JULY 2021

Annual Report of the Council of Inspectors General on Financial Oversight

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

Message from the Chair

As the country continues to recover from the novel Coronavirus Disease 2019 (COVID-19) pandemic, we are mindful of the unprecedented level of financial assistance and stimulus programs that continue to provide much needed relief to individuals, families, and businesses affected by the pandemic. In keeping with its mission, the Council of Inspectors General on Financial Oversight (CIGFO), which is authorized to oversee Financial Stability Oversight Council (FSOC) operations, continues to monitor the ongoing response of FSOC and its member agencies related to the public health and financial crisis. As warranted, this oversight will include reviews by the Inspectors General individually, or collectively as CIGFO, of FSOC and member Federal agencies' preparedness for events that cause significant stress to the U.S. financial system like the COVID-19 pandemic as well as their agencies' response to the current crisis.

During the pandemic and resultant financial crisis the Nation experienced the transition to a new President and Administration, which brought significant change in personnel and the rise of new initiatives. Both CIGFO member Inspectors General and CIGFO, as a collective body, perform a valuable role during Presidential transitions. Based on its experience and unique perspective, CIGFO is a valuable source of information about the key financial oversight issues that will confront the new Administration. In December 2020, CIGFO released a Presidential Transition Handbook as a guide on CIGFO's roles and authorities as well as transition issues and interactions. This handbook is provided as Appendix A.

To accomplish CIGFO's oversight and monitoring activities, 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. In September 2020, CIGFO approved a working group proposal to compile forward-looking guidance for FSOC and its members to consider in preparing for a crisis. This project is expected to be completed in the summer of 2021.

CIGFO's monitoring activities also include sharing financial regulatory information which enhance Inspectors General knowledge and insight about specific issues related to members' current and future work. For example, during its quarterly meetings, CIGFO members discussed oversight efforts related to programs established under the various COVID-19 relief packages; member activities under other pandemic response oversight bodies; as well as 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
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:

- Small Business Administration Office of Inspector General – overview of oversight of the Paycheck Protection Program
- FSOC – overview of Council activities and impact of the Coronavirus Disease 2019 (COVID-19) pandemic such as an increased monitoring of market issues and frequency of committee meetings
- FSOC's data call to assess designation of Financial Market Utilities
- Office of the Comptroller of the Currency's "fair access" regulations
- CIGFO member efforts on the Pandemic Response Accountability Committee (PRAC) Working Groups
- Components of various legislation introduced in Congress related to COVID-19, coronavirus relief, and economic stimulus packages
- The *National Defense Authorization Act for Fiscal Year 2021*, which amended requirements for anti-money laundering reporting and additional whistleblower provisions
- Executive Order No. 14018, *Revocation of Certain Presidential Actions*

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*
- *2019 - Top Management and Performance Challenges Facing Financial-Sector Regulatory Organizations*
- *2020 - Survey of FSOC and its Federal Member Agencies' Efforts to Implement the Cybersecurity Act of 2015*
- *2020 - Council of Inspectors General on Financial Oversight Presidential Transition Handbook*

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
Bureau of Consumer Financial Protection

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

We provide 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) and demonstrate leadership by making recommendations to improve economy, efficiency, and effectiveness, and by preventing and detecting fraud, waste, and abuse.

I. Background

Congress established our office 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), we conduct 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 our office. Section 38(k) of the Federal Deposit Insurance Act (FDI Act) requires us to 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 us 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 us 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.

II. 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 four major management challenges for the Board that apply to the financial sector in 2020:

- Designing and Operationalizing Emergency Lending Programs to Address the Economic Effects of the COVID-19 Pandemic
- Enhancing Organizational Governance and Risk Management
- Enhancing Oversight of Cybersecurity at Supervised Financial Institutions
- Remaining Adaptable to External Developments While Supervising Financial Institutions

Among other items, we identified two major management challenges for the Bureau that apply to the financial sector in 2020:

- Remaining Adaptable to External Developments While Continuing to Refine the Supervision and Enforcement Strategy
- Managing Consumer Complaints

The Board Economics Divisions Can Enhance Some of Their Planning Processes for Economic Analysis, OIG Report 2021-MO-B-001, February 24, 2021

The Board's four economics divisions—the Divisions of Research and Statistics, Monetary Affairs, International Finance, and Financial Stability—produce analysis and research to support the Board's mission. The economics divisions use a variety of processes and supporting practices to plan such analysis. We assessed the economics divisions' processes to plan certain research activities and identified opportunities to enhance the effectiveness of those processes.

We found that the economics divisions can enhance some of their planning processes for their economic analysis activities by considering additional practices to improve transparency, communication, and monitoring. In addition, the economics divisions' continuous improvement efforts can benefit from a more structured approach to sharing processes and supporting practices with each other.

We made recommendations designed to improve some of the economics divisions' planning processes. The Board concurred with our recommendations.

The Board's Approach to the Cybersecurity Supervision of LISCC Firms Continues to Evolve and Can Be Enhanced, OIG Report 2020-SR-B-019, September 30, 2020

Cybersecurity threats to financial institutions are becoming more frequent and sophisticated. We assessed the effectiveness of the Board's cybersecurity supervision approach for Large Institution Supervision Coordinating Committee (LISCC) firms—the largest, most systemically important domestic and foreign financial institutions supervised by the Board.

The Board's approach to cybersecurity supervision of LISCC firms continues to evolve and can be enhanced. The Board can strengthen its governance of LISCC firm cybersecurity supervision by clarifying the roles and responsibilities of the groups involved in supervision and planning activities and better defining how cybersecurity supervisory activities inform relevant ratings. The Board can also enhance its approach to cybersecurity training to ensure examiners keep their skills up to date. Additionally, the Board can improve its guidance and training for reporting cybersecurity events.

Our report contains recommendations designed to enhance the effectiveness of the Board's cybersecurity supervision of LISCC firms. The Board concurred with our recommendations.

The Bureau Can Improve Its Periodic Monitoring Program to Better Target Risk and Enhance Training for Examiners, OIG Report 2020-SR-C-015, June 24, 2020

The Bureau's Division of Supervision, Enforcement and Fair Lending (SEFL) monitors supervised institutions to maintain reasonably current information on their activities and to assess whether changes in risks to consumers or markets warrant changes in SEFL's planned supervisory activities. We evaluated SEFL's approach to monitoring supervised institutions for consistency with the Bureau's strategic plan and internal policies and procedures.

In July 2019, SEFL completed an internal initiative that included an assessment of its periodic monitoring program. Both SEFL's internal initiative and our independent assessment found that the agency can improve its supervisory monitoring program. Specifically, SEFL can expand the number of nondepository institutions it monitors, better tailor the resources dedicated to monitoring based on risk, and hire additional examiners to augment monitoring and the supervision program more broadly. Additionally, we determined that examiners did not consistently conduct or document periodic monitoring activities in accordance with SEFL's guidance. We also found that examiners may lack clarity on how periodic monitoring activities factor into SEFL's prioritization process and its broader supervision program. In January 2020, during the drafting of our report, SEFL finalized updates to its periodic monitoring policy, which include expanding its monitoring program to cover additional nondepository institutions. We also understand that in 2020, SEFL began to hire additional examiners, in part to support its monitoring efforts.

Our report contains recommendations designed to further enhance the Bureau's periodic monitoring program. The Bureau concurred with our recommendations.

Ongoing Work

Monitoring of the Federal Reserve's Lending Programs

In response to the economic effects of the COVID-19 pandemic, the Federal Reserve announced that it would create new lending programs to provide loans to employers, certain businesses, and communities across the country to support the U.S. economy. Specifically, the following programs have been created: the Main Street Lending Program, the Paycheck Protection Program Liquidity Facility, the Municipal Liquidity Facility, the Primary Market Corporate Credit Facility, and the Secondary Market Corporate Credit Facility. We initiated an active monitoring effort of these programs to gain an understanding of the operational, governance, reputational, and financial matters associated

with them. Through this monitoring effort, we will refine our focus on the programs and identify areas for future audits or evaluations. Some of the topics we are considering include the design, operation, governance, and oversight of the lending programs; data collection and reporting associated with the programs; and the effect of the programs on the Board's supervision and regulation activities.

Evaluation of the Board's Implementation of Enterprise Risk Management (ERM)

ERM is an approach to addressing the full spectrum of an organization's significant risks by considering them as an interrelated portfolio. Federal guidance highlights the importance of implementing an ERM capability that is coordinated with strategic planning and internal control processes. We are performing an evaluation of the Board's implementation of ERM. Our objective is to assess the effectiveness of the Board's ongoing efforts to plan, develop, and integrate ERM processes across the agency. Our scope focuses on (1) the establishment of supporting ERM governance and operational structures and (2) steps taken to cultivate a risk culture that aligns the risk management program with the Board's mission, vision, strategy, and values.

Evaluation of the Efficiency and Effectiveness of the Board's Consumer Compliance Examination and Enforcement Action Processes

The mission of the Board's Division of Consumer and Community Affairs (DCCA) is to promote a fair and transparent financial services marketplace and effective community development. DCCA supervises for compliance with and enforces consumer protection laws and regulations that govern how financial institutions interact with their customers and their communities. Supervision activities may include examinations assessing institutions' compliance with the following: the prohibition against unfair or deceptive acts or practices, fair lending laws and regulations, or other consumer protection laws and regulations. The Federal Reserve may also issue enforcement actions for violations of consumer protection laws or regulations. We are evaluating the efficiency and effectiveness of the Board's and the Reserve Banks' consumer compliance examination and enforcement action processes.

Audit of the Board's Data Aggregation, Validation, and Reporting Processes for Its CARES Act Lending Programs

Section 4026 of the CARES Act and section 13(3) of the Federal Reserve Act require the Board to report certain information regarding its emergency lending programs. The Board has stated its commitment to transparency and accountability by announcing that it will report, on a monthly basis, information on the lending programs using CARES Act funding, including the names and details of the participants in each program; the amounts borrowed and the interest rate charged; and overall costs, revenues, and fees for each program. The Board also reports aggregate information on its weekly comprehensive balance sheet, which is publicly available. We are assessing the Board's processes for aggregating and reporting lending information related to its CARES Act programs, including the data validation processes it uses to ensure that the information is current, accurate, and complete.

Evaluation of the Board's Processes for Reviewing and Approving Supervisory Proposals

The Board plays a significant role in supervising and regulating U.S. financial institutions. Through its oversight, the Board seeks to ensure that the institutions it supervises operate in a safe and sound manner and comply with applicable federal laws and regulations. Key aspects of the Board Division of Supervision and Regulation's mission include developing and implementing effective supervisory policy and guidance for supervised financial institutions. Board governors may be involved in reviewing and approving supervisory proposals addressing various matters, such as certain supervisory policy and guidance and aspects of the supervisory stress testing program. We plan to assess the effectiveness of the Board's processes for reviewing and approving supervisory proposals. We intend to focus on the Board's practices for determining which supervisory proposals and activities warrant consultation and approval by the governors. Our scope may include proposals related to supervisory policy and guidance as well as the supervisory stress testing program.

Evaluation of the Bureau's Approach to Assessing Independence and Mitigating the Risk of Conflicts of Interest

SEFL is responsible for ensuring compliance with federal consumer financial laws by supervising market participants and bringing enforcement actions where appropriate. To fulfill this responsibility, it is important to ensure that SEFL staff are independent and objective in executing their oversight activities. We plan to assess the extent to which the Bureau promotes a focus on independence and has policies, procedures, and controls to mitigate the risk of conflicts of interest among SEFL staff.

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 (vacant), two Attorney-Advisor, two Auditors, and one Senior Program Analyst. 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 to improve Information Technology Management and Security.

CFTC's Policies and Procedures Regarding Oversight of Cybersecurity Safeguards by Registered Entities
(September 8, 2020)

The OIG Office of Audits last evaluated the Commission's policies and procedures for reviewing registrants' cybersecurity policies in 2016.[2] At that time, the CFTC Rules on System Safeguards Testing Requirements were not final. While the rule became effective on September 19, 2016, the compliance dates were section specific with the last compliance date being September 19, 2017.[3] We contracted an independent public accountant (IPA) to conduct a performance audit of CFTC policies and procedures for conducting cybersecurity safeguard oversight of certain registered entities. This audit was conducted in accordance with Government Auditing Standards (2018 revision), also known as the "Yellow Book."

We concluded that two CFTC oversight divisions – Division of Clearing and Risk, and Division of Market Oversight – have developed sufficient and adequate policies and procedures to address proper cybersecurity safeguards at certain CFTC registered entities. While we recognized the adequacy of policies and procedures, the following recommendations we made:

- Increase the number of dedicated employees to the divisions' System Safeguard Examination (SSE) teams, in order to continuously assess cybersecurity risks at CFTC registrants.
- Conduct more thorough and in-depth testing of registrants in order to validate that their cybersecurity policies and procedures are being adhered to.
- Implement better data tracking and data analytics tools in order to use available registrant's incident data to analyze and predict trends of potential cybersecurity threats, and to keep track of registrant communication with CFTC personnel.
- Emphasize to CFTC registrants' usage of information sharing facilities so as to promote rapid awareness of emerging cyber threats.

Management agreed with the four recommendations; their planned actions were deemed responsive.

2 CFTC OIG, *Audit of Commodity Futures Trading Commission's Policies and Procedures For Reviewing Registrants' Cybersecurity,* October 11, 2016 (available here: https://www.cftc.gov/idc/groups/public/@aboutcftc/documents/file/oig_rrcp2016.pdf).

3 CFTC, *System Safeguards Testing Requirements; Final Rule,* September 19, 2016 (available here: http://www.cftc.gov/ucm/groups/public/@lrfederalregister/documents/file/2016-22174a.pdf).

FY 2020 FISMA Audit: Order Book On-Demand System Penetration Testing Results (February 26, 2021)

Annually the OIG reviews the Commodity Futures Trading Commission's information security program and practices as required by the Federal Information Security Modernization Act of 2014.[4] For FY 2020, this year's scope included a concentrated assessment of order book on-demand (OBOD) system security controls hosted on a public cloud. OBOD includes three Chicago Mercantile Exchange Group data sets—the Trade Capture Report (TCR), Order Entry, and Market by Order.[5] The OIG Office of Audits contracted information security professionals to assist in the technical control review. In its review, the security experts observed that the eleven controls under evaluation were effective and operating as designed with no exceptions. While the testing team noted a positive assessment conclusion, they conveyed one Process Improvement Opportunity.

In addition, the OIG Office of Audits contracted independent information security professionals to evaluate backup and recovery IT controls for CFTC Eastern Regional Office file servers. Overall, the backup and recovery IT controls were considered effective, with low and medium risks identified. We made three recommendations with which management concurred and are taking corrective action. These reports were not published on our webpage due to information technology sensitivity concerns.

4 P.L. 113-283, 128 Stat. 3073 (2014).
5 Information on OBOD may be found here: https://www.cftc.gov/media/3996/piaOBOD061120/download.

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 $9.5 trillion in deposits at about 5,000 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 3,200 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. We pursued audits and evaluations throughout the year in carrying out this mission. Importantly, and in connection with matters affecting the financial sector, in February 2021, 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 the Department of Justice and our IG counterparts and others on issues of mutual interest, most recently on matters relating to the Coronavirus pandemic, especially through our involvement as a member of the Pandemic Response Accountability Committee.

The FDIC OIG also played a key role as Co-Lead of the CIGFO Working Group that developed forward-looking guidance for the Financial Stability Oversight Council and its member agencies to consider in preparing for and managing future crises. *(Guidance in Preparing for and Managing Crises)*

Top Management and Performance Challenges Facing the Federal Deposit Insurance Corporation

We issued our report identifying the Top Management and Performance Challenges facing the FDIC. We did so pursuant to the Reports Consolidation Act of 2000 and Office of Management and Budget Circular A-136 (revised August 27, 2020). The purpose of our report was to summarize the most serious challenges facing the Agency and to briefly assess the FDIC's progress to address them. Our assessment of the challenges also helps guide the focus of our independent oversight work at the FDIC.

The Top Challenges document is based on the OIG's experience and observations from our oversight work, reports by other oversight bodies, review of academic and relevant literature, perspectives from Government agencies and officials, and information from private-sector entities. This year, we identified the following 10 Top Challenges facing the FDIC:

- **Ensuring Readiness in a Pandemic Environment:** The FDIC should continue to stand ready to fulfill its mission to maintain financial stability in the banking system, and to identify and mitigate risks through examinations. The FDIC should also prepare for bank failures in the event that losses overwhelm banks. Further, the FDIC should review banks' adherence to Government-guaranteed loan program requirements (such as the Paycheck Protection Program or PPP) and identify risks that may affect the safety and soundness of a financial institution.

- **Mitigating Cybersecurity Risks in the Banking Sector:** In recent months, cyberattacks against banks have increased with growing frequency and severity, and may intensify during the pandemic. The FDIC should ensure that it has Information Technology (IT) examination processes and staff with the requisite skills to identify and mitigate cybersecurity risks at banks, including those associated with third-party service providers.

- **Improving IT Security Within the FDIC:** Federal agencies face a growing risk of cybersecurity incidents. The rapid transition to remote work in response to pandemic protocols amplifies the Government's reliance on IT systems and accelerates implementation of technologies. The FDIC must have robust controls to secure its systems and ensure the protection of its information and data.

- **Securing FDIC Personnel, Facilities, and Information:** The FDIC is responsible for protecting a workforce of approximately 5,800 employees and 1,600 contract personnel who work at 94 FDIC facilities throughout the country. The FDIC should continue to strengthen its programs to ensure that its facilities are secure, that staff meet suitability requirements, and that the FDIC work environment is safe and free from discrimination and harassment. The FDIC should also maintain the security of its IT systems and hard-copy records containing sensitive information about banks and personally identifiable information (PII) of employees, contractors, bank management, and bank deposit holders.

- **Ensuring and Aligning Strong Governance at the FDIC:** Effective governance is critical to ensure that the FDIC assesses risks and consistently implements its policies. The FDIC should ensure the establishment and proper function of its governance processes, including an Enterprise Risk Management program. Quality data is also a critical component of FDIC governance to allow the Board, Executives, and Managers to assess the effectiveness of FDIC programs.

- **Augmenting the FDIC's Sharing of Threat Information:** Sharing threat information is critical to ensuring that banks and examiners have the necessary information to protect financial institutions, the banking sector, and the economy. Timely and actionable threat information allows bank management to mitigate risks and thwart dangers, and prompts the FDIC to adjust supervisory strategies in a timely fashion. Without effective threat information sharing, policy makers, bank examiners, and bank management may be unaware of threats that could affect the integrity, safety, and soundness of financial institutions.

- **Supporting Diversity in Banking:** Minority communities and businesses have suffered significantly during the pandemic. The FDIC plays an important role to support Minority Depository Institutions that serve and promote minority and low- and moderate-income communities. This work can be enhanced with the FDIC's continued commitment to diversity and inclusion in the Federal regulatory process, which is critical for the FDIC to foster greater financial inclusion for all Americans.

- **Managing Human Resources and Planning for the Future Workforce:** Forty-two percent of FDIC employees (nearly 2,400 individuals) are eligible to retire within 5 years. The FDIC faces retirement rates of almost 60 percent among FDIC Executives and Managers over that same time period. The FDIC should continue to manage the Agency's exposure to gaps in leadership and mission-critical skills, especially given the significant investments in, and time required for, bank examiner commissioning.

- **Overseeing Contracts and Managing Supply Chain Risk:** The FDIC's contracting budget for 2021 is approximately $549 million, including an increase from 2020 of more than $166 million (43 percent) for contractor-provided services. The FDIC should execute a contracting program that ensures effective oversight of its acquisition of goods and services. In addition, the FDIC should ensure that it adequately manages and mitigates supply chain risks associated with such contracts.

- **Enhancing Rulemaking at the FDIC:** The FDIC should have a transparent rulemaking process that balances the need for regulation and the burden on financial institutions' compliance. A foundational component of rulemaking is reliable information to measure a regulation's costs and benefits.

We believe that the researched and deliberative analysis in our Top Management and Performance Challenges document will be beneficial and constructive for policy makers, including the FDIC and Congressional oversight bodies. We further hope that it is informative for the American people regarding the programs and operations at the FDIC and the Challenges it faces.

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

During the 12-month period ending March 31, 2021, the FDIC OIG issued 16 audit, evaluation, and other products and made 100 recommendations to strengthen controls in FDIC programs and operations. Our work covered diverse topics such as crisis readiness, enterprise risk management, information security and cyber threats, personnel security and suitability, and bank failures, among others. Results of several of these reviews as they relate to the broader financial sector are presented below.

The FDIC's Readiness for Crises

We evaluated the FDIC's Readiness for Crises. We initiated this evaluation in 2018, and it covered the FDIC's readiness planning and preparedness activities up to early 2019. Our work was not conducted in response to the current pandemic situation, nor is the report specific to any particular type of crisis.

The FDIC's mission is to maintain stability and public confidence in the Nation's banking system by insuring deposits, examining and supervising financial institutions for safety and soundness and consumer protection, making large and complex financial institutions resolvable, and managing receiverships. To achieve its mission, the FDIC must be prepared for a broad range of crises that could impact the banking system.

The OIG identified best practices that could be used by the FDIC. Our review of these best practices identified seven important elements of a crisis readiness framework that are relevant to the FDIC – (i) Policy and Procedures; (ii) Plans; (iii) Training; (iv) Exercises; (v) Lessons Learned; (vi) Maintenance; and (vii) Assessment and Reporting.

We found that the FDIC should fully establish these seven elements of a readiness framework to address crises that could impact insured depository institutions. In summary, we found that the FDIC:

- Did not have a documented Agency policy and did not have documented procedures to provide for a consistent crisis readiness planning process;
- Should develop an Agency-wide all-hazards readiness plan as well as Agency-wide hazard-specific readiness plans, as needed;
- Did not train personnel to understand the content of crisis readiness plans;
- Should document the important results of all readiness plan exercises;
- Did not have a documented process to monitor implementation of lessons learned;
- Should establish a central repository of plans to facilitate periodic maintenance; and
- Should regularly assess and report on Agency-wide progress on crisis readiness plans and activities to the FDIC Chairman and senior management.

