committee and/or the Council receive briefings from relevant experts from FSOC member agencies to inform them about the topic.

In addition, several FSOC members and/or representatives stated that FSOC focuses more on domestic activities than those of an international nature due to the greater po-

7 The members of the Deputies Committee are senior officials from each of the member agencies. This committee coordinates and oversees the work of the other interagency staff committees.

tential influence of domestic developments on U.S. financial stability. For example, representatives from one member agency stated that FSOC member agencies that are the lead on domestic regulatory proposals and developments with financial stability implications are available to brief FSOC members and/or its committees. Despite the emphasis on domestic developments, briefings on international financial regulatory proposals and developments are provided by FSOC member experts.

Annual Reporting

The Dodd-Frank Act requires FSOC to report to Congress annually about: (1) its activities; (2) significant financial market and regulatory developments; (3) potential emerging threats to the financial stability of the United States; and (4) recommendations to: (i) enhance the integrity, efficiency, competitiveness, and stability of U.S. financial markets; (ii) promote market discipline; and (iii) maintain investor confidence, among other things. Consistent with this charge, we found that FSOC's annual reports described the activities of the Council and its subcommittees, including international financial regulatory proposals and developments. Most of the FSOC members and/or representatives we interviewed or coordinated with, told us that FSOC monitors international financial regulatory proposals and developments through its annual reporting process. Specifically, many FSOC members and/or representatives participate in FSOC's annual report drafting process, which serves as an opportunity for participating members and member agencies to discuss and provide input about international activities.

FSOC has made no recommendations related to international financial regulatory proposals and developments in its annual reports, which FSOC has issued to Congress each year since its inception in 2010. An FSOC Secretariat official told us that should the Council identify a need to make a recommendation related to an international regulatory proposal or development, it would likely accomplish this through its annual report.

Individual Member Agencies' Efforts

Some FSOC member agencies independently monitor international activities within their agencies' purview and hold discussions with foreign counterparts. The knowledge these member agencies gain from these activities can be shared among each other and at FSOC meetings. Examples of agencies' independent activities include: participation in working groups and committees of the Financial Stability Board (FSB) and other international organizations,[8] and information sharing with agencies' international affairs offices. For example, Treasury participates in the FSB. The Securities and Exchange Commission is active in monitoring international activities and regulatory developments through a variety of methods, including participation in international financial regulatory organizations of which it is a member (e.g.,

8 The FSB was established in April 2009 and serves as an international body that monitors and makes recommendations about the global financial system. The U.S. member institutions on the Board are the Board of Governors of the Federal Reserve System, the U.S. Securities and Exchange Commission, and Treasury. Additional background is available online at www.fsb.org.

FSB, International Organization of Securities Commission (IOSCO) and working groups thereof), and direct engagement with foreign counterparts that are market regulators. The Commodity Futures Trading Commission conducts its own monitoring of international financial regulatory proposals through its membership in the IOSCO, the Over-The-Counter Derivatives Regulators Group, and as an invited guest to working groups and committees of the FSB. The Federal Deposit Insurance Corporation participates in international standard-setting bodies and engages in its own discussions with international supervisors and regulators. The Board of Governors of the Federal Reserve System monitors international financial developments consistent with its mandate. For example, the Federal Reserve Board's Division of International Finance conducts research, analyzes policies, and reports in the areas of foreign economic activity, U.S. external trade and capital flows, and developments in international financial markets and institutions. FSOC Secretariat officials told us that FSOC seeks to avoid duplication or overlap with its member agencies' individual efforts in monitoring international developments.

FSOC MEMBERS CONSIDER THE MONITORING PROCESS ADEQUATE

All FSOC members and/or representatives who provided views on this issue described FSOC's monitoring of international financial regulatory proposals and developments as adequate since FSOC's monitoring process accomplishes its intended purpose, which is to keep abreast of international issues that may pose risks to the U.S. financial system and raise awareness of those issues. We note that as a practical matter, FSOC does not have decision making authority over international financial regulatory proposals or developments.