We made 11 recommendations to improve the FDIC's crisis readiness planning. Management concurred with seven recommendations and partially concurred with four recommendations.

The FDIC's Implementation of Enterprise Risk Management

ERM is an agency-wide approach to addressing the full spectrum of internal and external risks facing an agency. The FDIC Board of Directors (Board) designated the FDIC Operating Committee (OC) as the "focal point" for the coordination of risk management at the FDIC. The FDIC further designated the OC as the FDIC's Risk Management Council (RMC) and the oversight body for ERM.

We found that the FDIC needed to establish a clear governance structure, and clearly define authorities, roles, and responsibilities related to ERM. Importantly, the FDIC did not clearly articulate in its policies and procedures how the OC, as the FDIC's designated RMC, performed its responsibilities. In particular, we noted that the FDIC should define the OC's role with respect to its oversight of the establishment of the FDIC's Risk Profile; oversight of the assessment of risks; oversight of the development of risk responses; and the final determinations of the approaches and actions to address the risks included in the FDIC's Risk Profile.

We also found that the FDIC had not clearly defined the roles, responsibilities, and processes of other committees and groups involved in ERM. The FDIC did not:

- Ensure that the Board endorsed the Risk Appetite statement prior to its issuance;
- Ensure effective communications to the Board relating to ERM;
- Ensure that the Board understood its role with respect to ERM at the FDIC;
- Develop procedures to specify how risk committee activities were to be accomplished and how they interfaced with other ERM processes;
- Require documentation of meetings of the various risk committees; and
- Update and memorialize ERM processes for the Risk Management and Internal Controls Branch.

Without a clear governance structure over ERM, the FDIC cannot ensure that ERM will fully mature and be integrated into the Agency and its culture. Integrating ERM leads to improved decision-making and enhanced performance.

We made eight recommendations to strengthen the FDIC's implementation of ERM. Management concurred with five recommendations and non-concurred with the remaining three recommendations.

The FDIC's Information Security Program–2020

We issued our audit of the *FDIC's Information Security Program—2020*, in accordance with the Federal Information Security Modernization Act of 2014 (FISMA). We engaged a contractor firm to conduct this audit. The audit determined that the FDIC's overall information security program was operating at a Maturity Level 3 (Consistently Implemented) on a scale of 1-5. Programs operating below a Maturity Level 4 are not considered effective.

The FISMA report describes security control weaknesses that 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. Our findings fell into the following categories:

Risk Management. The FDIC had not fully defined its Enterprise Risk Management governance, roles, and responsibilities. In addition, the FDIC had not yet implemented recommendations to integrate privacy into its Risk Management Framework, nor did the FDIC always address Plans of Action and Milestones in a timely manner.

Risk Acceptance Decisions Not Consistently Reassessed. The FDIC did not consistently review its existing Acceptance of Risk documents after they were initially established, nor did it submit those documents for re-approval. Therefore, it could not effectively assess the level of risk it was incurring relative to established Risk Tolerance levels.

Unauthorized Software on the Network. In May 2020, the FDIC discovered an unauthorized commercial software application installed on 32 desktop workstations, and the application had not been approved by the FDIC's IT governance bodies or subject to established configuration management processes. Notably, the FDIC's Office of the Chief Information Security Officer had previously raised security concerns about this same software. The FDIC subsequently removed the unauthorized software from the workstations.

Privacy Control Weaknesses Not Fully Addressed. The FDIC had not completed actions to address previously-identified privacy control weaknesses, such as integration of privacy considerations into its Risk Management Framework; implementation of its planned Document Labeling initiative; establishment of controls to effectively secure PII stored in network shared drives; and disposal of PII within established timeframes.

Oversight and Monitoring of Outsourced Systems Not Adequate. In June 2020, the FDIC rescinded its *Outsourced Solution Assessment Methodology* used to assess security and privacy risks associated with outsourced information systems because it did not align with National Institute of Standards and Technology guidance. As a result, the FDIC had not properly categorized some of its systems covered by the assessment methodology or subjected these systems to a proper risk assessment, authorization to operate, and ongoing monitoring.

Cloud-based Systems Not Subject to Annual Control Assessments. As of April 2020, the FDIC had 14 cloudbased systems that provided critical IT services. The FDIC did not subject these cloud-based systems to required annual control assessments.

We made eight recommendations for the FDIC to reassess its risk acceptance decisions in accordance with policy; implement control improvements to prevent the unauthorized installation of software on the network; and complete actions to address open Plans of Action and Milestones related to baseline configurations. We also recommended that the FDIC assess and improve controls for managing administrative accounts; implement a process to ensure all outsourced information systems are subject to the Risk Management Framework; and ensure all cloud-based systems are subject to annual security and privacy control assessments. Finally, we recommended that the FDIC update its IT contingency planning policy and incorporate additional scenarios into its IT contingency plan testing. FDIC Management concurred with the eight recommendations in the report.

The FDIC's Personnel Security and Suitability Program

The effectiveness of the FDIC's Personnel Security and Suitability Program (PSSP) is critically important to ensure that FDIC employees and contractor personnel are properly screened and investigated prior to being granted access to systems and entrusted with sensitive, confidential, or, in some cases, classified information. We conducted an evaluation of the FDIC's PSSP to assess the effectiveness of the program.

Before individuals can be hired by the FDIC, they must meet minimum standards for employment with the FDIC. Contractor personnel must meet minimum standards of integrity and fitness. Determining whether an individual meets the FDIC's minimum employment or integrity and fitness standards is accomplished by way of a preliminary background investigation (PBI). Federal regulations also require that a background investigation (BI) be conducted on each Federal employee and contractor.

We found that the FDIC's PSSP was not fully effective in ensuring that: (1) PBIs were completed in a timely manner; (2) BIs were ordered and adjudicated commensurate with position risk designations; and (3) re-investigations were ordered within required timeframes. Specifically, after analyzing PSSP-related data for all employees and contractor personnel with access to the FDIC's IT systems as of December 2, 2019, we determined that:

- The FDIC did not remove multiple contractors with unfavorable background investigation adjudications in a timely manner;
- The FDIC did not follow its Insider Threat protocols and conducted limited risk assessments for the contractors with unfavorable adjudications;
- The FDIC did not initiate and order numerous required periodic reinvestigations in a timely manner;
- Data on contractor position risks were unreliable;
- Employee background investigations were sometimes not commensurate with position risk;
- Some of the FDIC files were missing certain PBI data; and
- The FDIC was not meeting its goals for completing PBIs within a specified timeframe.

Importantly, the results of our evaluation led us to conclude that the risks within the FDIC's PSSP were not fully reflected in the FDIC's Risk Inventory as a component of its Enterprise Risk Management program. This risk analysis was particularly important as the FDIC was beginning contingency planning for surge staffing in the event that the current pandemic negatively impacted the banking sector. We noted that the FDIC's Operating Committee, as the Risk Management Council, needed to ensure that the Division of Administration was satisfactorily addressing the risks associated with the PSSP.

We made 21 recommendations aimed at strengthening the PSSP's controls and ensuring that the FDIC is in full compliance with Federal requirements. The FDIC concurred with all 21 recommendations.

Reports of Failed Banks

One of the most important statutory responsibilities of our Office under the Federal Deposit Insurance (FDI) Act is to conduct material loss reviews of failed FDIC-supervised institutions when those failures cause a significant loss to the Deposit Insurance Fund (DIF), that is, a loss exceeding $50 million. When the DIF incurs a loss under $50 million, the FDI Act requires the Inspector General of the appropriate federal banking agency to determine the grounds upon which the state or federal banking agency appointed the FDIC as receiver and whether any unusual circumstances existed that might warrant an In-Depth Review (IDR) of the loss. In one case, that of Enloe State Bank, Cooper, Texas, although the failure did not meet the materiality threshold, we determined that an IDR was warranted. With respect

to five other failed institutions whose losses totaled less than $50 million, we determined that no further review was warranted.

In-Depth Review of the Failure of Enloe State Bank, Cooper, Texas

On May 31, 2019, the Texas Department of Banking (TDB) closed Enloe State Bank (ESB), and the FDIC was appointed as receiver for the Bank. As of July 31, 2020, the estimated loss to the DIF resulting from ESB's failure was approximately $21 million. Our review analyzed the causes of the Bank's failure and evaluated the FDIC's supervision of the Bank.

Causes of Failure: Enloe State Bank failed because the President and the senior-level Vice President perpetrated fraud by originating and concealing a large number of fraudulent loans over many years. ESB's President was a dominant official with significant control over Bank operations and limited oversight by the Bank's Board of Directors. The Bank President used her role as primary lender, with inadequately controlled systems access, to originate millions of dollars in fraudulent loans. She hid these loans from the Board and regulators with assistance from others. The losses on the fraudulent loans severely diminished the Bank's earnings and depleted capital to the point from which the Bank could not recover.

The FDIC's Supervision of ESB: The FDIC and the TDB provided ESB with supervisory recommendations and actions that addressed issues related to the eventual causes of the Bank's failure. However, these recommendations and actions did not persuade the Bank's Board and management to effectively resolve the identified weaknesses. We found that the FDIC did not:

- Identify the existence and impact of a dominant official in a timely manner;
- Consistently identify and follow up on weaknesses in the Bank's audit program;
- Conduct additional testing to address unusual loan-related activity, which may have helped identify the fraudulent activity sooner than 2019; and
- Perform additional procedures to determine the likelihood of fraud once the examination in 2018 identified a dominant official, unsatisfactory Board oversight, and inadequate internal controls and audits.

In the case of ESB, examiners did not identify that fraud might be occurring at the institution until 2019, which was too late to save the Bank.

We made eight recommendations for the FDIC to improve examiner guidance and training in such areas as identifying dominant officials; understanding the independence and qualifications of internal auditors; recognizing the importance of adequate external financial audit coverage; monitoring and following up on State-issued Matters Requiring Board Attention; ensuring that system user access controls are adequately tested; conducting additional procedures related to loan activity and the likelihood of fraud; and considering issues holistically to facilitate fraud detection.

The FDIC concurred with three recommendations in our report and stated that it "partially agreed" with five recommendations.

Other Failed Bank Reviews: We conducted failed bank reviews of the following five institutions, and corresponding reports are posted on our website:

- Louisa Community Bank, Louisa, Kentucky
- Ericson State Bank, Ericson, Nebraska

- First State Bank, Barboursville, West Virginia
- First City Bank of Florida, Fort Walton Beach, Florida
- Almena State Bank, Almena, Kansas

As noted earlier, for each of the above, we determined that proceeding with an IDR was not warranted, because we did not identify unusual circumstances in connection with the institution's failure.

FDIC OIG Investigations Seek to Ensure Integrity in the Banking Sector and Address Fraud in the Federal Pandemic Response

OIG investigations continue to complement our audit and evaluation work. Our investigative results over the 12 months ending March 31, 2021, included the following: 159 indictments; 78 arrests; 64 convictions; and potential monetary recoveries (fines, restitution, and asset forfeitures) of $71.7 million.

Our 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.

As illustrated in the case examples that follow, the FDIC OIG's Office of Investigations 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 continue to further develop our cyber capabilities to investigate computer crimes at banks. We also partner with other agencies, including the Small Business Administration (SBA), 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. In this regard, and as further discussed below, we continue to investigate numerous Paycheck Protection Program (PPP) cases of individuals defrauding the Government guaranteed-loan program intended to help those most in need during the pandemic crisis. Examples of our investigative work follow.

Bank President Sentenced for Arson and Fraud Scheme

On February 23, Anita Gail Moody, of Cooper, Texas, was sentenced to 96 months in federal prison, after pleading guilty in June 2020 to conspiracy to commit bank fraud and arson. In addition, Moody agreed to pay $11,136,241.82 in restitution.

On May 11, 2019, according to information presented at court, Moody was the President of Enloe State Bank in Cooper, Texas, when the bank had a fire that was determined to be arson. The fire was contained to the bank's boardroom, but the entire bank suffered smoke damage. Several files had been stacked on the boardroom table, all

of which were burned in the fire. Coincidentally, the bank was scheduled for a review by the Texas Department of Banking the following Monday.

Further investigation into the fire and the bank revealed that Moody had been creating false nominee loans in the names of several people, including some actual bank customers. Moody eventually admitted to setting the fire in the boardroom to cover up the criminal activity concerning the false loans. She also admitted to using the fraudulently obtained money to fund her boyfriend's business, other businesses of friends, and her own lifestyle. The fraudulent activity, which began in 2012, resulted in a loss to the bank of approximately $11 million. (*Responsible Agencies: FDIC OIG and Bureau of Alcohol, Tobacco, Firearms and Explosives. Prosecuted by the U.S. Attorney's Office (USAO) Eastern District of Texas*.)

Former Banker and Mortgage Broker Sent to Prison for Defrauding California Bank

On August 6, 2020, Carlos Wydler, and Leyla Wydler, both of Houston, Texas, were sentenced to prison following their convictions on multiple counts to include conspiracy, bank fraud, false statements on credit applications, wire fraud, and mail fraud.

Carlos Wydler was sentenced to 84 months in prison and was ordered to pay $6,804,260 in restitution to the victim bank and its insurer. Leyla Wydler was sentenced to 132 months and ordered to pay the $6.8 million in restitution joint and several with her stepson.

Leyla Wydler was the owner of several Houston-area businesses including Globan Mortgage Company, Casa Milagro, and First Milagro. In the spring of 2007, Carlos Wydler went to work at a California bank as a vice president in charge of the bank's credit card department. Shortly thereafter, the Wydlers developed a scheme in which Leyla Wydler would send credit card applications to the bank for Carlos Wydler to approve. He approved the applications for high credit lines and then, calling them "balance transfers," cash advanced the entire credit line to the borrower via wire or check with Leyla Wydler taking a fee from the borrowers' loan proceeds.

During trial, the evidence demonstrated that the Wydlers were also developing a real estate project in Houston at the time and used the "balance transfer" program to finance investors in their project. The jury heard that the bank did not know or approve of the fee-sharing or real estate financing arrangements.

For approximately a year, hundreds of loan applications were faxed or emailed from Leyla Wydler's business in Houston to Carlos Wydler at the bank in California. Many of these contained falsified income information and falsified supporting documents about borrowers' employment, income, and assets. Two eyewitnesses testified they saw Leyla Wydler routinely insert falsified income numbers, sometimes using white-out, on loan applications.

Leyla Wydler skimmed more than $1.4 million from loan proceeds, with Carlos Wydler approving approximately $600,000 more in unauthorized loans to family members. More than half of the Texas borrowers run through the Wydler family business in Houston defaulted on their loans. The bank sustained a loss of more than $6 million. (*Responsible Agencies: FDIC OIG, Federal Bureau of Investigation, and U.S. Postal Inspection Service (USPIS). Prosecuted by the USAO, Southern District of Texas.*)

Pandemic Relief-Related Cases

Since many of the programs under the Coronavirus Aid, Relief, and Economic Security Act (CARES Act) are administered through banks and other insured institutions, our Office of Investigations has been actively involved in investigating pandemic-related financial crimes affecting the banks. We do so in collaboration with the Pandemic Response Accountability Committee. In addition, our Office regularly coordinates with the supervisory and resolutions components within the FDIC to watch for developing patterns of crimes and other trends in light of the pandemic. Our Special Agents have been working proactively with other OIGs; U.S. Attorney's Offices (USAO); and other law enforcement agencies on cases involving frauds targeting the funds distributed through the CARES Act.

As mentioned earlier, these cases frequently involve fraud in the PPP, as illustrated in the examples that follow. We expect this important workload to continue to yield positive results in cases going forward.

Engineer Pleads Guilty to More Than $10 Million of COVID-Relief Fraud

On February 9, Shashank Rai, of Beaumont, Texas, pleaded guilty to one count of making false statements to a bank for his role in filing fraudulent bank loan applications seeking more than $10 million in forgivable loans guaranteed by the SBA under the CARES Act.

As part of his guilty plea, Rai admitted that he sought millions of dollars in forgivable loans guaranteed by the SBA from two different banks by claiming to have 250 employees earning wages when, in fact, no employees worked for his purported business. Rai made two fraudulent claims to two different lenders for loans guaranteed by the SBA for COVID-19 relief through the PPP.

According to court documents, the Texas Workforce Commission provided information to investigators of having no records of employee wages having been paid in 2020 by Rai or his purported business, Rai Family LLC. In addition, the Texas Comptroller's Office of Public Accounts reported to investigators that Rai Family LLC reported no revenues for the fourth quarter of 2019 or the first quarter of 2020.

According to court documents, materials recovered from the trash outside of Rai's residence included handwritten notes that appeared to reflect an investment strategy for the $3 million, which is the amount of money that Rai allegedly sought from the second lender. (*Responsible Agencies: Federal Housing Finance Agency OIG, SBA OIG, and USPIS. Prosecuted by the Fraud Section of the Criminal Division of DOJ and the USAO, Eastern District of Texas*.)

Man Purchased Lamborghini After Receiving $3.9 Million in PPP Loans

On February 10, David T. Hines, of Miami, Florida, pleaded guilty to one count of wire fraud for his role in obtaining $3.9 million in PPP funds, and using those funds, in part, to purchase a Lamborghini sports car.

As part of his guilty plea, Hines admitted that he fraudulently sought millions of dollars in PPP loans through applications to an insured financial institution on behalf of different companies. Hines caused to be submitted fraudulent loan applications that made numerous false and misleading statements about the companies' respective payroll expenses. The financial institution approved and funded approximately $3.9 million in PPP loans.

Hines further admitted that within days of receiving the PPP funds, he used the funds to purchase a 2020 Lamborghini Huracan sports car for approximately $318,000. Plea documents indicate that in the days and weeks following the disbursement of PPP funds, Hines did not make payroll payments that he claimed on his loan applications, but did, however, use the PPP proceeds for personal expenses. (*Responsible Agencies: FDIC OIG, USPIS, SBA OIG, Federal Reserve Board OIG, and Internal Revenue Service-Criminal Investigations. Prosecuted by the Fraud Section of the Criminal Division of DOJ.*)

Additional information about the FDIC OIG may be found at www.fdicoig.gov

Office of Inspector General Federal Housing Finance Agency

Established 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), the Federal Home Loan Mortgage Corporation (Freddie Mac) (together, the Enterprises), and the Common Securitization Solutions, LLC (CSS) , an affiliate entity of 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 2020, the Enterprises collectively reported more than $6.6 trillion in assets. The FHLBanks collectively reported more than $820 million in assets.

Also established 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 FHFA Director 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 13th year, are of unprecedented scope, scale, and complexity. FHFA's dual roles continue to present novel challenges. Consequently, OIG structures its oversight program to examine FHFA's exercise of its dual responsibilities, which differ significantly from the typical federal financial regulator.

Our annual Audit, Evaluation, and Compliance Plan explains our risk-based methodology and discusses the Agency's greatest financial, governance, and/or reputational risks identified by OIG. On an annual basis, we also assess FHFA's most serious management and performance challenges, If not addressed, the four challenges and one area of concern could adversely affect FHFA's accomplishment of its mission. OIG focuses 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. The management and performance challenges are:

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

The Enterprises are large, complex financial institutions that dominate the secondary mortgage market and the mortgage securitization sector of the U.S. housing finance industry. Given the taxpayers' enormous investment

in the Enterprises,[6] the unspecified timeline to end 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.

As the Enterprises' conservator, FHFA is vested by HERA with express authority to operate the Enterprises and conduct their business activities. Although FHFA has retained authority to make certain significant decisions for the Enterprises, it has delegated back to them authority for many matters, both large and small. However, FHFA has not clearly defined its expectations of the Enterprises for delegated matters, nor has it established the accountability standard that it expects the Enterprises to meet for such matters. Our work over the last six years has revealed continued challenges to Enterprise compliance with FHFA directives and Enterprise Board committees' execution of their responsibilities.

Our findings were echoed by Director Calabria in his September 2020 congressional testimony: "Fannie and Freddie have what I would consider some of the worst corporate cultures I've ever seen in corporate America. And fixing that is a fundamental prerequisite to getting out of conservatorship." For the Enterprises to be governed effectively, their boards of directors and committees thereof must fulfill their delegated responsibilities.

FHFA, as the Enterprises' conservator, 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 for the duration of the conservatorships and ensure that its established processes are followed for non-delegated matters to promote reasoned decision-making.

Notable Reports:

Corporate Governance: Fannie Mae Senior Executive Officers and Ethics Officials Again Failed to Follow Requirements for Disclosure and Resolution of Conflicts of Interest, Prompting the Need for FHFA Direction (EVL-2021-001, March 15, 2021)

Our prior reviews of Fannie Mae's conflict of interest (COI) framework revealed failures by its Chief Executive Officer (CEO) to timely and fully disclose potential conflicts and breakdowns by the Fannie Mae Board's Nominating and Corporate Governance Committee (NGC) and by FHFA. In this evaluation, we assessed, for the period from November 1, 2018, to June30, 2020, whether Fannie Mae and its senior executive officers followed FHFA's conservatorship directive (Directive) and Fannie Mae's revised governance documents for the disclosure and resolution of potential, actual, or apparent COIs. We found that Fannie Mae's CEO failed to make timely COI disclosures in 3 out of 7 instances and two other very senior executive officers failed to make timely disclosures in 2 out of 25 instances, in contravention of the Directive and Fannie Mae's governance documents. Their non-disclosures and untimely disclosures of COI matters were inconsistent with Fannie Mae's goal of operating with the highest standards of compliance and ethics. We also found that, for 3 of 7 COI matters involving the CEO, Fannie Mae documents show that Fannie Mae's Office of Compliance and Ethics substituted its judgment for that of the Board's NGC and displaced the NGC as the final decision maker, in contravention of the Directive and revised governance documents. FHFA agreed with the three recommendations in our evaluation report.

Freddie Mac Management Failed to Adopt and Implement Conflicts of Interest Policies Which Aligned Fully with FHFA's Directive on Senior Executive Officers' Conflicts of Interest, and With the Charter for the Freddie Mac Board's Nominating and Governance Committee (COM-2020-006, August 26, 2020)

In a September 2017 Management Alert to FHFA, we found that Freddie Mac's COI policies and procedures involving executive officers were not aligned with the Freddie Mac NGC's responsibilities. We recommended that FHFA, as conservator, direct the Freddie Mac Board of Directors to clarify the scope of the NGC's responsibilities under its Charter that relate to COI involving executive officers, and direct Freddie Mac to revise its policies and

6 While in conservatorship, the Enterprises have required almost $191.5 billion in financial investment from the Department of the Treasury (Treasury) to avert their insolvency and, through December 2020, the Enterprises have paid to the Treasury more than $301 billion in dividends on its investment.

procedures to align with the NGC's responsibilities. FHFA issued a Directive establishing its expectations concerning both Enterprises' internal processes for disclosing and resolving actual and potential COI involving senior executive officers. In this review, we found that Freddie Mac failed to comply with key requirements of the Directive. Accordingly, we reopened a recommendation from our Management Alert. FHFA agreed with our reopened recommendation and committed to direct Freddie Mac to revise its COI policy and procedures and require the Enterprise to train its Ethics Office staff on those revisions.

Supervision of the Regulated Entities: Upgrade Supervision of the Enterprises and Continue Supervision Efforts of the FHLBanks

As supervisor of the Enterprises, CSS, and the FHLBanks, FHFA is tasked by HERA to ensure that these entities operate safely and soundly so 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 Enterprise Regulation (DER) is responsible for supervision of the Enterprises and the Division of Federal Home Loan Bank Regulation (DBR) is responsible for supervision of the FHLBanks.

In its most recent annual Performance and Accountability Reports, FHFA cited its supervisory authority as its basis for ensuring the safe and sound operation of the Enterprises. FHFA also has advised that effective safety and soundness supervision "is essential to preparing the Agency and the Enterprises to responsibly exit and operate safely outside of conservatorship."

In March 2020, we reviewed the more than 40 reports we issued since October 2014 on FHFA's supervision program for the Enterprises. Thirty-four of these reports, read together, detailed chronic and pervasive deficiencies in the program itself, as well as in its execution. We identified deficiencies in these areas: (1) examination guidance and execution; (2) the size of the examiner workforce, and the training and qualifications of its members; (3) the communication of supervisory findings; and (4) quality control.

Consequently, the challenge facing FHFA is formidable: it must accomplish a great deal to remediate the deficiencies identified by us and by FHFA. FHFA has taken preliminary steps to upgrade and strengthen its supervision program. In May 2020, it engaged a contractor to prepare an "organizational optimization Blueprint" to ensure that FHFA "has the optimal workforce, infrastructure, and organization to carry out its supervisory mission in a post-conservatorship environment." In September 2020, FHFA announced, among other things, that it will "develop and maintain a world-class supervision program." The means and strategies to achieve this objective include, for example, "[a] dvance supervision practices, processes, systems, and tools to improve the efficiency and efficacy of the supervision programs…"

A year has passed since we issued our report summarizing the chronic and pervasive shortcomings in FHFA's supervision program. Since then, the Agency has not announced any key substantive decisions or definitive plans to "develop and maintain a world-class supervision program," which it recognizes is a pre-requisite to releasing the Enterprises from conservatorship. Instead, its efforts to "develop and maintain" an effective supervision program have been further delayed. In its December 2020 Annual Performance Plan, FHFA advised that it intends to "[d]evelop an action plan to address improvement opportunities identified in FHFA's optimization study to further the development of a world-class supervision program" by June 30, 2021.

We also review FHFA's supervision program for the FHLBanks. While we have found some shortcomings in that supervision program, we have not identified significant weaknesses in it. Like any other federal financial regulator, FHFA faces challenges in appropriately tailoring and keeping current its supervisory approach to the FHLBanks.

Notable Reports:

For Nine Years, FHFA Has Failed to Take Timely and Decisive Supervisory Action to Bring Fannie Mae into Compliance with its Prudential Standard to Ensure Business Resiliency (EVL-2021-002, March 22, 2021)

Pursuant to HERA, FHFA issued its prudential management and operations standards (PMOS) in 2012. PMOS 8, Principle 11 directs that a "regulated entity should have adequate and well-tested disaster recovery and business resumption plans for all major systems and have remote facilitates [sic] to limit the effect of disruptive events. "Beginning in 2012, FHFA consistently found critical deficiencies in Fannie Mae's business resiliency practices. Despite its awareness that these deficiencies had not been corrected, FHFA's Division of Enterprise Regulation (DER) never formally assessed whether Fannie Mae's business resiliency capabilities meet PMOS 8, Principle 11. DER neither issued an adverse examination finding nor directed Fannie Mae to submit a corrective plan to bring Fannie Mae's business resiliency program into compliance with PMOS 8, Principle 11. Rather than take timely and decisive supervisory action, DER has allowed the Enterprise to proceed at its own leisurely pace, with Fannie Mae currently projecting its work to be completed during 2021, nearly nine years after adoption of PMOS 8, Principle 11. We made two recommendations of which FHFA disagreed with one and proposed an alternative action for the other. We did not consider FHFA's alternative action to be reasonable. We closed both recommendations as rejected.

FHFA's Failure to Define and Clearly Communicate "Supervisory Concerns" Hinders the Enterprise Boards' Ability to Execute Their Oversight Obligations Under FHFA's Corporate Governance Regulation and Renders the Regulation Ineffective as a Supervisory Tool (EVL-2021-003, March 30, 2021)

FHFA's corporate governance regulation directs that each Enterprise Board of Directors (Board) is responsible for overseeing Enterprise management in its remediation of "all supervisory concerns" in a timely and appropriate manner. FHFA and DER guidance do not define "supervisory concern" for purposes of this regulation. According to DER's examiners-in-charge, a "supervisory concern" amounts to an issue or deficiency found during an examination activity that must be corrected but does not warrant a Matter Requiring Attention (MRA). They explained that DER communicates its "supervisory concerns" in the annual report of examination (ROE) issued to each Enterprise. Recognizing that an Enterprise Board can only satisfy its oversight responsibilities under the governance regulation when DER clearly advises it of "supervisory concerns," we assessed whether each of 12 sample statements from the 2018 and 2019 ROEs, which DER reported to us was a "supervisory concern," was clearly labeled as a "supervisory concern." We found that none were specifically categorized as "supervisory concerns" in the ROEs or DER's presentations to the Boards. Without clarity from DER, an Enterprise Board lacks a reasonable basis to understand that its oversight responsibilities under FHFA's governance regulation have been triggered. As a consequence, FHFA's ability to assess a Board's compliance with its governance regulation is impaired, and the regulation is rendered ineffective as a supervisory tool. FHFA agreed with the recommendation in our evaluation report.

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

FHFA's regulated entities are central components of the U.S. financial system and are interconnected with other large financial institutions. As part of their processes to guarantee or purchase mortgage loans, the Enterprises receive, store, and transmit significant information about borrowers, including financial data and personally identifiable information. Both the Enterprises and the FHLBanks have been the targets of cyberattacks.

As cyber threats and attacks at financial institutions increase in number and sophistication, FHFA faces challenges in designing and implementing its examination 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.

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.

Notable Report:

Landscape Report: Survey of the Impact of the SolarWinds Orion Supply Chain Compromise on FHFA and its Regulated Entities (OIG-2021-001, March 23, 2021)

FHFA-OIG issued a non-public report that surveyed the impact of the SolarWinds Orion compromise on FHFA and its regulated entities and the measures taken by the Agency and the regulated entities in response to the compromise.

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

The Enterprises rely heavily on counterparties and third parties to properly originate and service the mortgages the Enterprises purchase and to provide operational support for a wide array of professional services. As the Enterprises and FHFA recognize, that reliance exposes the Enterprises to a number of risks, including risks related to information security, business continuity, and other safety and soundness issues. There also is risk that a counterparty will not meet its contractual obligations, and risk that a counterparty may engage in fraudulent conduct.

FHFA has delegated to the Enterprises the management of their relationships with counterparties and third parties, and it reviews their management largely through its supervisory activities. We have noted our significant concerns with the strength and rigor of those supervisory activities. 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 these risks.

Notable Reports:

Oversight by Fannie Mae and Freddie Mac of Compliance with Forbearance Requirements Under the CARES Act and Implementing Guidance by Mortgage Servicers (OIG-2020-004, July 27, 2020)

Congress passed the Coronavirus Aid, Relief, and Economic Security Act (CARES Act) in March 2020 to address some of the adverse economic effects of the COVID-19 pandemic. Section 4022 of the CARES Act provides single-family homeowners, who are experiencing financial hardship due to the COVID-19 pandemic, the right to forbearance for up to 180 days (which can be extended for another 180 days) from making mortgage payments on loans owned or securitized by the Enterprises. An affected homeowner need only attest to the hardship; the Enterprises' mortgage servicers, counterparties who collect payments from borrowers and perform loss mitigation activities and other loan-related functions on behalf of the Enterprises, are prohibited from seeking documentation to support that attestation. FHFA publicly announced that homeowners will not be required to repay the missed or reduced payments in a lump sum payment once forbearance ends.

We undertook this review to provide information about oversight by the Enterprises over mortgage servicers' compliance with Section 4022 of the CARES Act and implementing guidance. We observed that neither Enterprise has collected data sufficient to permit an assessment of whether servicers are complying with the CARES Act and implementing guidance. The Enterprises reported to us that they have not asked any servicer to demonstrate compliance with the CARES Act and implementing guidance. National surveys conducted by one Enterprise suggested that a significant number of homeowners are not aware of the option of mortgage forbearance, and media reports stated that some servicers may have provided inaccurate advice to homeowners about repayment options. Because mortgage servicers are the primary point of contact for homeowners experiencing COVID-19 related financial hardship, we reviewed the information provided by a sample of 20 large servicers, 20 medium servicers, and 20 small servicers on their websites. Based on our survey of these websites, we could not determine whether homeowners were provided with accurate and complete information about forbearance.

Despite FHFA's Acknowledgement that Enterprise Reliance on Third-Parties Represents a Significant Operational Risk, No Targeted Examinations of Fannie Mae's Third-Party Risk Management Program Were Completed Over a Seven-Year Period (AUD-2021-007, March29, 2021)

We performed this audit in part to determine what examination activities DER completed, during the period 2014 through 2020, in response to identified risks in Fannie Mae's third-party risk management (TPRM) program. We found that, from 2014 through 2020, DER's completed examination activities related to Fannie Mae's TPRM program consisted solely of ongoing monitoring activities. No targeted examinations, included as part of DER's governing

supervisory framework to enable examiners to conduct "a deep or comprehensive assessment" of selected areas found to be of high importance or risk, were completed in this risk area. In light of the express recognition by DER and Fannie Mae of the risk associated with management of these third-party providers, the more than six years that Fannie Mae took to remediate an MRA identified in 2013, and DER's governing supervisory framework warranted the completion of one or more targeted examinations of this risk during the period 2014 through 2020. FHFA agreed with the recommendation in our audit report.

OIG Investigative Accomplishments

OIG's investigative mission is to prevent and detect fraud, waste, and abuse in the programs and operations of FHFA and its regulated entities. OIG's Office of Investigations (OI) executes its mission by investigating allegations of significant criminal and civil wrongdoing that affect the Agency and its regulated entities. OI's investigations are conducted in strict accordance with professional guidelines established by the Attorney General of the United States and CIGIE's *Quality Standards for Investigations*.

OI is comprised of highly-trained law enforcement officers, investigative counsels, analysts, and attorney advisors. We maximize the impact of our criminal and civil law enforcement efforts by working closely with federal, state, and local law enforcement agencies nationwide.

Notable Criminal Cases

Three Conspirators Sentenced in Loan Origination Scheme, Illinois

During this reporting period, Ryan Bailey, Amber Cook, and Irma Holloway were sentenced to prison for their roles in a loan origination scheme.

Court documentation revealed Holloway operated a construction company. Bailey was a loan originator and worked with Cook who was a loan processor. Holloway conspired with Bailey, Cook, and other bank insiders to defraud lenders by obtaining mortgage loans using materially false information. Holloway recruited straw buyers to purchase properties using fraudulent documentation, including fictitious verifications of deposit and documents concerning the buyers' income and assets. Once the loans closed, Holloway derived a financial benefit and provided kickback payments to the straw buyers, which were not disclosed to the lenders. The Enterprises, as investors in these loans, suffered losses.

Cook was sentenced to 48 months in prison, five years of supervised release and was ordered to pay over $4.7 million in restitution; Holloway was sentenced to 24 months in prison, five years of supervised release, and was ordered to pay approximately $3.7 million in restitution; and Bailey was sentenced to three months in prison followed by six months of home confinement, three years of supervised release and was ordered to pay over $5.3 million in restitution. Restitution for each defendant was ordered, at least in part, jointly and severally.

Project Manager Sentenced in Connection with COVID Relief Fraud, Oklahoma

On December 7, 2020, Benjamin Hayford was sentenced to 24 months in prison and five years supervised release, in the Northern District of Oklahoma, for fraudulently seeking more than $8 million in forgivable Paycheck Protection Program (PPP) loans under the CARES Act. In August 2020, Hayford pled guilty to bank fraud and making false statements to a financial institution.

Hayford fraudulently pursued millions of dollars in forgivable PPP loans from multiple banks by claiming fictitious payroll expenses. To support his applications, Hayford provided lenders with fraudulent payroll documentation purporting to establish payroll expenses that were, in fact, nonexistent. In addition, Hayford falsified the date for the establishment of a Limited Liability Partnership for which he sought relief.

A member bank of the FHLBank of Topeka was a target of one of the alleged fraudulent applications for a PPP forgivable loan.

Former Bank Executive Sentenced in $15 Million Construction Loan Fraud Scheme, Kansas

On November 10, 2020, Troy Gregory, former bank executive, was sentenced to 60 months in prison, three years of supervised release, and ordered to pay over $4.7 million in restitution in the District of Kansas for his role in carrying out a bank fraud scheme to obtain a $15 million construction loan from 26 banks.

In August 2019, Gregory was found guilty by a federal jury on charges of bank fraud and false statements.

According to the evidence presented at trial and at the sentencing hearing, Gregory was a bank executive and loan officer who had loaned millions to a group of borrowers who were struggling to make payments on the loans. Gregory initiated the process of making a $15.2 million construction loan to build an apartment complex to that same group of borrowers so they could pay back the other outstanding loans. To convince the other banks to participate, Gregory made and caused others to make false statements about the strength of the borrowers, the debt status of the apartment property and the existence of approximately $1.7 million in certificates of deposit for collateral on the loan, all to get the loan approved.

Instead of using the loan funds promised for building the apartments, Gregory immediately diverted over $1 million of the loan to pay for part of the certificates of deposit pledged as collateral, pay off debt on the apartment property and make payments on unrelated loans. Other banks that shared in this loan would not have participated in the loan without Gregory's false representations and promises. The victimized banks collectively lost approximately $5 million.

University National Bank, Gregory's employer, is a member bank of the FHLBank of Topeka.

Former Bank Executive Sentenced in Embezzlement Fraud Scheme, Tennessee

On July 22, 2020, former bank executive Connie Clabo was sentenced to 15 months in prison, four years of supervised release, and ordered to pay $516,630 in restitution for her role in an embezzlement fraud scheme. In November 2019, Clabo pled guilty in the Eastern District of Tennessee to charges of theft, embezzlement, and willful misapplication of moneys, funds, and credits of a bank the deposits of which are insured by the FDIC and willfully filing a false federal income tax return for her participation in this scheme.

According to court documents, Clabo was the Vice President of Loan Operations at SmartBank responsible for overseeing the accurate entry of financial transactions into the bank's general ledger system. Clabo admitted to abusing her position with SmartBank to embezzle more than $600,000. To do this, Clabo manipulated SmartBank's general ledger to fund 60 cashier's checks that were then deposited into either Clabo's personal bank account or to third parties to whom she owed money. Additionally, Clabo manipulated SmartBank's general ledger system to fraudulently reduce her parents' home mortgage loan by $46,000 to under $400. Similarly, Clabo manipulated SmartBank's general ledger system to fraudulently pay off her own SmartBank home mortgage loan amount of over $200,000.

SmartBank, Clabo's employer and the victim bank, is a member bank of the FHLBank of Cincinnati.

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

The U.S. Department of Housing and Urban Development (HUD), Office of Inspector General (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

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, use housing as a platform for improving quality of life, and build inclusive and sustainable communities free from discrimination. Its programs are funded through roughly $50 billion in annual congressional appropriations. While organizationally located within HUD, HUD OIG provides independent oversight of HUD programs and operations.

HUD has two component entities that have a major impact on the Nation's financial system: the Federal Housing Administration (FHA) and the Government National Mortgage Association (Ginnie Mae). FHA mortgage insurance provides lenders with protection against losses when homeowners and owners of multifamily properties and healthcare facilities default on their loans. FHA is one of the largest providers of mortgage insurance in the world, having insured more than 50.8 million single-family and roughly 68,000 multifamily and healthcare facility mortgages since its inception in 1934. FHA reported that in fiscal year 2020, more than 800,000 single-family home buyers purchased a home using an FHA-insured mortgage, while FHA also insured 977 loans for multifamily properties. As of September 2020, FHA had an active insurance portfolio valued at more than $1.3 trillion. 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. The pools of loans are those insured or guaranteed by FHA, HUD's Office of Public and Indian Housing (PIH), the U.S. Department of Veterans Affairs (VA), and the U.S. Department of Agriculture. 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 MBSs valued at approximately $2.12 trillion. A majority of the MBSs consist of FHA-insured mortgages. Ginnie Mae offers the only MBSs 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 an MBS fails to make the required pass-through payment of principal and interest to investors, Ginnie Mae is required to advance the payment and will assume control of the issuer's MBS securities pools and the servicing of the loans in those pools. In fiscal year 2020, $749 billion in newly issued MBSs guaranteed by Ginnie Mae were purchased by investors.

HUD OIG Oversight Relating to Financial Matters

HUD OIG continually looks for ways to meet the needs of HUD's beneficiaries and to protect taxpayer dollars. HUD OIG's oversight efforts focus on identifying and addressing HUD's most serious management challenges. Of the challenges identified in our Top Management Challenges for 2021 report,[7] the following relate to financial oversight:

- Responding to the COVID-19 pandemic
- Protecting the FHA insurance fund
- Instituting sound financial management
- Management and oversight of information technology

HUD OIG uses these challenges to target its oversight efforts, as demonstrated in the following summaries and descriptions of related HUD OIG oversight work.

Responding to the COVID-19 Pandemic

HUD, like all Federal agencies, faced unprecedented challenges caused by the COVID-19 pandemic. Through successive stimulus appropriations, Congress has provided more than $24 billion in funding to HUD to assist renters, landlords, vulnerable populations, and impacted communities in preventing, preparing for, and responding to the COVID-19 pandemic. The Coronavirus Aid, Relief, and Economic Security Act (CARES Act) and subsequent administrative actions created protections for renters, homeowners, and landlords participating in HUD programs through temporary moratoriums on evictions and certain foreclosure actions, as well as forbearance on payments of federally backed mortgage loans.

To evaluate HUD's pandemic response, HUD OIG has initiated agile, limited-scope engagements to complete work quickly and offer insights to policymakers and the public in a timely manner. For example, HUD OIG reported key considerations from prior audits of the Single Family Default Monitoring System (SFDMS) and the partial claim loss mitigation option. Additionally, HUD OIG has identified ongoing challenges that relate to financial oversight: (1) ensuring that the public receives accurate information about HUD's pandemic response and relief programs and (2) implementing mortgage loan forbearance requirements in HUD's programs.

Ensuring That the Public Receives Accurate Information

For HUD's pandemic response efforts to be effective, the American public needs complete and accurate information about HUD's pandemic response and relief programs. It is crucial that HUD have clear, complete, and accessible guidance available to help renters at a time when their health and financial stability may be at risk. If HUD maintains up-to-date and easily accessible information for all impacted renters, including information on any new renter protections, it will help to ensure that renters know their rights, maintain housing stability through the pandemic, and avoid homelessness. Similarly, it is important that HUD provide quality customer service to homeowners, industry partners, and the general public with direct, accurate, and complete responses to inquiries regarding forbearance and foreclosure relief provided by the CARES Act.

HUD OIG has completed reviews of HUD's communications with renters about the CARES Act eviction moratorium[8] and of HUD's responses to inquiries from homeowners, industry partners,[9] and the general public.[10] In those reviews,

7 Top Management Challenges Facing the U.S. Department of Housing and Urban Development in 2021 (Nov. 25, 2020), available at https://www.hudoig.gov/sites/default/files/2020-12/TMC%202021_0.pdf.

8 Audit Memorandum 2021-NY-0801, Opportunities Exist To Improve HUD's Communication to Renters About Eviction Protections, issued October 13, 2020.

9 Industry partners include mortgage servicers, real estate agents, housing counseling agents, nonprofit organizations, and local government agencies.

10 Audit Memorandum 2020-PH-0801, Opportunities Existed To Improve HUD's Responses to Inquiries From Borrowers, Industry Partners, and the General Public Regarding Forbearance and Foreclosure Relief Provided by the CARES Act, issued September 22, 2020.

HUD OIG found many instances in which HUD's communications were clear and sufficient but also identified several opportunities for improvement. For example, (1) guidance for renters can be difficult to locate, does not cover all impacted renters, and does not consistently provide key information; (2) search tools and other information on its website do not help all impacted renters determine whether they are protected; and (3) HUD's website and published guidance do not consistently inform renters about additional eviction protections available. With regard to HUD's responses to inquiries regarding forbearance and foreclosure relief, HUD did not clearly answer questions related to eligibility requirements for forbearance and stand-alone partial claims. Therefore, HUD could provide better customer service to homeowners, industry partners, and the general public with more direct, accurate, and complete responses to their inquiries.

HUD OIG also performed two reviews, 5 months apart, of whether websites of mortgage loan servicers offered complete and accurate information to homeowners with FHA-insured mortgages.[11] Through this work, HUD OIG highlighted for FHA leadership several ways in which the servicers participating in FHA programs could improve the quality of information the servicers provide to homeowners with FHA loans by noting where servicer website information was incomplete, inconsistent, dated, or unclear.