A couple of members suggested that FSOC could enhance its monitoring process by incorporating additional or more focused briefings at its principals and committee meetings. One of these members suggested that FSOC's RRC could receive periodic updates on key international regulatory proposals being considered in various financial sectors while the SRC could receive periodic updates on international market developments. That member also suggested that it would be appropriate for the Nonbank Financial Companies Designations Committee (Nonbank Designations Committee)[9] to receive updates regarding the global systemically important insurers'[10] process and/or activities-based ap-

9 The Nonbank Designations Committee supports FSOC in fulfilling its responsibilities to consider, make, and review determinations that nonbank financial companies shall be supervised by the Board of Governors of the Federal Reserve System and be subject to enhanced prudential standards, pursuant to the Dodd-Frank Act.

10 Insurers identified by the FSB as those whose distress or disorderly failure, because of their size, complexity, and interconnectedness, would cause significant disruption to the global financial system and economic activity.

proach being discussed at the International Association of Insurance Supervisors.[11] In addition, the member stated that it would make sense for the principals to receive briefings regarding the most significant proposals and market developments to the extent that those proposals and developments may impact U.S. financial stability.

Another member suggested that agencies who participate in international regulatory coordination and standard-setting bodies could make a greater effort to regularly present to the SRC, RRC, or other FSOC committees about their coordination efforts with international regulatory authorities, as appropriate. The member suggested FSOC should make a greater effort to cover, in committee meetings, the risks posed to systemically important foreign financial institutions by domestic and international financial regulatory proposals and developments. According to that member, international topics covered by the SRC are generally related to international economic or political developments as opposed to international financial regulatory developments. This member suggested that FSOC could make a greater effort to connect emerging international risks to international financial regulatory proposals intended to mitigate those risks. Additionally, this member stated that greater effort could be made by the SRC to cover international developments and proposals discussed in FSOC's annual report.

Additionally, representatives from one FSOC member agency stated that FSOC does not need to get involved in areas where regulators already exist and should continue monitoring areas such as risks related to LIBOR, European debt, and the Chinese shadow banking system, where there is no lead U.S. financial regulatory agency.

11 Established in 1994, the International Association of Insurance Supervisors is the international standard-setting body responsible for developing principles, standards, and other supporting material for the supervision of the insurance sector and assisting in their implementation.

CONCLUSION

We determined that FSOC has a process for monitoring international financial regulatory proposals and developments. FSOC's monitoring is evidenced by the discussion of international topics at FSOC principals' meetings, information sharing at FSOC committee-level meetings, and the development and publishing of its annual report.

All FSOC members or member representatives who offered an opinion described FSOC's process to monitor international financial regulatory proposals and developments as adequate. Although they described FSOC's monitoring process as adequate, several members and/or representatives offered suggestions for enhancing the process which included, but were not limited to: (1) asking member agencies who participate in international regulatory coordination, as well as standard-setting bodies, to regularly present to FSOC's committees on coordination efforts with international regulatory authorities; (2) making a greater effort to cover the risks posed to systemically important foreign financial institutions by domestic and international financial regulatory proposals and developments; (3) separating the types of periodic updates received by the SRC and RRC—specifically, international market updates versus international financial regulatory proposals, respectively; (4) receiving briefings at principals' meetings regarding the most significant international financial regulatory proposals and market developments to the extent that those activities may impact U.S. financial stability; and (5) continuing FSOC's monitoring efforts in areas where no lead financial regulatory agency exists.

We encourage FSOC to consider incorporating into its process the suggestions made by its members to the extent the suggestions are consistent with FSOC's focus on identifying and addressing threats to the stability of U.S. financial system. We are not making any recommendations to FSOC as a result of our audit.

FSOC Response

In a written response, Treasury, on behalf of the FSOC Chairperson, acknowledged its monitoring of international financial regulatory proposals and developments as outlined in this report. The response stated that the suggestions made by several FSOC members to further enhance the Council's work will be considered.

Appendix I: Objective, Scope, and Methodology

Objective

The audit objective was to assess the Financial Stability Oversight Council's (FSOC) monitoring of international financial regulatory proposals and developments.

Scope and Methodology

The scope of this audit included FSOC's monitoring of international financial regulatory proposals and developments from January 2016 through January 2018.