Implementing Forbearance Requirement in HUD's Mortgage Programs

The CARES Act and subsequent administrative action provided financial relief to homeowners with HUD-insured mortgage loans experiencing COVID-19-related hardships by permitting forbearance of their mortgage payments for up to 360 days, with up to 6 additional months of forbearance in limited circumstances. FHA moved quickly to make program changes to account for forbearance and allow servicers to file partial claims for insurance benefits to recoup missed payments from borrowers. However, it is important that FHA ensure that it has accurate and complete data from its servicers regarding loans in forbearance, data which are necessary to estimate and prepare for the processing of future partial claims. HUD OIG is concerned that inaccuracies in forbearance data reported by servicers could mean that servicers are not complying with HUD's forbearance requirements. OIG is conducting oversight in this area, as well as performing work looking at the forbearance options servicers are offering to homeowners.

Key Considerations from Prior Audits of the Single Family Default Monitoring System and the Partial Claim Loss Mitigation Option

HUD OIG recently provided to HUD key considerations from prior audits of HUD's SFDMS and the partial claim loss mitigation option.[12] These audits previously identified HUD's lack of effective controls to ensure that lenders reported default information accurately and in a timely manner, lenders promptly filed and reported partial claims, and partial claims fully reinstated delinquent loans. Prior audits also identified how the current design of partial claims results in an inferior lien position on the securing property during a foreclosure sale and negatively affects HUD's ability to identify and collect partial claims out of surplus proceeds from foreclosure sales to third parties. HUD should address these situations now to ensure program integrity and minimize the risk of financial loss during the COVID-19 national emergency. In the memorandum, HUD OIG noted that if HUD does not expedite corrective actions from prior audits, it may experience financial loss (1) due to its inability to evaluate policy effectiveness and initiate required policy changes and (2) from improper or uncollectible partial claims.

HUD's challenges with default reporting could impact its ability to report to Congress, establish a budget, and evaluate policy effectiveness or potential policy changes. Default reporting issues could also hinder HUD in determining the actual number of borrowers seeking and obtaining forbearance assistance due to the COVID-19 national emergency. Further, if HUD had challenges with partial claims during the periods audited, it might have serious challenges during the COVID-19 national emergency, given the substantial number of loans in forbearance and the delinquency status and timing of many of the forbearance periods ending at the same time.)

11 Evaluation Memorandum, Some Mortgage Loan Servicers' Websites Offer Information About CARES Act Loan Forbearance That Is Incomplete, Inconsistent, Dated, and Unclear, issued April 27, 2020; Evaluation Memorandum, Some Mortgage Loan Servicers' Websites Continue To Offer Information About CARES Act Loan Forbearance That Could Mislead or Confuse Borrowers or Provide Little or No Information at All, issued September 30, 2020.

12 Audit Memorandum 2021-KC-0801, Key Considerations From Prior Audits of the Single Family Default Monitoring System and the Partial Claim Loss Mitigation Option (Mar. 12, 2021).

Protecting the FHA Insurance Fund

As previously discussed, FHA provides government insurance-guarantees on mortgages for single-family homes, apartment buildings, residential healthcare facilities, and hospitals as well as reverse mortgages called home equity conversion mortgages (HECM). By committing the full faith and credit of the United States to repayment of lenders should the borrower default, HUD expands affordable home ownership, rental housing, and healthcare facilities. Yet HUD is challenged in protecting the FHA mortgage insurance fund. Through the Mutual Mortgage Insurance (MMI) fund,[13] FHA insures participating lenders against losses when borrowers default on loans, which allows lenders to make loans to borrowers who otherwise might not qualify. From April 2019 through March 2020, the MMI fund paid out almost $14 billion in reimbursements to servicers for defaulted loans. For those claims for which the lender conveyed the property to HUD and HUD resold the property, HUD recovered only about 53 percent of the funds paid out.

Without sufficient controls, sufficient 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 (Treasury) is required, as authorized for Federal credit programs.

As highlighted in the Top Management Challenges for 2021 report, in protecting the FHA and Ginnie Mae programs, HUD is confronted with

- a lack of sufficient safeguards in FHA's mortgage insurance programs,
- large losses to FHA's MMI fund due to HECMs, and
- potential risk to the MMI fund and HUD programs due to increased claims resulting from COVID 19.

For more than a decade, HUD OIG has reported the need for more safeguards to protect FHA insurance programs. Recently, HUD OIG noted concerns regarding the need to better protect FHA insurance programs, both as a Top Management Challenge for 2021 and through our oversight work. In addition, HUD OIG continues to have significant investigative activity related to FHA programs.

As noted in our Top Management Challenges for 2021 report, OIG remains concerned about the continued adverse impact that HECMs have on the FHA insurance fund. The HECM portfolio has had a longstanding negative impact on the insurance fund. HUD has made progress in addressing the financial stress that the HECM portfolio puts on the insurance fund through a series of policy changes and other efforts. Although FHA recently reported improvements in this area, the negative cash flow of the HECM portfolio continues to be covered by the positive cash flow from the forward mortgages that make up the remainder of the insurance fund portfolio. To address our concerns in this area, we are conducting an audit to determine whether HUD designed the HECM program to control the risk of loss related to assignment claims and ensure program viability, including whether the program can operate without a Federal subsidy.

Our Top Management Challenges for 2021 report highlighted that HUD is also challenged by the significant increase in the number of nonbanks[14] issuing MBS pools that Ginnie Mae guarantees. At the end of fiscal year 2019, nonbank issuers accounted for 82 percent of Ginnie Mae's business volume, up from 78 percent in the prior year and considerably increased from 51 percent in June 2014 and 18 percent in fiscal year 2010. Nonbanks must have sufficient liquidity to advance payments to investors when a borrower does not pay, or to purchase the loan out of the pool. They are also less regulated than banking institutions. Ginnie Mae noted in its 2020 Annual Report, "As 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 transactions and other types of external financing, and sales of mortgage servicing rights to

13 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.

14 Nonbanks are financial institutions that offer only mortgage-related services and thus have no depositor base.

provide liquidity. Regardless, Ginnie Mae's issuer composition greatly reduces the risk of exposure to the failure of any one institution."[15]

FHA Insured $940 Million in Loans for Properties in Flood Zones without the Required Flood Insurance

FHA insured loans for properties in special flood hazard areas that did not have the required National Flood Insurance Program (NFIP) insurance. FHA insured at least 3,870 loans that closed in 2019, totaling $940 million, which were not eligible for insurance because they were made for properties that lacked the required flood insurance coverage. OIG identified loans that had private flood insurance instead of the required NFIP coverage, coverage that did not meet the minimum required amount, or no NFIP coverage at the time the loan was closed and endorsed with FHA insurance. This condition occurred because FHA did not have information in its system that would be needed to identify flood insurance issues, making it unable to prevent endorsement of ineligible loans. HUD would be able to detect and mitigate this issue during reviews of loan files, but because more than 96 percent of the loan files were not reviewed by HUD, the lack of required flood insurance was often not detected. By implementing OIG recommendations, HUD will be able to identify the lack of flood insurance and avoid insuring at least $940 million in ineligible loans each year. The potential loss on these loans is $432.6 million based on the FHA insurance fund average loss rate of 46 percent as of June 30, 2020.

Investigative Activity Involving FHA Insurance Fund

OIG also helps protect the FHA insurance fund by conducting investigations of alleged fraud negatively affecting the fund and securing recoveries. For the period April 1, 2020, through March 31, 2021, HUD OIG completed 91 single-family investigations of fraud against the FHA insurance fund. A majority of the investigations focused on loan origination fraud involving forward mortgages. Recoveries from these cases totaled nearly $127.6 million (both criminal and civil recoveries). For example:

HUD-Approved Direct Endorsement Lender Agrees To Pay $24.9 Million

Guild Mortgage Company, a HUD-approved direct endorsement lender, entered into a settlement agreement with the United States and agreed to pay $24.9 million to resolve allegations that the lender violated the False Claims Act. The Guild Mortgage Company failed to comply with program rules that require lenders to maintain quality control programs and failed to follow self-reporting requirements. Although the Guild Mortgage Company's participation in this settlement did not constitute an admission of liability, the defined unallowable costs make it clear that the company certified and approved loans that were not eligible for FHA mortgage insurance and that without the lender's actions, HUD would not have insured or guaranteed the loans. The lender also indicated in the agreement that it would identify similar situations not covered by this agreement and reimburse the United States for additional unallowable costs.

Investors Agree To Pay HUD $200,000 In Real Estate Owned Flipping Scheme

Laziza Abdullaeva and Aziz Ashurov, real estate investors, entered into a settlement agreement with the United States and agreed to pay $200,000 to HUD to resolve allegations that they violated HUD's Real Estate Owned (REO) program rules. During the purchase of four REO properties, Abdullaeva and Ashurov falsely represented to HUD that they intended to occupy the properties as a primary residence for a period of 12 months. Abdullaeva and Ashurov failed to comply with the residency requirement and instead purchased, renovated, and resold the properties through their real estate investment company, Capital Invest, LLC.

15 Audit Report 2021-KC-0002, FHA Insured $940 Million in Loans for Properties in Flood Zones Without the Required Flood Insurance, issued January 5, 2021.

Trio Sentenced in Mortgage Loan Modification Scam

Sara Cordry and Ruby Price, co-owners of The Arize Group, Incorporated (AGI), and Tylor Korn, co-owner of Reliant Home Financial Group (RHFG), were collectively sentenced in U.S. District Court to 63 months incarceration, 6 years supervised release, and 1 year probation. During a 1-year span, the conspirators, through AGI and RHFG, orchestrated a mortgage loan modification scheme, whereby they promised struggling homeowners that they would provide them with mortgage modification services in exchange for an advance fee. However, no modification services were provided, and the homeowners often found themselves worse off financially than they were before dealing with the conspirators. Cordry was found guilty of conspiracy, mail fraud, and wire fraud and was ordered to pay FHA more than $1 million in restitution after pleading guilty to defrauding HUD. Korn and Price were ordered to pay more than $1.3 million in restitution to individual victims in connection with their guilty plea to conspiracy to commit mail and wire fraud. HUD OIG and Federal Housing Finance Administration (FHFA) OIG conducted this investigation.

Home-Repair Con Man Sentenced to 11 Years Incarceration

Businessman Gregory Ziglar was sentenced in U.S. District Court to 11 years incarceration and 5 years supervised release and ordered to pay $325,522 in restitution, of which $18,310 is to be paid to FHA, $54,147 to the Internal Revenue Service (IRS), and $253,065 to individual victims. For more than 4 years, Ziglar defrauded homeowners through FHA's Title I Home and Property Improvement Loan Program. Ziglar, who used aliases and multiple shell companies, solicited homeowners through advertisements that offered home repair services and assistance with federally insured financing. Ziglar claimed to prospective clients that he would obtain financing on behalf of the homeowners and that all construction would be performed by his contractors. Without authorization, he created false estimates or purported agreements, which he sent to Title I lenders to secure the loans. He inflated the estimates and agreement amounts to maximize the loan amounts. Once the homeowners provided the loan proceeds to Ziglar, he hired contractors to perform the work, paid them substantially less than what was listed on the estimates and agreements submitted to the lenders, and kept the remaining funds. In some instances, the contractors performed little to no work or performed work that was shoddy and incomplete. Also, in violation of the Title I loan program, Ziglar fraudulently charged the homeowners a $2,500 referral fee for the financing. The majority of Ziglar's victims were elderly. HUD OIG, the IRS, the Newport News, Virginia, Police Department, and the United States Postal Inspection Service conducted this investigation.

HUD-Approved Direct Endorsement Lender Agrees To Pay $15.06 Million

Guaranteed Rate, Inc., a HUD-approved direct endorsement lender, entered into a $15.06 million settlement agreement with the United States, of which $7.8 million is required to be paid to FHA to resolve allegations that the lender violated the False Claims Act and the Financial Institutions Reform, Recovery, and Enforcement Act of 1989 by knowingly violating the material program requirements when it originated and underwrote mortgages insured by FHA and guaranteed by the VA. Guaranteed Rate failed to comply with program rules that require lenders to maintain quality control programs and failed to follow the self-reporting requirements. In violation of the program's rules, Guaranteed Rate's FHA underwriters received commissions and gifts and in certain instances, failed to review documents that were relevant to the underwriting decision. As part of the settlement agreement, Guaranteed Rate acknowledged that it certified and approved loans that were not eligible for FHA mortgage insurance or VA guarantees and that, without the lender's actions, HUD and the VA would not have insured or guaranteed the loans. The lender also indicated in the agreement that it had made changes to its self-reporting procedures, underwriter compensation practices, and underwriting filing and documentation procedures.

Investigation Leads To Return of More Than $1.6 Million to FHA

NOVA Financial & Investment Corporation, a lender approved to participate in HUD's FHA Title II Single Family Mortgage Insurance Program, entered into a $752,518 settlement agreement after HUD's Mortgagee Review Board (MRB) issued a notice of violation and notice of intent to seek civil money penalties for violations of FHA underwriting

requirements. The MRB action was due to the successful criminal prosecution of three individuals who, from October 2008 through May 2009, made false statements and created false loan documents for the purpose of influencing NOVA's lending actions and persuading NOVA to qualify borrowers for FHA-insured loans. The false statements and documents concealed the true source of the borrowers'"gift" funds and made it appear as though the borrowers' family members provided the funds when the defendants had provided the gift funds, contrary to FHA prohibitions. HUD OIG and the Federal Bureau of Investigation conducted this investigation.

Former Title Insurance Underwriter To Pay More Than $400,000 in Restitution for Title Insurance Scam

Former title insurance underwriter, Ginger Cunningham, was sentenced in U.S. District Court to a total of 14 months incarceration and 3 years supervised release and ordered to pay more than $412,344 in restitution to the title company and other individual victims. For approximately 19 months after she was dismissed by the title company, Cunningham continued to represent herself as an independent agent of the title company, sold fictitious title insurance policies, and collected premium payments for approximately 973 fictitious title insurance policies with associated mortgage loans totaling more than $123 million, of which more than $9.1 million was attributable to FHA-insured mortgages. As a result of this investigation, legitimate title insurance policies were retroactively issued for the affected mortgages to protect the FHA insurance fund, mortgage lending institutions, and mortgage borrowers. HUD OIG, FHFA OIG, and the North Carolina Department of Insurance conducted this investigation.

Instituting Sound Financial Management

HUD made progress during fiscal year 2020 in addressing its financial management weaknesses. For fiscal year 2020, HUD received an unmodified opinion[16] on its consolidated financial statements, the first such opinion since fiscal year 2012. HUD OIG reported only one material weakness in internal control over financial reporting and one instance of noncompliance with applicable laws and regulations.[17] HUD OIG attributes this substantial improvement in financial management to the Office of the Chief Financial Officer's (OCFO) financial transformation initiative and coordination with program offices. However, while significant progress has been made, work remains to ensure the integrity and effectiveness of the HUD financial management systems that underpin programs and operations.

OCFO's financial transformation initiative continued to strengthen internal controls through HUD's actions to evaluate audit findings and to develop and implement overall remediation plans and executions. HUD's efforts are starting to show results, but it is important that HUD continue to work toward a complete financial management transformation to ensure a sustained commitment to the identification and mitigation of internal control weaknesses and significant risks. This work is especially important in light of the COVID-19 pandemic environment, in which waivers of normal processes and controls and competing priorities may pressure components to forgo proper financial management and accounting processes.

HUD continues to operate at a "basic" level of financial maturity based on Treasury's Financial Management Maturity Model. In prior years, OIG has cited HUD as being at an "inadequate" level of financial management maturity; however, in some areas, HUD now operates at the "capable" level, and HUD is trending toward an overall classification of "capable." Further, HUD's enterprise risk management program is approaching a classification of "effective."

HUD needs to continue to remediate OIG's open recommendations and improve its internal control effectiveness to ensure reliable and accurate financial reporting and compliance with laws and regulations. In addition, HUD needs to be able to sustain the improvements it has made so that HUD and its program offices can operate at a level that will consistently produce reliable and timely financial reports and ensure continuity during challenging times, such as those brought on by the COVID-19 pandemic.

16 The American Institute of Certified Public Accountants' The Clarified Statements on Auditing Standards, AU-C 700.18, which states: "The auditor should express an unmodified opinion when the auditor concludes that the financial statements are presented fairly, in all material respects, in accordance with the applicable financial reporting framework."

17 Audit Report 2021-FO-0003, Audit of HUD's Fiscal Year 2020 Consolidated Financial Statements, issued December 4, 2020.

However, HUD continues to experience financial management system weaknesses. Several significant financial business processes continue to be manual or nonexistent, resulting in unreliable and untimely financial reporting and poor financial management oversight. For example, PIH uses manual processes and Excel spreadsheets to comply with cash management requirements, resulting in untimely reports on HUD's prepayments, accounts payable, and accounts receivable. HUD also does not have a cost accounting system that can accurately report program costs, and, specifically, PIH lacks a system capable of fully accounting for its loan guarantee programs. However, HUD continues its efforts to implement financial management systems in all program areas and offices. HUD planned to start developing a cost accounting system during 2020 and had already started developing a system to address PIH's cash management needs; however, neither system is expected to be operational by the time its fiscal year 2021 financial reporting is due.

HUD is making progress in its efforts to bring its financial management system into compliance with the Federal Financial Management Improvement Act of 1996 (FFMIA), a law designed to ensure that Federal financial management systems provide accurate, reliable, and timely financial management information. During fiscal year 2020, HUD brought four systems into compliance with FFMIA and assessed a fifth that was previously determined to be noncompliant as a nonfinancial system due to the implementation of a new module within HUD's financial management system that replaced its functionality. However, the challenges in maintaining and ensuring that HUD's legacy systems can support the proper financial management of HUD's programs and operations will persist until they are modernized.

HUD needs to remain committed to modernizing its financial systems to ensure that it can continue to operate as effectively and efficiently as possible during challenging times, such as the pandemic, as well as in times of normalcy.

Management and Oversight of Information Technology

The Federal Information Security Modernization Act of 2014 (FISMA) requires Federal agencies to develop, document, and implement an agencywide program to provide information security for the information and information systems that support their operations. HUD financial systems are integral to HUD programs, and maintaining data integrity and security of those systems is vital to management of Federal resource and asset stewardship. Consistent with FISMA, HUD OIG annually evaluates HUD's information security and privacy program effectiveness, including information security controls over HUD's resources.

Using the annual Inspector General FISMA metrics, our fiscal year 2020 evaluation determined that HUD's information security had increased in overall maturity from "defined" to "consistently implemented," which is HUD's first time achieving this level.[18] Despite this improvement, OIG assessed HUD's overall program as not effective, based on FISMA measures. OIG observed progress in key Office of the Chief Information Officer (OCIO) initiatives in fiscal year 2020 to address HUD's information security, privacy, and information technology challenges. Throughout fiscal year 2020, HUD created remediation plans and took corrective actions for many prior-year FISMA and privacy recommendations. HUD OCIO had success in modernizing parts of the HUD infrastructure, such as the data centers, cloud adoption, and a mainframe system. HUD's progress in cloud adoption, such as the FHA Catalyst platform, demonstrated positive movement that should help HUD securely modernize.

Ongoing executive leadership and support will enable HUD to continue its focus on managing and prioritizing its information security program, maturing the FISMA domains, and securing all information systems that support HUD's mission.

18 Evaluation Report 2020-OE-0001, HUD Fiscal Year 2020 Federal Information Security Modernization Act of 2014 (FISMA), issued Nov. 30, 2020.

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,[19] the Community Development Revolving Loan Fund,[20] and the Central Liquidity Facility.[21]

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

19 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.

20 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.

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

services to consumer credit unions (also known as natural person credit unions). Due to the relative size of their 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 federally-insured 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.[22] 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, 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 conducted NCUA-specific work that could be instructive for the broader financial sector. In September 2020, we issued an audit report that assessed the NCUA's examination and oversight authority of credit union service organizations (CUSOs) and third party vendors. Unlike Federal banking agencies that have direct statutory examination and oversight authority over bank service providers and bank vendors, the NCUA lacks authority over CUSOs and third party vendors. Our audit found that the NCUA gaining this statutory authority could enable it to more effectively identify and reduce the risks that CUSOs and vendors pose to credit unions, particularly in light of credit unions' increased reliance on them to perform mission-critical functions that impact over 120 million credit union members. The NCUA could exercise this authority efficiently because many credit unions use the same vendors.Only five core processor vendors serve multiple credit unions that control approximately 85 percent of credit union data, and only five technology service provider vendors serve over 52 percent of credit unions that hold 75 percent of total credit union assets.We recommended that NCUA management work with appropriate Congressional committees regarding amending the Federal Credit Union Act to grant the NCUA the authority to subject credit union service organizations and credit union vendors to examination and enforcement authority to the same extent as if they were an insured credit union. Our recommendation is consistent with recommendations previously made by the Financial Stability Oversight Council and the Government Accountability Office. A recent discussion draft of legislation being circulated in the U.S. House of Representatives would provide the NCUA this statutory oversight authority.

In June 2020, we issued an audit report that reviewed AMAC's ability to protect personally identifiable information (PII) found within the records of liquidated credit unions. We determined that AMAC's staff considered the safeguard of PII during the pre-liquidation planning process, records maintenance, and destruction of records of liquidated credit unions. In addition, we also determined that AMAC staff charged with overseeing the liquidation of credit unions generally complied with applicable policies and procedures related to the safeguarding of PII.

In April 2020, OIG became part of a working group of CIGFO members designed to coordinate investigative efforts combating fraud associated with the CARES Act stimulus programs.

22 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.

I. 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), 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 6 divisions and 24 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 (FY) 2020, the SEC employed 4,430 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 Dodd-Frank 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.