To accomplish our objective, we:

- reviewed the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) to determine FSOC's statutory purposes and duties;
- interviewed staff from the FSOC Secretariat to determine FSOC's process of monitoring international financial regulatory proposals and developments;
- interviewed or coordinated with FSOC members and member agency representatives to obtain their views and to determine their involvement in FSOC's process of monitoring international financial regulatory proposals and developments;
- reviewed past FSOC and Council of Inspectors General on Financial Oversight annual reports, FSOC's bylaws, FSOC's committee charters for the following committees: Data Committee; Financial Market Utilities and Payment, Clearing and Settlement Activities Committee; Nonbank Financial Companies Designations Committee; Regulation and Resolution Committee; and the Systemic Risk Committee;
- reviewed FSOC's Principals' meeting minutes, and meeting agendas for FSOC's Systemic Risk Committee and Regulation and Resolution Committee (FSOC is not required to prepare meeting minutes for committee meetings;

therefore, we could only review agendas for these groups); and

- created a questionnaire designed to gather specific information regarding each FSOC member and member agency's participation in the monitoring of international financial regulatory proposals and developments as well as their assessment of FSOC's work in this area. This questionnaire was used by each of the Working Group members to facilitate the consistent collection of information from all interviewees. Several members self-reported their responses to the questionnaire.

We performed fieldwork from February through June 2018. We conducted this 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Prior CIGFO Reports

The Council of Inspectors General on Financial Oversight (CIGFO) has issued the following prior reports:

- Audit of the Financial Stability Oversight Council's Controls over Non-public Information, June 2012
- Audit of the Financial Stability Oversight Council's Designation of Financial Market Utilities, July 2013
- Audit of the Financial Stability Oversight Council's Compliance with Its Transparency Policy, July 2014
- Audit of the Financial Stability Oversight Council's Monitoring of Interest Rate Risk to the Financial System, July 2015
- Audit of the Financial Stability Oversight Council's Efforts to Promote Market Discipline, February 2017
- CIGFO's Corrective Verification Action on the Audit of the Financial Stability Oversight Council's Designation of Financial Market Utilities, May 2017
- Top Management and Performance Challenges Facing Financial Regulatory Organizations, September 2018

Appendix III: FSOC Response

December 19, 2018

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

Re: Response to Draft Audit Report: CIGFO's Audit of the Financial Stability Oversight Council's Monitoring of International Financial Regulatory Proposals and Developments

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 Monitoring of International Financial Regulatory Proposals and Developments (the Draft Report). The Financial Stability Oversight Council (FSOC) appreciates the CIGFO working group's review of the FSOC's efforts to monitor international issues consistent with its statutory duties. This letter responds on behalf of Secretary Mnuchin, as Chairperson of FSOC, to the Draft Report.

As the Draft Report notes, FSOC monitors international financial regulatory proposals and developments in several ways, including through the development of its annual reports; discussions at Council and staff-level committee meetings and other staff-level discussions; and through the direct international engagement of its member agencies that inform their participation on FSOC. The report noted that FSOC members and their staffs expressed their overall satisfaction with FSOC's monitoring in this area and believe the process is adequate. CIGFO made no recommendations as a result of the working group review. The Draft Report notes that several FSOC members offered suggestions to further enhance FSOC's work, which we will consider in the future.

Thank you again for the opportunity to review and comment on the Draft Report. We value CIGFO's input and look forward to continuing our constructive engagement with you.

Sincerely,

/s/

Bimal Patel
Deputy Assistant Secretary for the Financial
Stability Oversight Council

Appendix IV: CIGFO Working Group

Department of the Treasury Office of Inspector General, Lead Agency		
Eric M. Thorson, Inspector General, Department of the Treasury, and CIGFO Chair		
Deborah Harker	Lisa Carter	Jeffrey Dye
Vicki Preston	Virginia Shirley	Clyburn Perry III
Board of Governors of the Federal Reserve System and the Bureau of Consumer Financial Protection Office of Inspector General		
Mark Bialek, Inspector General, Board of Governors of the Federal Reserve System and Bureau of Consumer Financial Protection		
Chie Hogenmiller	Melissa Chammas	
Commodity Futures Trading Commission Office of Inspector General		
A. Roy Lavik, Inspector General, Commodity Futures Trading Commission		
Miguel Castillo	Branco Garcia	
Federal Deposit Insurance Corporation Office of Inspector General		
Jay N. Lerner, Inspector General, Federal Deposit Insurance Corporation		
Robert Fry		
Federal Housing Finance Agency Office of Inspector General		
Laura Wertheimer, Inspector General, Federal Housing Finance Agency		
Marla Freedman	Bob Taylor	Jim Lisle
April Ellison		
Securities and Exchange Commission Office of Inspector General		
Carl W. Hoecker, Inspector General, Securities and Exchange Commission		
Rebecca L. Sharek	Carrie Fleming	