II. SEC OIG Work Related to the Broader Financial Sector

In accordance with Section 989E(a)(2)(B)(i) of Dodd-Frank, 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

Final Management Letter: Actions May Be Needed To Improve Processes for Receiving and Coordinating Investor Submissions; May 24, 2021

During our recent evaluations of the Office of Investor Education and Advocacy (OIEA) operations and the SEC's management of its tips, complaints, and referrals (TCR) program, we observed that OIEA sends thousands of investor submissions (that is, investor questions and complaints; TCRs of suspected securities fraud or wrongdoings; and other matters) it receives to the Division of Enforcement's (Enforcement) TCR system; at the same time, Enforcement transfers to OIEA thousands of investor submissions that Enforcement receives. The majority of matters received are not transferred, and, when needed, processes and controls are in place to transfer matters between OIEA and Enforcement. Nonetheless, during our evaluation of the TCR program, we identified 2 matters of the 3,303 we reviewed that were not timely and properly transferred from OIEA to the TCR system. Notably, OIEA management took prompt corrective action and the vast majority of matters we reviewed were transferred properly when needed. However, if the SEC continues to maintain multiple reporting mechanisms, the agency may gain efficiencies and reduce certain risks if it can better ensure investors submit matters directly to the appropriate division or office.

We also noted that the majority of investor submissions are received from portals on the SEC's public website. However, the primary landing page for the public to submit matters to the SEC (https://www.sec.gov/complaint/select.shtml) provides minimal information to help investors choose one reporting mechanism over another, and does not provide examples of common concerns associated with each option. In addition, other public-facing instructions, including a 2011 investor publication and a 2017 investor bulletin, provide conflicting information about how to file a complaint. These resources serve as enabling functions that affect the SEC's mission and involve several divisions and offices. Therefore, the SEC may benefit from assessing and, as needed, revising information on its public website to ensure retail investors and others have clear and easily understood instructions for reporting matters to the SEC.

Lastly, the SEC Ombudsman receives a variety of matters, including matters the Ombudsman categorizes and publicly reports as "Allegations of Securities Law Violations/Fraud." However, it appears that the Ombudsman has not always entered those matters into the agency's TCR system because, in some cases, the Ombudsman did not believe the matters warranted a TCR. Use of the broad descriptive label "Allegations of Securities Law Violations/Fraud" for

matters that do not warrant TCRs may unintentionally misrepresent the nature of matters submitted by investors. Management's review of the handling, categorization, and public reporting of matters submitted to the Ombudsman, particularly those matters related to potential securities law violations and fraud, may be beneficial.

On May 24, 2021, we issued our final management letter encouraging management to review and respond to each of these concerns. This management letter is available on our website at https://www.sec.gov/files/Final-Mgmt-Ltr-Actions-May-Be-Needed-To-Improve-Processes-for-Receiving-Coordinating-Investor-Submissions.pdf.

The SEC Can Further Strengthen the Tips, Complaints, and Referrals Program; Report No. 566; February 24, 2021

The SEC encourages the public to file complaints or submit tips related to possible securities law violations, broker or firm misconduct, or any unfair practices in the securities industry that pose a risk of harm to investors, collectively referred to as Tips, Complaints, and Referrals (TCRs). Between FY 2018 and quarter 1 of FY 2020, the SEC received more than 40,000 TCRs, which are maintained in the agency's TCR system. Since 2012, the SEC's TCR Oversight Board has governed the TCR program.

We conducted this evaluation to assess the SEC's management of the TCR program. Specifically, we sought to determine whether (1) the SEC established an effective internal control system for collecting, triaging, and responding to credible allegations of violations of the federal securities laws; (2) the SEC safeguarded and maintained TCR source materials, as required; and (3) the TCR Oversight Board used effective tools, such as a risk management framework, to evaluate, respond to, and monitor TCR program risks and trends.

Overall, the SEC's TCR program has established an effective internal control system for collecting, triaging, and responding to credible allegations of violations of the federal securities laws. Safeguards to maintain TCR source materials are in place, as well as a risk management framework to evaluate, respond to, and monitor TCR program risks and trends. Policies, procedures, and training are available to SEC staff, and generally, TCR Points of Contact are satisfied with the work performed by the current TCR business owner (the Office of Market Intelligence within the agency's Division of Enforcement). However, the TCR program could be strengthened by better ensuring compliance with established requirements.

For example, we found that some TCRs exceeded the prescribed number of business days for entry into the TCR system. Delays in this process could delay the identification and investigation of allegations of wrongdoing. Moreover, we determined that, for TCRs open 90 business days or more, required notes explaining the circumstances preventing timely resolution of these TCRs did not always exist or include sufficient detail. Ensuring that staff enter into the TCR system required notes explaining the circumstances preventing timely resolution of TCRs could help inform management of TCRs requiring additional work and could assist management in better monitoring the status of TCRs. We also identified opportunities for improving communication within the TCR program, including communication related to policies and procedures for assigning TCRs to Points of Contact, the handling of certain TCRs, and work performed during early stage triage within the Office of Market Intelligence.

In addition, we found that the SEC has initiated a process to plan and develop a future TCR system. As the SEC engages in this planning process, we recommend that it: incorporate lessons learned from the existing system's development history, and consider end-user recommendations when gathering system requirements; and assess the benefits of a reporting function, available to end-users, within the TCR system and, if needed, include this reporting function in the requirements for the new TCR system.

Lastly, we identified two matters that did not warrant recommendations. The first matter involved TCR system downtime, and the second matter related to a consistent upward trend in the volume of TCRs submitted to the agency. We discussed these matters with agency management for their consideration.

We issued our final report on February 24, 2021, and made five recommendations to further strengthen the SEC's TCR program. Because the report contains non-public information about the SEC's TCR program, we released a redacted

version on our website at https://www.sec.gov/files/The-SEC-Can-Further-Strengthen-the-Tips-Complaints-and-Referrals-Program-Report-No-566.pdf.

The SEC's Office of Investor Education and Advocacy Could Benefit From Increased Coordination, Additional Performance Metrics, and Formal Strategic Planning; Report No. 564; January 13, 2021

The SEC's Office of Investor Education and Advocacy (OIEA) plays an important role in accomplishing the SEC's mission of protecting investors. OIEA seeks to provide Main Street investors with the information they need to make sound investment decisions and administers two programs to promote this mission: (1) assisting investors with complaints and questions about the securities markets and market participants, and (2) conducting educational outreach to individual investors.

We conducted this evaluation to assess OIEA's processes and controls for reviewing, referring, and responding to investor complaints and other investor assistance matters, and managing the SEC's investor education and outreach activities in support of the agency's mission and strategic goals and the National Strategy for Financial Literacy (NSFL). We found that OIEA has a well-established system for resolving investor assistance matters, has identified relevant risks, and has developed controls to mitigate those risks. In addition, Office of Investor Assistance staff generally complied with standard operating procedures, and OIEA has taken action to address previously identified investor financial literacy goals and the NSFL. Finally, OIEA's Office of Investor Education obtains some feedback related to its investor education and outreach activities, and previously sought to use a survey in OIEA's outreach activities. Nonetheless, we noted the following:

The Office of Investor Assistance Could Improve Its Communication and Coordination With the SEC's Regional Offices on the Handling of Investor Assistance Matters. Although OIEA's Office of Investor Assistance has a well-established system for resolving investor assistance matters and is required to implement and administer a nationwide system for resolving investor complaints, SEC regional office staff receive and respond to investor complaints and other matters independent of Office of Investor Assistance oversight. Previous OIG audits have consistently reported the need for improved coordination and communication in this area. For example, in September 2011, the OIG recommended, among other things, that OIEA provide ongoing investor assistance training to regional office staff and establish a system for communicating regularly with regional offices to help ensure that investor specialists throughout the SEC provide consistent assistance to investors. Based on our review, it does not appear that OIEA has continued to meet the intent of our 2011 recommendation.

OIEA Should Engage in Formal Strategic Planning To Further Develop Measurable Goals and Detailed Objectives To Inform Investor Education and Outreach Decision-Making. In 2012, OIEA staff completed a statutorily mandated study establishing that, among other things, effective investor education programs have clearly-defined and measurable goals. The nation's Financial Literacy and Education Commission also encouraged its members (including the SEC) to build "relevant, measurable objectives" and evidence-based outcomes to incorporate the NSFL into members' financial education programs and activities. Without engaging in strategic planning to help determine the best course of action to achieve the SEC's investor education and outreach goals and objectives, OIEA increases the risk that its investor education and outreach activities may not fully address the agency's strategic plan or the goals and intent of the national strategy.

OIEA Has Not Developed Methods To Measure the Efficacy of Its Investor Education and Outreach Activities. OIEA's 2012 study established that effective investor education programs use research and evaluation to improve and develop educational materials, and conduct evaluations to measure program efficacy. Moreover, the Financial Literacy and Education Commission's 2020 update to the NSFL states as a best practice that financial education providers should evaluate their programs for impact. By not measuring impact, OIEA potentially limits the effectiveness of its financial education activities and its ability to make data-driven improvements in the future to ensure the organization achieves established goals and objectives.

We issued our final report on January 13, 2021, and made four recommendations, including that OIEA improve communication and coordination with SEC regional offices on investor assistance matters and that OIEA develop and implement formal investor education and outreach strategic planning and methods to measure the impact and

efficacy of its investor education program. The report is available on our website at *https://www.sec.gov/files/The-SECs-OIEA-Could-Benefit-From-Increased-Coordination-Additional-Performance-Metrics-and-Formal-Strategic-Planning-Report-No-564.pdf.*

Ongoing Work

Evaluation of Controls Over the Division of Economic and Risk Analysis Staff Research and Publications

SEC regulations encourage agency staff to "engage in teaching, lecturing, and writing activities." Within the SEC, the Division of Economic and Risk Analysis (DERA) engages across the entire range of the agency's functions, including rulemaking, examination, and enforcement. Its multi-disciplinary analyses are informed by research insights, and they rely on the knowledge of institutions and practices when examining regulatory and risk-related matters. DERA assists the Commission in its efforts to identify, analyze, and respond to economic and market issues, including those related to new financial products, investment and trading strategies, systemic risk, and fraud. As part of their SEC responsibilities and for the benefit of the public, DERA staff (primarily, economists) produce reports and publications that are identified as either SEC products or individual publications. DERA staff may also independently publish personal research outside of their work for the agency.

The SEC OIG initiated an engagement to evaluate the role that the DERA staff's research and publications—including working papers, academic publications, and other published research—play in furthering the mission of the SEC and to determine whether effective controls exist to (a) review and approve staff research and publications, and (b) safeguard SEC nonpublic or other sensitive information used for such activities.

We expect to issue a report summarizing our findings during the next reporting period.

Special Inspector General for the Troubled Asset Relief Program

The mission of the Office of the Special Inspector General for the Troubled Asset Relief Program (SIGTARP) is to prevent and detect fraud, waste, and abuse in the more than $442 billion funded by Congress through the Emergency Economic Stabilization Act (EESA) and $2 billion funded through the Consolidated Appropriations Act of 2016, and to promote economy, efficiency, effectiveness, and accountability in these economic stability programs. SIGTARP prioritizes conducting investigations of suspected illegal activity in, and independent audits of, these EESA long-term economic stability programs.

Background

EESA has two parts:

(1) Short-term Treasury purchases of "troubled assets," which led to investments in banks, insurance companies and automotive companies; and

(2) Long-term programs intended to bring economic stability to the financial industry and communities by protecting home values and preserving homeownership - programs that spent nearly $1 billion in fiscal year 2020, and will continue to operate until at least 2024.

Under these long-term economic stability programs, the Department of Treasury and Fannie Mae (with assistance from Freddie Mac) run a program that funds incentives to more than 150 financial institutions, including some of the largest in our nation, to lower mortgage payments to terms that are affordable and sustainable for homeowners at risk of foreclosure. Treasury also funds grant-like programs administered by housing finance agencies in 19 states. In 2016, Congress provided an additional $2 billion for ongoing housing market needs. This currently includes assistance for homeowners unemployed, underemployed, or suffering other hardships due to the COVID-19 pandemic.

SIGTARP is primarily a federal law enforcement office. SIGTARP investigations have resulted in criminal charges against 456 defendants with a 97% DOJ conviction rate. Courts have sentenced to prison 306 defendants, including 74 bankers. SIGTARP's investigations have also resulted in DOJ, the SEC and others bringing enforcement actions against 25 banks/corporations, including some of the largest financial institutions.

Already, more than $11 billion has been recovered from SIGTARP investigations – a cumulative 30 times return on investment. FY 2020 recoveries were $157.3 million, exceeding SIGTARP's $22 million budget by more than seven times. Recoveries for the first half of FY 2021 are $87 million, exceeding SIGTARP's annual $19 million budget for 2021 by more than four times.

SIGTARP's Select Audit Results (April 1, 2020 to March 31, 2021)

SIGTARP Recommended that Treasury Shift EESA Programs to Address Pandemic-Related Unemployment and Other Hardships

While TARP investments in banks under EESA and other government intervention during the financial crisis shored up banks such that they have weathered the pandemic, large numbers of Americans have suffered personal financial insecurity during the pandemic. Millions lost their job, saw their income reduced or left the workforce as they cared for loved ones or children out of school. Lines at food banks have stretched for miles, and homeowners and tenants faced foreclosure and eviction.

In April 2020, SIGTARP recommended (1) that Treasury put to better use all remaining $685 million in the Hardest Hit Fund, to be used for HHF's traditional form of assistance – mortgage assistance related to unemployment – including the significant recent unemployment caused by the coronavirus. SIGTARP also recommended (2) that Treasury expand HHF by any amounts that will be unspent in TARP's HAMP program for that same purpose, given that Treasury has deobligated $4.86 billion from the HAMP program in fiscal years 2018-2020.[23]

Treasury has been implementing the first recommendation, but not the second. Treasury extended the program deadline. Treasury has approved state finance agencies participating in the Hardest Hit Fund to reopen programs to provide mortgage assistance for unemployed homeowners, and to change program eligibility or other requirements to address pandemic-related hardships. SIGTARP continues to recommend that Treasury shift these funds to open HHF programs. Four states closed HHF in 2020, returning more than $118 million to Treasury.

SIGTARP's Select Investigative Results (April 1, 2020 to March 31, 2021)

Risk of Fraud, Waste, and Abuse by Financial Institutions in the HAMP Program

SIGTARP's top law enforcement priority is unlawful conduct by any of the banks and other financial institutions that received $21.6 billion in HAMP (as of March 25, 2021). HAMP modifies mortgages (interest rates, terms, etc.) for homeowners at risk of foreclosure, to make mortgage payments more affordable and sustainable for homeowners. There are over 650,000 homeowners participating in all 50 states. California, Florida, New York, and Illinois each have more than 30,000 homeowners actively in HAMP. In fiscal years 2020-2021, Treasury distributed $919.5 million under HAMP, including to banks ($91.7 million to Wells Fargo, $51.4 million to JP Morgan Chase, $49.4 million to Bank of America, and $17.7 million to Citigroup), and non-banks (i.e. $233.6 million to Ocwen Financial, $117.7 million to Nationstar). Treasury's payment of EESA to these financial institutions is not automatic, but instead requires that the financial institutions comply with the law and rules of the program. SIGTARP has a number of open confidential investigations. One investigation did have public activity during this reporting period.

On December 7, 2020, the Attorneys General, state financial services regulators, and the Consumer Financial Protection Bureau (CFPB) brought three separate but related enforcement actions, which resulted in part from SIGTARP's investigation, against Nationstar. Nationstar is the fourth largest mortgage servicer in the nation and one of the largest participants and recipients of EESA-funding in the HAMP program. Under HAMP, Treasury pays incentive payments to mortgage servicers and investors to modify mortgages to terms and payments that are affordable and sustainable. The CFPB complaint charged Nationstar with unfair and deceptive practices from 2012-2016. State Attorney Generals filed charges under the applicable state law, some for conduct from 2011-2017.

23 From inception through the end of fiscal year 2020, Treasury has deobligated over $13.16 billion in housing program funds. U.S. Gov't Accountability Off., Rep. No. 21-39, at 8 (December 2020). Deobligated funds languish. HHF maximizes EESA's homeownership preservation mandate, directly helping struggling homeowners.

As stated by Attorneys General in press releases, in 2012, Nationstar began purchasing mortgage servicing portfolios from competitors and grew quickly into the nation's largest non-bank servicer. The lawsuit alleged that as loan data was transferred to Nationstar, borrowers who had sought assistance with payments and loan modifications sometimes fell through the cracks. SIGTARP previously warned Treasury of this very risk. See SIGTARP, "*Homeowners Can Get Lost in the Shuffle and Suffer Harm When Their Servicer Transfers Their Mortgage But Not the HAMP Application or Modification,*" dated October 29, 2014.[24]

The lawsuit alleged other unlawful acts and practices by Nationstar, including:

- Failing to properly oversee and implement the transfer of mortgage loans;
- Failing to appropriately identify loans with pending loan modification applications when a loan was being transferred to Nationstar for servicing;
- Failing to timely and accurately apply payments made by certain borrowers;
- Threatening foreclosure and conveying conflicting messages to certain borrowers engaged in loss mitigation;
- Failing to properly process borrowers' applications for loan modifications;
- Failing to properly review and respond to borrower complaints;
- Failing to make timely escrow disbursements, including the failure to timely remit property tax payments;
- Failing to timely terminate borrowers' private mortgage insurance; and
- Collecting monthly modified payment amounts on certain loans where the amounts charged for principal and interest exceed the principal and interest amount contained in the trial plan agreement.

Nationstar resolved the charges by agreeing to enhance policies and processes and paying $86.3 million, including redress to more than 115,000 harmed homeowners and a $1.5 million civil penalty. This included payments of:

- $16,242,809 to in-flight modification borrowers;
- $9,728,960 + $13.5 million to modification payment increase borrowers;
- $93,307 to tax disbursement borrowers;
- $10,832,738 to PMI borrowers;
- $20,825,235 + more than $2 million to escrow borrowers; and
- $100,000 to unlawful foreclosure borrowers.

24 Specifically, SIGTARP's 2014 special report included a highlight that Nationstar's growth rate in mortgages serviced neared 400% in only three years. This increase was largely due to transfers. SIGTARP called upon Treasury at the time to protect borrowers by reporting transfers as part of public servicer assessments. The recommendation included publishing information regarding transfers to non-bank servicers, like Nationstar.

From 2014-2016, Treasury assessed Nationstar itself as "Substantial Improvement Needed" in second and third quarters of 2015, and withheld servicer incentives during the latter. Nationstar again ranked "Substantial Improvement Needed," in the fourth quarter of 2016. Treasury's assessments missed the opportunity to identify publicly those servicers, or investors, that transferred homeowners' mortgage servicing to Nationstar.

To put this figure in perspective, Treasury has distributed $1.7 billion to Nationstar under HAMP and related programs, including $117.7 million in fiscal year 2020-2021, making Nationstar the third largest current recipient of EESA funds in HAMP.

Justice for Defendants Convicted of Scamming Homeowners Who Were Seeking Foreclosure Assistance Through HAMP

SIGTARP has caught 121 scammers who were convicted for defrauding nearly 31,000 homeowners nationwide seeking foreclosure relief through HAMP. Courts sentenced 98 scammers to prison.

Judge Sentences to 12 Years in Prison and 5 Years in Prison the Co-Owners of U.S. Homeowners Relief for a Nationwide $3.5 Million Fraud Scheme Targeting More Than 250 Homeowners Seeking Loan Modifications, Including Through HAMP

In August 2020, a federal court sentenced Aminullah Sarpas to 12 years in prison after a jury convicted him on 10 counts of conspiracy and mail fraud, and sentenced co-owner Samuel Paul Bain, who plead guilty, to 5 years in prison. In July 2014, SIGTARP agents and our law enforcement partners arrested Sarpas and Bain, co-owners of U.S. Homeowners Relief, a business that from 2008 to 2010 operated as a telemarketing "boiler room" in California that pitched loan modification services to distressed homeowners. Sarpas and Bain demanded up-front fees of up to $4,200 from homeowners in exchange for false promises of securing mortgage loan modifications on their behalf, touting a 97 percent success rate in securing modifications, and advertising money-back guarantees.

The company's marketing materials implied they were affiliated with HAMP's umbrella program, the Making Home Affordable Program, making specific reference to the government website, www.MakingHomeAffordable.gov, and displayed official Government logos. Telemarketers told consumers that their mortgage relief was part of the "Obama Act." The defendants advised customer victims to stop making mortgage payments and not have contact with their lender.

The vast majority of more than 250 victims received no favorable loan modifications, instead losing their payments to the $3.5 million scam. Several of the victims learned from their mortgage lenders that the defendants' companies had never made any contact on the homeowners' behalf.

Many victims lost their homes to foreclosure. When pressure from customer complaints to the Better Business Bureau or state regulators grew, the defendants would shut down the company and open a new company to continue the scheme. Victims included homeowners in California (Ramona, San Diego, Palm Desert, Carson, Long Beach, Los Angeles); Nevada (North Las Vegas, Sparks, Henderson); Florida (Miami, Jacksonville, Launderhill); Hawaii (Waipahu, Ewa Beach) Newark, Delaware; Ohio (Dayton, Massilon); Chaska, Minnesota; Phoenix, Arizona; and Corpus Christi, Texas. SIGTARP was joined in the investigation by the U.S. Postal Inspection Service and the Criminal Division of the Internal Revenue Service. The U.S. Attorney's Office for the Central District of California is prosecuting the case.

Conviction Upheld for Lawyer Participating in a Multimillion-Dollar Wire and Bank Fraud Conspiracy, Including Defrauding Those Seeking Assistance from HAMP

On June 17, 2020, the United States Court of Appeals for the Second Circuit upheld the conviction of lawyer Rajesh Maddiwar. After a trial in July 2019, a federal court convicted Maddiwar of conspiracy to commit wire fraud and bank fraud. The trial court sentenced Maddiwar to five years in prison, and the appellate court's Summary Order held that, upon de novo review of evidence sufficiency, Maddiwar "knew of the existence of the scheme alleged in the indictment and knowingly joined and participated in it."

According to the complaint, since at least 2013, Alvarenga, Maddiwar, and Meiri defrauded distressed homeowners throughout the Bronx, Brooklyn, and Queens, New York. Alvarenga, Maddiwar, and Meiri falsely represented to these homeowners – some of whom were elderly or in poor health – that they could assist them with a loan modification or similar relief from foreclosure that would allow the homeowners to save their homes. But rather than actually

assisting these homeowners, the defendants deceived them into selling their homes to Launch Development LLC (Launch Development), a for-profit real estate company also affiliated with the defendants.

Alvarenga, Maddiwar, and Meiri lured victims through the Homeowners Assistance Service of New York (HASNY), which purported to provide assistance to homeowners who were seeking to avoid foreclosure of their homes. As part of the scheme, Meiri directed employees of Launch Development, a company owned in part by Meiri, to solicit owners of distressed properties and invite them to meet with HASNY representatives so that they could learn more about avoiding foreclosure and saving their homes. When a homeowner arrived at the HASNY office, he or she met with Alvarenga, who typically advised the homeowner that HASNY could assist him or her with a loan modification. In still other cases, Alvarenga advised the homeowner that a loan modification could not be completed, but that the homeowner could engage in a type of short sale in which the homeowner would sell the property to a third party, Launch Development, and then within approximately 90 days arrange for a relative of the homeowner to repurchase the property from Launch Development. Alvarenga typically explained that the homeowner could remain in his or her home throughout the entire process. Alvarenga then typically scheduled a closing at which the homeowner would meet with Maddiwar, who was described as the homeowner's attorney for the transaction.

At the closing, a homeowner who had been led to believe that he or she was about to receive a loan modification or transfer his or her property to a trusted relative was encouraged to sign documents presented by Maddiwar, which in some cases were blank. Unbeknownst to the homeowners, by signing the documents, they were selling to Launch Development the homes they had hoped to save. Homeowners often were then forced to vacate their homes soon thereafter.

SIGTARP agents participated in the arrests of Maddiwar, and others including Owen Reid, Mario Alvarenga, Herzel Meiri and Samantha Boubert. The court sentenced Herzel Meiri and Amir Meiri, the owners of Launch Development, to ten years in prison, and five years in prison. SIGTARP was joined in the investigation by the FBI and the New York State Department of Financial Services. The U.S. Attorney's Office Southern District of New York prosecuted the case.

SIGTARP Uses an Innovative Intelligence-Based System to Find Crime in Financial Institutions

SIGTARP continued its longstanding record of holding financial institutions and bankers accountable. SIGTARP supports the Justice Department's prosecutions of individuals and entities investigated by SIGTARP. SIGTARP investigators use an innovative intelligence-based strategy to find crime. SIGTARP uncovered and caught a new type of crisis-related crime in banks – bankers who cooked the books and lied to regulators and investors to hide bad loans and the bank's declining condition. When first created, SIGTARP found that financial institution fraud had evolved from the insider self-dealing fraud that marked the savings and loan crisis. Fraud schemes were now designed to escape detection by traditional fraud identification methods of self-reporting and regulator referrals. As a result, SIGTARP created an intelligence-driven approach and leveraged technological solutions to discover insider crimes at banks that previously went undetected. SIGTARP also caught bankers who personally profited from fraudulent loans and used TARP to hide their fraud. Additionally, SIGTARP uncovered fraudulent sales practices related to residential mortgage backed securities (RMBS). TARP's program known as PPIP involved the purchase and sale of RMBS.

Mexican National Sentenced to Prison in Operation Phantom Bank After RICO Conviction That Included Criminal Enterprise: (1) to Launder International Narcotics Trafficking Proceeds Including Through TARP Bank; and (2) to Buy TARP Bank to Conceal Money Laundering. Co-conspirator of Banker also Sentenced to Time Served in Prison.

In January 2021, a court sentenced Pablo Hernandez from Mexico to 7 years 3 months in prison after his conviction under the Racketeer Influenced and Corrupt Organizations (RICO) Act. The California Department of Justice in 2014, in a separate investigation, identified Hernandez as a drug broker and money launderer for a drug trafficking organization considered to be an extension of the Sinaloa Cartel.

The Department of Justice charged 25 defendants in Operation Phantom Bank across six indictments. Hernandez, Emilio Herrera, and Saigon National Bank CEO Tu Chau ("Bill") Lu were charged in a December 2015 indictment. SIGTARP participated in their arrest. They were charged with violating the RICO Act by playing key roles in a series of schemes to launder drug proceeds. At the center of the schemes is CEO Lu, 71, of Fullerton, California, who was CEO and President of Saigon National Bank from 2009 through January 2015. Saigon National Bank was in TARP from December 2008 until April 2017.

The indictment alleged that Lu and the other five defendants were members of a criminal organization that was involved in narcotics trafficking and international money laundering in countries that included the United States, China, Cambodia, Lichtenstein, Mexico, and Switzerland. Lu allegedly used his insider knowledge, position as an official at Saigon National Bank, and network of connections to promote and facilitate money laundering transactions involving members and associates of the enterprise. Several members of the organization established or engaged in separate money laundering schemes, but all the defendants allegedly worked with Lu, through him or at his direction.

Federal Agents introduced a confidential source to Hernandez and co-defendant Emilio Herrera (who died post-indictment). Hernandez and Herrera sought to hire the government's confidential source to launder significant amounts of drug money from Mexico for their clients. Hernandez admitted having discussions with the confidential source about laundering cash for the Sinaloa Cartel for a fee. Hernandez also sought, along with co-defendant Herrera, to buy Saigon National Bank with the help of CEO Lu as another way to launder cash from Mexico.

In August 2011, at a restaurant in Westminster, California, Saigon National Bank CEO Lu told Hernandez that he must listen to Lu about how to conduct the money laundering transactions so as to avoid the closure of any account used to receive cash deposits. At that same meeting, in discussing laundering drug money, Hernandez told the confidential source that his clients would like to deposit money each day in the United States in exchange for the confidential source sending the money back to Mexico for a fee. When CEO Lu suggested sending the wire transfer to Panama rather than Mexico, Hernandez said that Panama was not an option because his associates had previously lost $100 million in drug money that was confiscated in Panama.

In the fall of 2011, CEO Lu met with Hernandez at Saigon National Bank to make sure that Hernandez's name was not on financial watch lists that would prohibit Hernandez from opening a bank account. In October 2011, CEO Lu told the confidential source that $2 million had already been laundered through Saigon National Bank and that he was worried about the government coming in for an audit.

In August 2012, Hernandez said they had tried to launder money through Saigon Bank, but that when the account was closed, his associates had previously tried to buy Saigon National Bank, and that Bill Lu had facilitated their purchase of one million shares. Hernandez admitted that the purpose of buying the bank was to launder money. In August 2012, co-defendant Herrera stated that he knew people who had $5 million in cash in the United States, and asked whether that cash could be used to become one of the shareholders in Saigon National Bank, in order for him and Hernandez to continue their money laundering.

Additionally, in June 2020, a federal court sentenced co-conspirator of a banker Mina Chau to time served in prison. She had pleaded guilty to conspiracy to commit money laundering. Chau agreed with co-defendant Eddie Kim and her unindicted cousin to provide cashier's checks in exchange for cash. Chau was involved in three money laundering transactions, laundering what the Department of Justice called "stacks and stacks of cash" that she knew did not belong to her over the course of six months in ever-increasing amounts. Chau was convicted of laundering $1.25 million, excluding money laundering fees paid to co-defendant Kim.

SIGTARP was joined in the investigation by the Federal Bureau of Investigation and the Criminal Division of the Internal Revenue Service. The U.S. Attorney's Office for the Central District of California is prosecuting the case.

Wall Street Supervisory Bond Trader at Nomura Securities Sentenced for Conspiracy to Commit Securities Fraud and Wire Fraud for Fraudulent Sales Practices in Sale of Residential Mortgage Backed Securities. Fraud at Nomura Included 161 Trades with Losses of $15.1 Million, Including Trades in TARP's PPIP Program. SEC Brought Parallel Civil Charges Against Nomura Traders and a $26.5 Million Case Against Nomura.

In December 2020, Michael Gramins, a former supervisory trader with Nomura Securities International was sentenced after his conviction at trial for fraud in the sale of residential mortgage backed securities (RMBS). The court sentenced Gramins to six months home confinement, probation, and 300 hours community service. Nomura was a securities and investment banking company that, among other things, engaged in the purchase, sale and brokering of RMBS. Gramins was the Executive Director of Nomura's RMBS desk in New York. He principally oversaw Nomura's trading of bonds comprised of subprime and option ARM loans.

During the financial crisis, the RMBS market froze, and in 2009, the federal government created TARP's Public Private Investment Partnerships (PPIP) program to buy and sell RMBS securities to help unfreeze the markets. RMBS is an opaque market. Because it is not on an exchange, buyers and sellers do not know the fair market value of RMBS bonds. Broker-dealers like Nomura facilitated trades between buyers and sellers of RMBS, including trades in the PPIP program.

In conducting oversight over the PPIP program, SIGTARP became the first to uncover a securities fraud scheme by some Wall Street bond traders in RMBS sales practices. In January 2013, SIGTARP arrested a Wall Street trader at Jefferies who was charged by the United States Attorney for the District of Connecticut with fraudulent sale's practices in RMBS designed to increase compensation. The Securities and Exchange Commission brought a parallel civil action. Following this arrest, Special Inspector General Christy Romero and United States Attorney David Fein requested that broker-dealers review trades in the PPIP program and self-report if it was discovered their traders had engaged in similar conduct as that charged in the January 2013 indictment. Various firms self-reported to SIGTARP, including Nomura.

Nomura traders, including Gramins, often attempted to match a prospective buyer of a particular RMBS with a prospective seller of that RMBS (and vice versa), reaping a small commission in return. These are called "order trades." Gramins and Nomura also engaged in "BWIC" ("Bids Wanted in Competition") trades, wherein a putative seller sends a list of bonds potentially for sale to multiple broker-dealers, who then solicit expressions of interest and price ranges from potential buyers and place a bid in the auction for that particular security. Both order and BWIC trades fall within the "riskless" category because the broker-dealer has the potential buyer and potential seller already matched up at the time of the transaction. In both contexts, the broker-dealer typically obtains compensation for its "matching" efforts by selling the bond for slightly more than it paid for it. Industry participants refer to this difference as "commission," "pay on top," or "spread," and often negotiate the amount of the difference explicitly with their broker-dealer.

Gramins, his supervisor Ross Shapiro and a third trader Tyler Peters were indicted on September 3, 2015. A federal jury convicted Gramins of conspiracy after a six-week trial in June 2017, was a hung jury for Ross Shapiro, and acquitted Peters. The U.S. Attorney's office entered into a plea agreement with a junior trader who testified at trial and several Non-Prosecution Agreements with other Nomura traders, some of whom testified at trial.

Between 2009 and 2013, Gramins engaged in a scheme and conspiracy to commit wire and securities fraud. Time and again, he lied to Nomura's customers during negotiations to buy and sell bonds in the opaque RMBS marketplace, inducing them to buy at higher prices or sell at lower prices than they would have otherwise. Gramins' motive was not complex—he did it to make more money for Nomura's RMBS desk and, ultimately, for himself. Taking advantage of the opaque RMBS market, he expected to get away with lying. The testimony at trial showed that Gramins was motivated to lie in order to make more money for the RMBS desk, which factored into his compensation.

There was trial testimony that Gramins continued to use the same tactics after the Jefferies indictment in January 2013 but took steps to conceal his conduct. In early February 2013, about a week after the indictment of the Jefferies trader, Nomura scheduled a compliance training session for traders and salespeople in its securitized products groups, which Gramins attended specifically to discuss the conduct at issue in the indictment. A Nomura employee

testified at trial that the "general focus of the session was if you say something, make sure it's accurate." The training session also operated as a "refresher" on principles from Nomura's compliance manual, including its prohibitions on making misrepresentations to clients. A junior analyst testified at trial that there was an increased use of the phone after the Jefferies indictment by everyone on the trading floor and affirmed that the head of compliance told employees to use the phones more, which at the time were not recorded.

Gramins' crime did not stop with his own conduct—he trained and helped others to do the same thing, ultimately resulting in millions of dollars of loss to victims. A former vice president at Nomura testified that he and other Nomura RMBS traders "would lie about where we were actually buying or selling securities to clients" in order to "increase the profit for Nomura." The Vice President testified that such misrepresentations induced Nomura's counterparties to adjust their bid or offer prices because counterparties "typically only had the information that we were giving them regarding price" and thus "basically had to take our word when it came to the actual price on the bond." The former Vice President testified that he had originally learned these deceptive tactics from Gramins and that he had observed Gramins engage in them. The former Vice President and another associate testified that Nomura's RMBS traders would engage in these tactics to defraud their clients "every time the opportunity presents," with the associated testifying that he believed it to be "on a daily basis."

One former junior analyst at Nomura, explained that Gramins and others would "misrepresent...prices to clients," for instance by "tell[ing] the seller that we were seeing a bid that was lower than what the bidder had actually bid" or "tell[ing] a bidder that we had an offer that was higher than the offer actually was." That junior analyst testified that the effect of these representations "was to get either one side or both sides to lower their offer [to sell] or increase their bid [to buy]," thereby "increas[ing] the spread or money that Nomura earned on the trade." He testified that Gramins taught him to engage in these deceptive tactics and that he had observed Gramins engaging in them himself.

In total, SIGTARP's investigation has revealed that the conspiracy executed 161 fraudulent trades, which caused a total of $15,262,651.93 in fraud loss, including in the PPIP program. These figures are limited to fraudulent trades negotiated by the conspirators in writing or over a recorded phone line.

This case was investigated by SIGTARP, the Federal Bureau of Investigation, the U.S. Department of Labor's Office of Inspector General, Office of Labor Racketeering and Fraud Investigations, and the Federal Housing Finance Agency's Office of Inspector General. The criminal case was prosecuted by the United States Attorney's office for the District of Connecticut.

In a parallel civil case, the Securities and Exchange Commission also charged Gramins and Shapiro, as well as others from Nomura. Shapiro settled with the SEC. The SEC barred Shapiro from the industry for two years and fined him $200,000. The SEC also charged Nomura with failure to supervise its traders in July 2019. Nomura resolved the SEC's charges by paying approximately $25 million in restitution to customers for its failure to adequately supervise traders in mortgage-backed securities, and an additional $1.5 million in penalties. The SEC noted that Nomura had engaged in substantial cooperation including improving its surveillance procedures and other internal controls.

Chief Executive Officer of Failed TARP Bank in Maryland Sentenced to Two Years in Prison for Fraud Conspiracy and Bribery, Becoming the 74th Banker Sentenced to Prison as a Result of SIGTARP's Investigation. Treasury Wrote Off More Than $11 Million in TARP After the Bank Filed Bankruptcy.

Co-Conspirator Straw Buyer Sentenced to Time Served in Prison.

On November 6, 2020, a federal court sentenced Mary Halsey, former CEO and President of Cecil Bank of Rising Sun, Maryland, to two years in prison, followed by five years of supervised release. She was ordered to pay $145,000 in restitution. Halsey was convicted in July of secretly orchestrating a fraud by using a straw buyer to acquire a house foreclosed upon by the bank, thereby acquiring the house for herself at a price significantly below its market value, and taking the house off of the bank's growing list of owned properties (OREOs) after the bank examiners expressed concern about OREOs. She lied to the bank's board of directors and a Federal Reserve Bank (FRB) examiner about her purchase. In February 2021, the court also sentenced Halsey's co-conspirator Daniel Whitehurst, the straw buyer, to

time served in prison, two years supervised release, and $72,500 in restitution. In a quid pro quo transaction, Halsey had the bank provide Whitehurst a $650,000 bank line of credit.

Halsey picked the worst time in Cecil Bank's history to devise and carry out her scheme. When Halsey started her fraud scheme in 2012, the bank had 89 employees and 11 branches throughout Maryland. Cecil Bank's parent company traded on NASDAQ. However, due to a poor economy and bad banking practices, by 2012 the bank had fallen on difficult times and it was in serious financial distress. In 2009, regulatory examination by FRB reflected multiple concerns about the bank's financial condition and its lack of risk management. The bank had experienced six straight quarters of net losses, and OREOs represented over nine percent of the bank's total assets.

Treasury invested $10.5 million in TARP in the bank in a program limited to "healthy banks." By October 12, 2011, the bank's condition had deteriorated even more and was labeled "critically deficient." Improperly accounting for the sale of OREOs was one of the many problems identified in the report, along with deficient liquidity.

Halsey had been tracking and controlling the bank's foreclosure process in ways that guaranteed the property would be available to her at a greatly reduced price. Halsey also knew the bank had ways to dispose of OREO properties it wanted off its books without using a realtor. Halsey chose to reduce the number of employees who might scrutinize the steps she planned to take to effect the straw sale of the house. Halsey emailed an employee managing OREO properties and told him not to list the property with a realtor. She falsely claimed her son had a friend who might be interested in buying it. She recruited Whitehurst at a dinner where he was requesting a line of credit. She also gave money to Whitehurst to make improvements that she wanted. She planned to wait a period of time then buy the house from Whitehurst on the grounds that she liked his renovations.

Treasury wrote off approximately $11 million from its TARP investment in Cecil Bank after it filed for bankruptcy in 2017. SIGTARP was joined in the investigation by the Federal Housing Finance Agency Office of the Inspector General, the Federal Deposit Insurance Corporation (FDIC) Office of the Inspector General, and the Small Business Administration Office of the Inspector General. The U.S. Attorney for the District of Maryland prosecuted the case.

Senior Loan Officer and Executive Vice President in TARP Bank in Georgia and Two Co-Conspirators Indicted for Fraud

In February 2021, Michael Craig Brewster of Huntsville, Alabama, former Senior Loan Officer and Executive Vice President at River City Bank in Rome, Georgia, was indicted on charges of bank fraud conspiracy, bank fraud, and false statement in a loan application. Co-conspirators Edmond Cash and LaDonna Barton were also indicted. River City Bank failed to pay nine quarterly dividend payments to Treasury while in TARP, totaling more than $1 million. Treasury also wrote off $826,721 after auctioning off its preferred shares at a loss. According to the indictment, Brewster and his co-conspirators were involved in developing and investing in residential neighborhood construction projects, including in the Longbranch Lakes development in Spencer, Tennessee. Brewster purchased and sold property in the development. Cash was the lead developer for Longbranch Lakes and Barton was his company's employee and investor in the development. Cash and his business partners allegedly were past due on several loans taken out from River City Bank.

According to the indictment, Brewster, Cash, and Barton falsely applied for a bank loan for Barton to purchase two parcels of property when the true purpose of the loan was for Cash to make overdue payments on loans that he and his business partners owed to the bank. One day after the bank disbursed the loan proceeds to Barton, Cash allegedly made past due payments on loans he and his business partners owed to the bank, paid operating costs for Longbranch Lakes, then he and Barton pocketed the remaining loan proceeds.

Due to his position at the bank, Brewster is alleged to have been able to push the loan application through for approval despite knowing of the false statements in the application. SIGTARP was joined in the investigation by the FDIC Office of the Inspector General. The U.S. Attorney for the Northern District of Georgia is prosecuting the case.

Owner of Real Estate Development Company in Illinois Convicted After Being Charged in 2014 with Defrauding Bank While it was in TARP in a Construction Loan to Build Chicago Condominiums

On November 13, 2020, See Y. Wong, the owner of Emerald Homes, an Illinois real estate development company, was convicted of wire fraud for defrauding TARP recipient Cathay Bank. In December 2008, Treasury invested $258 million in TARP in Cathay Bank. Beginning in the summer of 2009 through the fall of 2011 while the bank was in TARP, Wong defrauded the bank in a $13.7 million loan to finance construction of a condominium project called Canal Crossing in Chicago. Cathay Bank lost approximately $1.8 million. The bank was not able to repay TARP until 2013.

Cathay Bank paid out more than $4 million under the loan based on false representations by Wong. The bank's contract with Wong required that he put buyer deposits into an escrow account at the bank. Instead, Wong misappropriated buyer deposits to fund his portion of construction costs and a personal loan to a friend, knowing that the bank would not have made payments if they had known the truth. Wong defrauded potential victim buyers and the bank by offering buyers 40-50 percent discounts if they paid upfront and altering the documents he gave to the bank to hide the discount. Wong instructed certain potential victim buyers that they could not disclose the discount they were getting to anyone so that he could continue to hide the vastly discounted purchase from the bank.

SIGTARP was joined in the investigation by the FBI. The U.S. Attorney's Office for the Northern District of Illinois is prosecuting the case.

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 1,200 financial institutions.

Introduction

Treasury 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), the Troubled Asset Relief Program (TARP), and those programs and activities under the jurisdictional oversight of the Special Inspector General for Pandemic Recovery (SIGPR). Treasury OIG also keeps the Secretary of the Treasury and Congress fully informed of problems, deficiencies, and the need for corrective action. 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.

Treasury OIG has oversight responsibility for OCC, which supervises approximately 821 national banks, 284 federal savings associations, and 53 federal branches of foreign banks. The total assets under OCC's supervision are $14.1 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, (2) the Federal Insurance Office, (3) the Office of Minority and Women Inclusion within Treasury's Departmental Offices, 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 and the Federal Home Loan Mortgage Corporation under the Housing and Economic Recovery Act of 2008, to include Treasury's Senior Preferred Stock Purchase Agreements established for the purpose of maintaining the positive net worth of both entities.

Treasury OIG is also responsible for audit and investigative oversight of Treasury programs providing financial assistance to address the economic impacts of Coronavirus Disease 2019 (COVID-19). Since March 2020, more than $645 billion of financial assistance, overseen by Treasury OIG, has been authorized by the *Coronavirus Aid, Relief, and Economic Security Act* (CARES Act)[25] enacted on March 27, 2020; the *Consolidated Appropriations Act, 2021*[26] enacted on December 27, 2020; and the *American Rescue Plan*[27] enacted on March11, 2021. Through these pieces of legislation, Treasury provides financial assistance to the transportation industry for the continuation of salaries and benefits; to all 50 States, units of local government, U.S. territories, and tribal governments to provide economic relief including rental and mortgage assistance and support for small businesses; and to community development financial institutions to inject emergency capital investment into low-income communities to address the ongoing pandemic.

25 Public Law 116-136 (March 27, 2020).
26 Public Law 116-260 (December 27, 2020)
27 Public Law 117-2 (March 11, 2021)

Treasury established the Office of Recovery Programs to administer the pandemic relief funds. The enormity of these programs requires continued coordination between the Office of Audit, the Office of Investigations, and the Office of Counsel to handle complaints concerning hundreds of recipients and sub-recipients that received financial relief.

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 29, 2020, the Inspector General reported five management and performance challenges that were directed towards financial regulation and economic recovery. Those challenges are discussed below and include: COVID-19 Pandemic Relief, Operating in an Uncertain Environment, Cyber Threats, Anti-Money Laundering and Terrorist Financing/Bank Secrecy Act Enforcement, and Efforts to Promote Spending Transparency and to Prevent and Detect Improper Payments.[28]

COVID-19 Pandemic Relief

As discussed above, Treasury OIG is responsible for audit and investigative oversight of Treasury programs providing more than $645 billion of financial assistance authorized by legislation since March 2020 to address the economic impacts of COVID-19. These and other programs throughout the government, which Treasury has provided assistance in implementing, have and will continue to bring significant challenges to the Department. As of the time of the October 2020 memorandum, Congress had passed legislation to address the impact of the COVID-19 health crisis and the economic fallout, including the Coronavirus Preparedness and Response Supplemental Appropriation Act of 2020[29] providing emergency funding to address health and medical care; the Families First Coronavirus Response Act[30] addressing the financial stress of individuals and households; and the CARES Act, discussed above, providing health and economic relief to hospitals and healthcare providers, individuals and households, businesses and employees, as well as, states, territories, local and tribal governments, and federal agencies, among other things.

Treasury has been instrumental in implementing and/or supporting other federal agencies in implementation of economic relief provisions of the CARES Act. For example, to assist individuals and households, Treasury directed Economic Impact Payments (EIPs) to workers and households through the IRS. Through the IRS, Treasury also implemented the Employee Retention Tax Credit and Payroll Tax Deferral CARES Act provisions to protect workers and jobs. Treasury also assisted the Small Business Administration in carrying out the Paycheck Protection Program and the Economic Injury Disaster Loans authorized by the CARES Act. In addition to all this, Treasury established programs to preserve airline industry jobs, provide liquidity to the financial sector, and disburse payments to other levels of government within the United States impacted by the increasing costs caused by the COVID-19 pandemic.

Additionally, the Emergency Relief and Taxpayer Protections (commonly referred to as Section 4003 of the CARES Act) provisions authorized Treasury to make up to $500 billion in loans, loan guarantees, and other investments to eligible businesses, States, and municipalities. Up to $46 billion of this amount was made available as loans and loan guarantees to air passenger carriers, air cargo carriers, businesses engaged in national security and up to $454 billion was made available as loans, loan guarantees and other investments in programs and facilities of the Board of Governors of the Federal Reserve System to provide liquidity to the

28 The Treasury Inspector General's memorandum included one other challenge not directly related to financial regulation and economic recovery: Information Technology Acquisition and Project Management. The memorandum also discussed concerns about three matters: the coin redemption program at the United States Mint, managerial cost accounting, and internal control issues at the Bureau of Engraving and Printing.

29 Public Law 116-123 (March 6, 2020).

30 Public Law 116-127 (March 18, 2020).

financial system.[31] The Emergency Relief and Taxpayer Protections provisions also authorized the establishment of the Special Inspector General for Pandemic Recovery (SIGPR) within Treasury to oversee the $500 billion in loans, loan guarantees, and other investments provided by Treasury.

Although some of the aforementioned legislative provisions do not fall under the oversight jurisdiction of Treasury OIG, the payment work streams and mechanisms administered by the Bureau of the Fiscal Service (Fiscal Service) do. In the context of this overarching challenge, Treasury OIG recognizes the breadth and scope of Treasury's responsibilities as it impacts programs, operations, and activities regardless of jurisdictional oversight boundaries.

For example, to maintain pay and benefits of airline industry workers, Treasury implemented the Air Carrier Worker Support (hereinafter referred to as the Payroll Support Program) to provide direct financial assistance for passenger air carriers, cargo air carriers, and contractors. Financial assistance is to ensure the continuation of workers' payroll and benefits with the stipulation that employees are not involuntarily furloughed and do not receive reductions in pay and benefits. Using existing resources and contractor support, Treasury quickly stood up the Payroll Support Program to establish, among other things, the application requirements for requesting financial assistance, terms and conditions for receiving financial assistance, and subsequent compliance monitoring of air carriers and contractors.

Treasury also consults with the Department of Transportation (DOT) on the larger air carriers that report financial information to DOT on a regular basis (referred to as 241 carriers[32]). The CARES Act requires Treasury OIG to audit the certifications of sworn financial data submitted to Treasury by passenger and cargo carriers and contractors that do not report to DOT (referred to as non-241 carriers). While Treasury OIG has ongoing audits of Treasury's program implementation and non-241 carriers' certifications submitted to Treasury, it is incumbent upon the Department to establish and maintain strong internal control over recipients' compliance with signed terms and conditions for receiving financial assistance. That is, Treasury's compliance monitoring function is essential to ensuring that recipients use funds for the continuation of salaries and benefits as intended.

In addition, the $150 billion Coronavirus Relief Fund, established under Title VI of the Social Security Act, as amended by Title V of the CARES Act, has been a large endeavor for Treasury. The Department has been responsible for making direct payments to States, units of local government, the District of Columbia, U.S. Territories, and Tribal governments. Furthermore, disbursement of funds was a complicated undertaking given the number of recipients at varying levels of government and other payment requirements of the CARES Act. The CARES Act created a unique challenge in distinguishing between the programmatic administrative responsibility for payments made from the Coronavirus Relief Fund and Treasury OIG's independent oversight. Although Treasury was authorized to make payments, the CARES Act assigned Treasury OIG with responsibility for monitoring and oversight of the receipt, disbursement, and use of funds. Additionally, Treasury OIG was given authority to recoup funds if it is determined that recipients fail to comply with uses of funds for COVID-19 related costs under Section 601 (d), "Uses of Funds," of the Social Security Act, as amended.[33] [34]

Given the direct oversight authorities of the Treasury OIG, the Department did not establish an administrative program to ensure recipient compliance. Recipients were not bound to any terms and conditions for the

31 The *Consolidated Appropriations Act, 2021* (December 27, 2020), eliminated Treasury's ability to make new loans and investments under Section 4003 of the CARES Act, effective January 9, 2021. In addition, the statute prohibited the Federal Reserve from engaging in further lending or extensions of credit after December 31, 2020 through facilities in which Treasury made investments under Section 4003 of the CARES Act other than a loan submitted on or before December 14, 2020, to the Main Street facilities for the sale of a participation interest in such loan, provided that the Main Street facilities purchase a participation interest in such loan on or before January 8, 2021. After December 31, 2020, the Federal Reserve is also prohibited from modifying the terms and conditions of any of the facilities in which Treasury made investments under the CARES Act.

32 14 CFR Part 241, Uniform System of Accounts and Reporting for Large Certified Air Carriers.

33 Section 601 (d), Use of Funds, " to cover only those costs of the State, Tribal government, or unit of local government that (1) are necessary expenditures incurred due to the public health emergency with respect to COVID–19; (2) were not accounted for in the budget most recently approved as of the date of enactment of this section for the State or government; and (3) were incurred during the period that begins on March 1, 2020, and ends on December 30, 2020."

34 The *Consolidated Appropriations Act, 2021*, Division N, Title X, Miscellaneous, amended Title VI of the Social Security Act to extend the Coronavirus Relief Fund covered period to December 31, 2021.

receipt of funds. Treasury OIG reported this in its first audit of the Coronavirus Relief Fund regarding the lack of terms and conditions and accountability and transparency of funds.[35] While this is unusual for a Federal agency that administers financial assistance programs, Treasury officials stated commitment to supporting Treasury OIG's oversight role for ensuring transparency, accountability, and adherence to all statutory requirements and will continue to collaborate with Treasury OIG to ensure compliance by recipients. This continued collaboration is critical for overseeing such a large and widely dispersed recipient population given the challenges of defining and interpreting eligible uses of Coronavirus Relief Fund proceeds. That said, it is crucial that the Department maintain its fundamental role to establish and interpret policy over the uses of funds.

As recipients are still in the process of using these funds, Treasury OIG anticipates that questions will continue to arise that will require interpretation and consultation with Treasury's Coronavirus Relief Fund guidance and Frequently Asked Questions. Providing as much clarity as possible over allowable uses of Coronavirus Relief Fund proceeds is essential for ensuring recipients understand the compliance requirements and are accountable and transparent in how they report uses of funds. As part of its compliance monitoring and oversight function, Treasury OIG established a portal using GrantSolutions[36] for recipients to report their uses of funds on a quarterly basis starting September 2020 through the quarter ending September 2022. Recipient data is reported to the newly created Pandemic Response Accountability Committee for display on its website (https://pandemicoversight.gov).

Furthermore, with enactment of additional legislation, such as the American Rescue Plan of 2021, Treasury must continue to navigate through this challenging time and be prepared to administer these fast-paced relief packages. To date, Treasury has had to leverage its existing workforce and hire contractors to address the demands of the pandemic related workload. That said, there was reported strain associated with working remotely while managing normal responsibilities and additional work due to the COVID-19 pandemic. Going forward, Treasury may experience difficulties in balancing its new responsibilities and workloads while managing several ongoing challenges.

Operating in an Uncertain Environment

The COVID-19 outbreak presented unique complexities for Treasury to include, among other things, implementing measures for the health and safety of its workforce, as well as, administering more than $2 trillion in financial assistance under the CARES Act. Despite these challenges, Treasury responded with limited onsite staff from within Treasury, detailees from other Federal agencies, and outside contractors. Treasury acted quickly to work with its business partners[37] to prepare disbursements of more than 160 million of EIPs totaling over $267 billion within two months after the passage of the CARES Act; $28 billion in financial assistance under the Payroll Support Program to hundreds of companies in the aviation industry; up to $500 billion in loans to the aviation industries ($46 billion administered by Treasury, and the remainder through the Federal Reserve); $150 billion to state, local, territorial, and tribal governments; as well as working closely with the Small Business Administration to disburse up to $659 billion to over 5 million small businesses through the Payroll Protection Program and $190 billion through the Economic Injury Disaster Loan program.

In addition to its normal payment operations and the delivery of EIPs, Fiscal Service facilitated the delivery of billions of dollars in other CARES Act funding and other urgent agency payments as a result of the pandemic in the most efficient and effective manner. Fiscal Service is also leveraging existing resources and processes in the disbursement of payments related tothe Payroll Support Program and Coronavirus Relief Fund, as well as, disbursements under the "Coronavirus Economic Stabilization Act" under the oversight of SIGPR. Dealing with additional workloads, staffing, and other critical matters during the COVID-19 pandemic may be more challenging than usual. Additionally, concern was raised that with anticipated funding levels for fiscal year 2021, the cost associated with administering certain CARES Act programs may have an impact on Treasury's ability to fund other work.

35 OIG, *Interim Audit Update–Coronavirus Relief Fund Recipient Reporting* (OIG-20-036; May 27, 2020).
36 GrantSolutions is a grant program management Federal Shared service provider under the U.S. Department of Health and Human Services.
37 Partners include the Federal Reserve Banks (Kansas City and St. Louis), financial agents, and vendors.

The Office of International Affairs proposed an increase in staffing levels to address the expanding demands on the Committee on Foreign Investments in the United States[38] (CFIUS), which is charged with reviewing transactions involving foreign investments in the United States to determine national security risks. The Office of International Affairs carries out the Secretary's role as Chair of CFIUS and coordinates the interagency review process. While the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA)[39] modernized the review process, it also expanded CFIUS' jurisdiction to address growing concerns over certain investment structures that were not within CFIUS' jurisdiction such as investments involving U.S. businesses in close proximity to U.S. military bases and investments with impacts to critical infrastructure and personally identifiable information (PII). Treasury issued two final regulations in February 2020 to implement changes to jurisdiction and process. The fiscal year 2020 budget cited an expected increase in workload from approximately 200 to 1,000 cases annually.

Because CFIUS' expanded jurisdiction under FIRRMA became effective on February13, 2020, and the COVID-19 pandemic impact on case volume is tough to measure, it is difficult for Treasury to predict the effect of FIRRMA changes over the next year. With increased telework during the COVID-19 pandemic, CFIUS activities that involve sensitive and classified materials have been more difficult to perform. In addition, coordination with other Federal partners has been tougher as they are experiencing their own COVID-19 challenges.

Over the past several years, Treasury OIG has reported that the recruitment of cybersecurity personnel was a government-wide challenge due to the lengthy security clearance process. Previous audits of select Treasury bureaus found that the cause for many findings related to information systems' security measures involved a lack of resources and/or management oversight. In its April 23, 2020 letter[40] to the Department regarding its top open recommendations, the Government Accountability Office (GAO) included a recommendation from 2016 that emphasized the need for Treasury to address shortfalls in Information Technology (IT) workforce planning. While GAO acknowledged that some progress was made, Treasury had yet to develop an IT workforce plan that contained the key actions to address workforce skill gaps. In addition, GAO reported in 2019 that Treasury likely incorrectly categorized more than a thousand positions performing IT management functions. This means that Treasury may have unreliable information about its cybersecurity workforce that it will need to identify its workforce roles of critical need.

To further complicate matters, Treasury must also operate in the repeated cycle of budget and debt ceiling stopgaps. A long-term solution has yet to be found, and the U.S. debt limit was reinstated at $22 trillion on March 2, 2019. At that time, Treasury immediately implemented extraordinary measures to prevent the United States from defaulting on its obligations. Measures included (1) suspending State and Local Government Series securities sales, (2) declaring a "debt issuance suspension period" which suspended additional investments in the Civil Service Retirement and Disability Fund and Postal Retiree Health Benefits Fund, and (3) suspending investment in the Government Securities Investment Fund of the Federal Employees' Retirement System Thrift Savings Plan. In July 2019, Treasury informed Congress that these extraordinary measures would be exhausted before September 2019. Consequently, legislation was passed to suspend the statutory debt limit through July 31, 2021.[41] While the debt ceiling has been lifted, it is only temporary as Congress has yet to resolve unfinished business when it comes to the Nation's debt, and the long-term sustainability of the large programs. Although not included as a top open recommendation in its April 2020 letter to the Department, GAO raised the same concerns to Congress in its July 2015 report[42] with the approach to managing the federal debt limit and its impact on Treasury's borrowing costs and the need for alternative approaches.

The impact of this challenge and the uncertainties require Treasury to continue to focus its resources on programs that are in the highest need to citizens and/or where there is a unique federal role. It is essential

38 CFIUS is an interagency committee comprised of the departments of Commerce, Defense, Energy, Homeland Security, Justice, State, Treasury and the Office of the U.S. Trade Representative and the Office of Science and Technology.
39 Public Law 115-232 (August 13, 2018).
40 GAO, *Treasury Priority Recommendations* (GAO-20-549PR; April 23, 2020).
41 Public Law 116-37 (August 2, 2019).
42 GAO, *Debt Limit: Market Response to Recent Impasses Underscores Need to Consider Alternative Approaches* (GAO-15-476; July 9, 2015).

that new programs and reforms be managed and communicated effectively for achieving performance and accountability.

Cyber Threats

Cybersecurity remains a long-standing and serious challenge facing the Nation. 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, subtle, and easier to perform they pose ongoing challenges for Treasury to fortify and safeguard its internal systems and operations along with the financial sector it oversees. While managing known risks is an ongoing challenge, Treasury must also be ready to reinforce and/or redirect cybersecurity efforts when unforeseen events occur such as the COVID-19 global pandemic. As discussed throughout this challenge, the ongoing healthcare crisis has created more opportunities for malicious actors to disrupt and exploit information systems.

Attackers frequently exploit vulnerable networks or systems in a string of trusted connections to gain access to government systems. Attempted cyber-attacks against Federal agencies, including Treasury, and financial institutions continue to increase in frequency and severity while continuously evolving. 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; disrupt, degrade, or deny access to information systems; or infiltrate information systems and maintain a presence to enable future actions. Through cyber information sharing, Federal agencies are better prepared to thwart potential attacks to the cyber infrastructure of the Federal government and the financial sector that it serves. In its 2019 high risk list published biennially, GAO reported the nations' cybersecurity as a government-wide issue.

Long-standing cyber threats pose increased risks to networks and information systems during the ongoing COVID-19 global health pandemic as more opportunities are available for bad actors to stage cyber-attacks. As the tools used to perpetrate cyber-attacks become easier to use and more widespread, less technological knowledge and fewer resources are needed to launch successful attacks of increasing sophistication. Such attacks include distributed denial of service, phishing or whaling, fraudulent wire payments, malicious spam (malspam), ransomware, and compromise of supply chains (both hardware and software). The COVID-19 pandemic has shifted the Federal workforce to a primarily telework status which has provided attackers with more possibilities to disrupt services. Increased network traffic from remote sources provides cover for attackers to blend in with the Federal workforce and launch cyber assaults. Attackers may take advantage of the increased demand for information on COVID-19 by crafting highly attractive phishing, whaling, and malspam attacks that are more likely to succeed by luring workers in with promises of information related to COVID-19. These opportunities may allow hackers to launch a denial of service attack upon a network that can prevent remote workers from performing their duties and disrupt operations. Furthermore, information systems and its users are at heightened risk of COVID-19 related exploitation such as stimulus check scams, tax-fraud schemes, and fraudulent coronavirus testing kit scams, among other things.

There is continuing concern over foreign adversaries creating and exploiting vulnerabilities in the Nation's information and communication technology and services. Executive Order 13873 was issued on May 15, 2019, to secure the supply technology and services chain by banning the import, use, or sale of technology or services designed, developed, manufactured, or supplied from persons or companies that are owned or controlled by governments defined as hostile to the United States.[43] On May 13, 2020, this Executive Order was extended for one year.[44] There are risks that Treasury's systems and resources already in use, including critical infrastructure, contain components from sources that have yet to be designated as threats. Once a source is

43 *Executive Order on Securing the Information and Communications Technology and Services Supply Chain* (May 15, 2019).
44 *Text of a Notice on the Continuation of the National Emergency on Securing the Information and Communications Technology and Services Supply Chain* (May 13, 2020).

designated as such, repairs and/or upgrades of key system components may no longer be available. Therefore, there is risk of disruption of critical operations. The Department will need to monitor developments in this area closely and plan for the possibility that its current supply chain may no longer be available. This is especially true during this global pandemic as companies continue to temporarily close manufacturing plants due to COVID-19 outbreaks or shipping is disrupted by travel restrictions.

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 to the Nation's critical infrastructure. As such, effective public-private coordination is essential to the Nation's financial and national security. In this regard, The Office of Critical Infrastructure Protection and Compliance Policy coordinates Treasury's efforts to enhance the security and resilience of the financial services sector critical infrastructure and reduce operational risk including risks associated with cybersecurity. Given the stress that the global COVID-19 pandemic has placed on financial institutions and the financial sector, as a whole, it is important that the Department reassess cyber risks in these areas. That said, Treasury and other Federal agencies have yet to fully implement the National Institute of Standards and Technology (NIST) guidance to assist Federal agencies in managing cybersecurity risks.[45] In 2018, GAO had reported that the extent of adoption of the NIST framework by critical infrastructure sectors was unknown since agencies were not measuring framework implementation. With respect to Treasury, GAO had recommended that steps be taken to consult with respective sector partners to develop methods for determining the level and type of adoption by entities across the financial services sector. In its April 23, 2020 letter regarding its top open recommendations, GAO noted that Treasury had established ongoing initiatives such as developing common terminology for cyber terms, but had not developed methods to determine the level and type of framework adoption; the recommendation remained open. GAO also noted in its April 23, 2020 letter that Treasury has not provided actions related to a July 2019 report[46] to Treasury to develop a cybersecurity risk management strategy that includes key elements identified in federal guidance and establish a process for conducting an organization-wide cybersecurity risk assessment.

While addressing potential increases in cyber threats during the COVID-19 global pandemic, Treasury will need to continue to balance cybersecurity demands while modernizing and maintaining IT systems. To this end, Treasury must ensure that cyber security is fully integrated into to its IT investment decisions.

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

Treasury's Office of Terrorism and Financial Intelligence (TFI) has remained dedicated to countering the ability of financial networks that support terrorists, organized transnational crime, weapons of mass destruction proliferators, and other threats to international security through intelligence analysis, sanctions, and international private-sector cooperation. Identifying, disrupting, and dismantling the financial networks that support rogue regimes, terrorist organizations, transnational criminal organizations, and other threats to the national security of the United States and our allies continues to be challenging as TFI's role to counter these financial networks and threats has grown because its economic authorities are key tools to carry out U.S. policy.

TFI's counter-terrorism designations disrupt the financial networks that support terrorist organizations. Disrupting terrorist financing depends on a whole-of-government approach and requires collaboration and coordination within Treasury and with other Federal agencies. Collaboration and coordination are key to successfully identifying and disrupting all of these financial networks and meeting TFI's mission. This effort requires effective and efficient working relationships among components within TFI and the Intelligence Community.

Data security and information sharing are challenges for the Financial Crimes Enforcement Network (FinCEN), which has experienced unauthorized disclosures of Bank Secrecy Act information. FinCEN is required to maintain a highly secure database for financial institutions to report suspicious activity. FinCEN has previously

45 NIST, *Framework for Improving Critical Infrastructure Cybersecurity* (Version 1.0, February 12, 2014; superseded by Version 1.1; April 16, 2018).
46 GAO, *Cybersecurity Risk Management* (GAO-19-384 , July 25, 2019)

identified that the success of that system depends on the financial sector's confidence that those reports are adequately protected, but data breaches threaten to undermine that confidence. FinCEN is also required to maintain a government-wide data access service to make information available and useful to Federal, State, local, and foreign law enforcement agencies and appropriate regulators and to support intelligence and counterintelligence activities and anti-money laundering initiatives. The challenge for FinCEN is to ensure the Bank Secrecy Act data remains secure in order to maintain the confidence of the financial sector while meeting the access needs of law enforcement, regulatory, and intelligence partners.

Given the criticality of Treasury's mission and its role to carry out U.S. policy, Treasury OIG continues to consider anti-money laundering and combating terrorist financing programs and operations as inherently high-risk.

Efforts to Promote Spending Transparency and to Prevent and Detect Improper Payments

Given the broad implications and critical roles assigned to Treasury by the Digital Accountability and Transparency Act of 2014 (DATA Act), Treasury OIG notes the challenges facing the Department given the need to ensure transparency to the taxpayer and other stakeholders on the use of funds distributed under economic relief packages enacted to address individuals and industry sectors impacted by the COVID-19 global pandemic. As noted earlier, Treasury was tasked with responsibilities to administer over $2 trillion of emergency funding. DATA Act reporting is now seen as one of the means to ensure transparency into the use of Federal funds related to COVID-19 expenditures. The speed in which supplemental funding was distributed created new data management needs for Treasury along with labor intensive ingestion of data associated with the application for, and issuance of, economic relief. The rapid delivery of funds within short timeframes may create opportunities and risks for illicit activity by anyone attempting to misuse or abuse funds that were intended for COVID-19 relief. Considering the challenges and risks associated with ensuring economic relief is deployed and used for intended purposes, Treasury must continue to address reporting and data quality issues noted in DATA Act audits and intensify efforts to reduce improper payments.

Completed and In-Progress Work on Financial Oversight

OCC's Supervision of Wells Fargo Bank

We initiated an audit to assess OCC's supervision of incentive-based compensation structures within Wells Fargo and the timeliness and adequacy of OCC's supervisory and other actions taken related to Wells Fargo's sales practices, including the opening of accounts. We concluded that OCC examiners missed opportunities from 2010 to 2014 to analyze and address issues within Wells Fargo's incentive-based compensation structures. More specifically, although OCC assessed Wells Fargo's governance and risk management practices related to compliance and operational risk during this period; it did not assess the bank's oversight and governance of sales practices until 2015. We believe this was due, in part, to OCC examiners not sufficiently reviewing Wells Fargo's internal complaint data. We also determined that OCC lacked a formal complaint process for tracking "whistleblower-related" referrals made to OCC from initiation through resolution. Specifically, OCC's former complaint process did not adequately record and track the research and resolution of matters that were whistleblower-related.

In order to improve its supervisory process, OCC's Enterprise Governance Supervision (EGS) division performed an independent review of the Wells Fargo supervisory record and summarized the findings of that review in its "Lessons-Learned Review of Supervision of Sales Practices at Wells Fargo" report, dated April 2017. In its review, EGS identified significant issues relating to OCC's supervisory actions regarding complaint management and sales practices which align with our conclusion that prior to 2015, OCC examiners missed opportunities to analyze and address issues within Wells Fargo's incentive-based compensation structures. EGS made nine recommendations for OCC to address these and other supervisory issues. As of June 2018, all nine recommendations had been addressed by OCC. Based on OCC taking corrective actions to implement the nine recommendations identified in its lessons-learned review, we did not make any recommendations to OCC.

In order to improve its supervisory process, OCC's Enterprise Governance Supervision (EGS) division performed an independent review of the Wells Fargo supervisory record and summarized the findings of that review in its "Lessons-Learned Review of Supervision of Sales Practices at Wells Fargo" report, dated April 2017. In its review, EGS identified significant issues relating to OCC's supervisory actions regarding complaint management and sales practices which align with our conclusion that prior to 2015, OCC examiners missed opportunities to analyze and address issues within Wells Fargo's incentive-based compensation structures. EGS made nine recommendations for OCC to address these and other supervisory issues. As of June 2018, all nine recommendations had been addressed by OCC. Based on OCC taking corrective actions to implement the nine recommendations identified in its lessons-learned review, we did not make any recommendations to OCC.

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 Related to De-risking by Banks (In Progress)

We initiated an audit of OCC's supervisory impact on the practice of de-risking[47] 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.

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.

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.

OCC's Crisis Readiness (In Progress)

We initiated an audit of OCC's crisis readiness. The objective for this audit is to assess OCC's readiness to address crises that could impact OCC's operations and the institutions it supervises.

Failed Bank Reviews

In 1991, Congress enacted the Federal Deposit Insurance Corporation Improvement Act 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 $50million for 2014 and thereafter (with a provision to temporarily raise the threshold to $75million 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

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

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.[48] As appropriate, OIG auditors also make recommendations for preventing any such loss in the future.

From 2007 through March 2021, FDIC and other banking regulators closed 536 banks and federal savings associations. One hundred and forty-four (144) of these were Treasury-regulated financial institutions; in total, the estimated loss to FDIC's Deposit Insurance Fund for these failures was $36.5 billion. Of the 144 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 did not perform a material loss review. We completed two reviews of bank failures, each of which with losses under the material loss review threshold. Resolute Bank, Maumee, Ohio failed on October 25, 2019 and City National Bank of New Jersey failed on November 1, 2019, resulting in an estimated loss to the Deposit Insurance Fund of $2.2 million and $2.5 million, respectively. Our reviews determined that there were no unusual circumstances warranting an in-depth review of either failure.

48 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.

Appendix A:

CIGFO Presidential Transition Handbook

Council of Inspectors General on Financial Oversight

Presidential Transition Handbook

December 2020

Council of Inspectors General on Financial Oversight

MISSION

The Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act)* established the Council of Inspectors General on Financial Oversight (CIGFO) to provide oversight of the Financial Stability Oversight Council's (FSOC) operations and suggest measures to improve financial oversight.

* Public Law 111-203 (July 21, 2010).

Executive Summary

Introduction to CIGFO

In the aftermath of the 2008 financial crisis, Congress passed, and President Obama signed, the Dodd-Frank Act "to promote the financial stability of the United States by improving accountability and transparency in the financial system, to end 'too big to fail', to protect the American taxpayer by ending bailouts, to protect consumers from abusive financial services practices, and for other purposes."

Created by the Dodd-Frank Act, CIGFO is comprised of the Inspectors General (IG) of the nine major government Financial-Sector Regulatory Organizations and the Special Inspector General for the Troubled Asset Relief Program to provide oversight of FSOC and facilitate information sharing among the IG members.

We are once again in the midst of a series of unprecedented events. A public health and subsequent economic crisis has gripped the United States and the world. In recent months, the Coronavirus Disease 2019 (COVID-19) has swept across the globe. Individuals, families, and businesses are affected by the pandemic. Many are in need of assistance, whether it is health care assistance caused by illness or financial assistance resulting from pandemic-related disruptions to their livelihoods. In keeping with its mission, CIGFO, which is authorized to provide oversight of FSOC operations, is monitoring the ongoing response of FSOC and its member agencies related to the public health and financial crisis. As warranted, this oversight will include reviews by the individual IG of their agencies and collectively as CIGFO, of FSOC and member Federal agencies' preparedness and responses to events that cause significant stress to the U.S. financial system, like the COVID-19 pandemic.

In addition to CIGFO's oversight activities, it has performed monitoring activities and shares financial regulatory information among the member IGs, which enhance each IG's knowledge and insight about specific issues related to current and future work. For example, during its quarterly meetings, CIGFO members discuss audits on bank enforcement actions; financial research activities; compliance with the Bank Secrecy Act; issues with continuity of operations resulting from increased teleworking; as well as legislative activities that could impact the financial regulatory system.

Transition Issues Relating to CIGFO

Once leadership of FSOC and its member agencies are appointed, it is critical for CIGFO and FSOC's leadership to have regular and candid communications. Regular communications will enable CIGFO to inform FSOC leadership about ongoing work, the results of completed work, and the status of any open recommendations from CIGFO working group reports.

The transition team should review the *Top Management and Performance Challenges Facing Financial-Sector Regulatory Organizations* (CIGFO TMPC 2019-07-19) as this document consolidates the top management and performance challenges facing the Financial-Sector Regulatory Organizations identified by the CIGFO members.

Dodd-Frank Act, FSOC, and Role of CIGFO

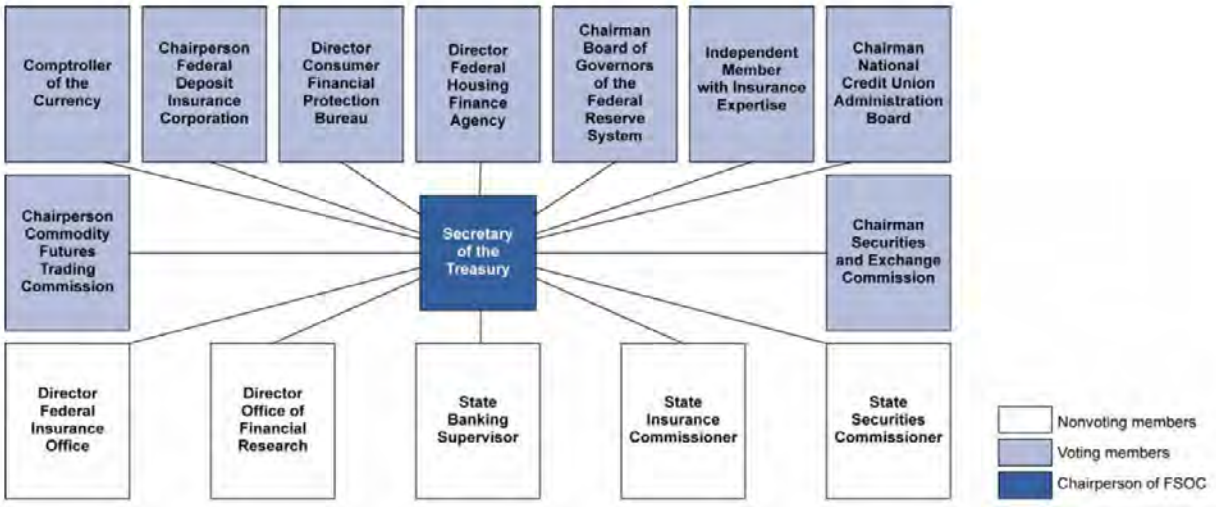
Dodd-Frank Act, FSOC, and Role of CIGFO

Dodd-Frank Act and FSOC

In July 2010, the Dodd-Frank Act was signed into law and created a new regulatory and resolution framework designed to promote the financial stability of the United States. The Dodd-Frank Act is comprehensive in scope, providing for significant changes to the structure of federal financial regulation and substantive requirements that apply to a broad range of market participants, including public companies that are not financial institutions. Among other measures, the Dodd-Frank Act included corporate governance and executive compensation reforms, new registration requirements for hedge fund and private equity fund advisers, heightened regulation of over-the-counter derivatives and asset-backed securities, and new rules for credit rating agencies. The Dodd-Frank Act also mandated significant changes to the authority of the Board of Governors of the Federal Reserve System and the Securities and Exchange Commission as well as enhanced oversight and regulation of banks and non-bank financial institutions. Finally, the Dodd-Frank Act established the Consumer Financial Protection Bureau as a new federal agency to regulate the offering and provision of consumer financial products and services under various consumer financial protection laws.

The Dodd-Frank Act created FSOC which is comprised of ten voting members and five nonvoting members (see Figure 1). Chaired by the Secretary of the Treasury, FSOC is charged with identifying risks to the financial stability of the United States; promoting market discipline; and responding to emerging threats to the stability of the U.S. financial system.

Figure 1: FSOC Membership



Source: GAO 12-886, Financial Stability – New Council and Research Office Should Strengthen Accountability and Transparency of Decisions, September 2012

Role and Authorities of CIGFO

The Dodd-Frank Act created, among other things, CIGFO, which is comprised of the IGs of the nine major government Financial-Sector Regulatory Organizations and the Special Inspector General for the Troubled Asset Relief Program, to facilitate information sharing among the IG members, provide a forum for discussion of IG member work as it relates to the broader financial sector, and evaluate the effectiveness and internal operations of the FSOC. CIGFO is chaired by the Inspector General of Treasury and its members include the Inspectors General of 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 Consumer Financial Protection Bureau, 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 and the Troubled Asset Relief Program, as shown in Figure 2.

Figure 2: CIGFO Membership & Oversight Responsibilities

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 Consumer Financial Protection Bureau	• Board of Governors of the Federal Reserve System • Consumer Financial Protection Bureau
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	Troubled Asset Relief Program

Source: CIGFO's Top Management and Performance Challenges Facing Financial-Sector Regulatory Organizations (July 2019).

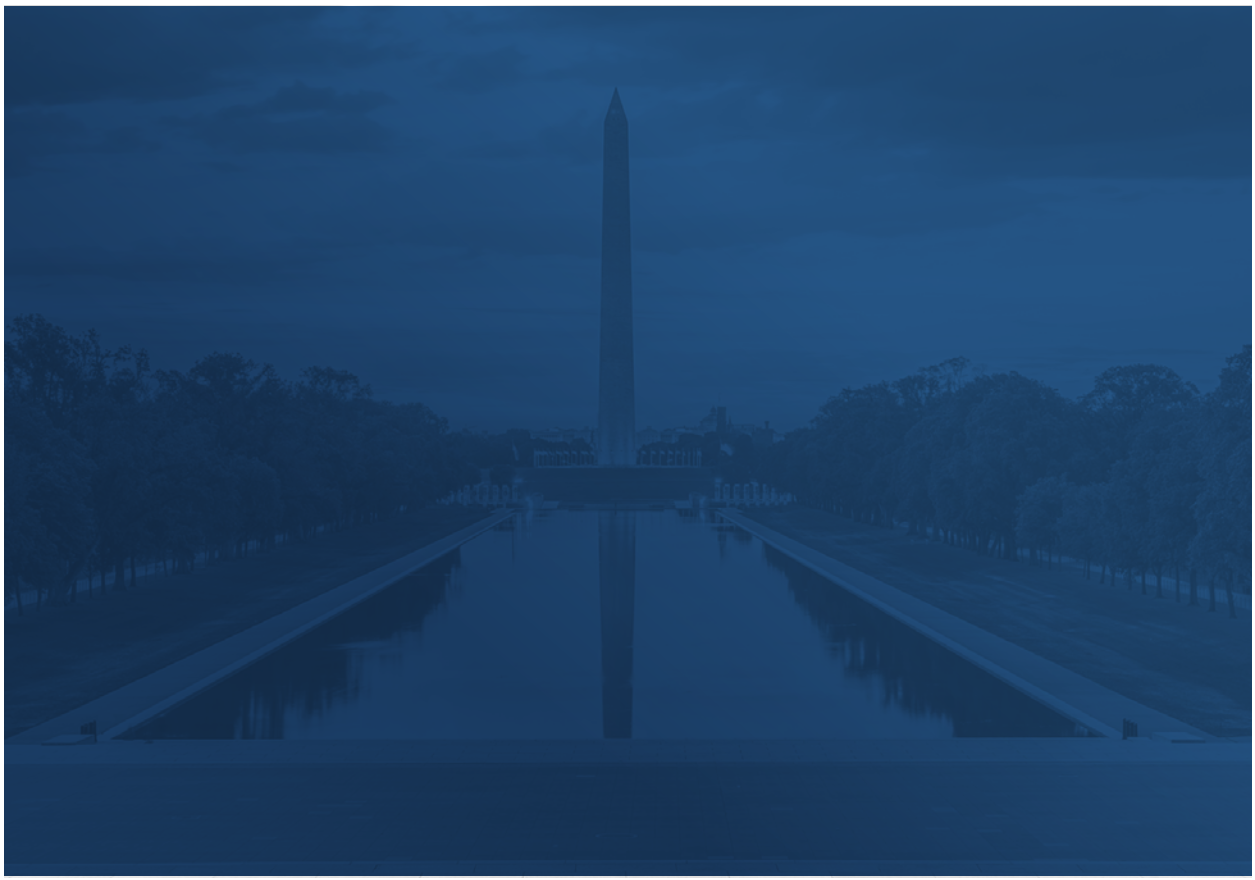
CIGFO provides an opportunity to leverage the expertise and experience of its IG members, who bring unique independent perspectives to the table on both joint projects and individual efforts.

The Dodd-Frank Act assigns CIGFO the following duties:

- Meet not less than once each quarter to facilitate the sharing of information and to discuss the ongoing work of each IG who is a member of CIGFO as it applies to the broader financial sector and ways to improve financial oversight.

- Submit annually to Congress and FSOC a report highlighting the concerns and recommendations of each IG, with a focus on issues that may apply to the broader financial sector, and a summary of general observations of CIGFO, with a focus on measures that should be taken to improve financial oversight.

In addition, the Dodd-Frank Act authorizes CIGFO to convene working groups to evaluate the effectiveness and internal operations of the FSOC and shall submit regular reports to FSOC and to Congress on these evaluations.



CIGFO Independence

CIGFO Independence

IGs, and by extension, CIGFO, must perform their audits, investigations, evaluations, and special reviews objectively and independently from the agency. As in past transitions, the CIGFO member IGs remain in office when Presidential Administrations change.

Several key provisions of the Inspector General Act of 1978, as amended (IG Act),[1] seek to ensure IG independence, in both reality and appearance. For example, according to the IG Act, an agency head may not prevent the IG from initiating, carrying out, or completing any audit or investigation, except for in very limited circumstances.

Moreover, IGs report only to the agency head or in certain instances, the officer next in rank below the agency head. To ensure IG access to relevant information, the IG Act requires IGs to report to their agency heads "without delay" the circumstances of any unreasonable refusal of their information requests. In regards to FSOC, CIGFO reports to its chair, the Treasury Secretary and its members.

1. Public Law 95-452 (October 12, 1978).

CIGFO Reports and Process

CIGFO Reports and Process

CIGFO Working Group Projects

Since 2011, CIGFO has established working groups, comprised of staff from the CIGFO member IG offices, to conduct reviews of FSOC operations. CIGFO relies on these working groups to fulfill its mission as outlined in the Dodd-Frank Act. To learn more about CIGFO and to review each of the reports mentioned below and others, visit our website: Council of Inspectors General on Financial Oversight.

A current working group project is the compilation of *Forward Looking Guidance for FSOC and Its Members in Preparing for a Crisis*. This forward-looking guidance is intended to be a compilation of lessons learned drawn from the experiences of federal agencies during prior crises and any lessons learned during the recent pandemic. The forward-looking guidance will facilitate effective crisis response as FSOC fulfills its mission to identify threats to the financial stability of our country, promote market discipline, and respond to emerging threats to the stability of the U.S. financial system. This report is expected to be issued in spring 2021.

In recent years, CIGFO has convened working groups and reported on such projects as; *CIGFO Audit of FSOC's Monitoring of International Financial Regulatory Proposals and Developments* and *CIGFO Working Group's Survey of FSOC and its Federal Member Agencies' Efforts to Implement the Cybersecurity Act of 2015*.

CIGFO Audit of the Financial Stability Oversight Council's Monitoring of International Financial Regulatory Proposals and Developments *(CIGFO-2019-01; May 2019)*

CIGFO convened a working group to assess FSOC's monitoring of international financial regulatory proposals and developments. CIGFO 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 but several FSOC members or representatives offered suggestions for enhancing the process. The report does not make any recommendations but encourages FSOC to consider incorporating the suggestions made by members. FSOC acknowledged the findings and conclusions in this report and stated that the suggestions made to further enhance FSOC's work would be considered.

Survey Results— CIGFO Working Group's Survey of FSOC and its Federal Member Agencies' Efforts to Implement the Cybersecurity Act of 2015 *(CIGFO-2020-01; January 2020)*

The working group conducted a survey of FSOC and its Federal voting member agencies' efforts to implement the information sharing provisions under the Cybersecurity Information Sharing Act of 2015 (CISA)[2]. Agencies provided responses to a set of questions on their implementation of CISA. Specifically, the responses addressed: (1) sufficiency of policies and procedures related to sharing cyber threat indicators (CTIs)[3] within the federal government, (2) classification of the CTIs

2. Public Law 114-113 (December 18, 2015).

3. Per CISA, CTI is information used to describe or identify security vulnerabilities, tools and procedures that may be used by attackers to compromise information systems.

and defensive measures (DMs)[4], and an accounting of the security clearances for the purpose of sharing with the private sector, (3) actions taken based on CTIs or DMs sharing with the Federal Government, (4) CTIs and DMs shared with federal entities containing information not directly related to a threat that is personal information, and (5) any barriers to sharing information among federal entities. The working group provided FSOC and its Federal voting member agencies comparative information on how member agencies have implemented CISA from January 1, 2017 through March 31, 2019. The working group did not assess Federal voting member agencies' compliance with CISA and did not make any recommendations to FSOC.

CIGFO also issued a report by a working group convened in March 2019 that reported on the top management and performance challenges identified across CIGFO member agencies.

Top Management and Performance Challenges Facing Financial-Sector Regulatory Organizations *(July 2019)*

The purpose of this report was to consolidate and provide insight into cross-cutting management and performance challenges facing Financial-Sector Regulatory Organizations in 2019, as identified by members of CIGFO. The challenges identified in this report are: (1) enhancing oversight of financial institution cybersecurity, (2) managing and securing information technology at regulatory organizations, (3) sharing threat information, (4) ensuring readiness for crises, (5) strengthening agency governance, (6) managing human capital, and (7) improving contract and grant management.

CIGFO Annual Reports

The Dodd-Frank Act mandates that CIGFO submit to FSOC and Congress an annual report that summarizes the general observations of CIGFO based on the views expressed by each IG with a focus on measures that should be taken to improve financial oversight. Each IG who is a member of CIGFO has a section within the annual report with exclusive editorial control to highlight the concerns and recommendations from ongoing and completed work of their office. Additionally, CIGFO provides a section within the annual report on all CIGFO issued working group reports. In July 2020, CIGFO was proud to issue its tenth annual report to FSOC and Congress and noted that to date, the corrective actions described by FSOC, with respect to the issued CIGFO working group reports, have met the intent of CIGFO's recommendations.

4. Per CISA, DM is an action, device, procedure, technique, or other measure that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability.

CIGFO and Council of the Inspectors General on Integrity and Efficiency (CIGIE) Coordination

CIGFO and Council of the Inspectors General on Integrity and Efficiency (CIGIE) Coordination

All nine IGs comprising CIGFO are also members of the Council of the Inspectors General on Integrity and Efficiency (CIGIE). Several of them are currently serving, or have served, on various CIGIE committees and working groups such as CIGIE's Inspection and Evaluation Committee which supports and promotes evaluation and inspection practices in the IG community, and CIGIE's Suspension and Debarment Working Group which is charged with improving the effectiveness of federal suspension and debarment practices. CIGIE's Pandemic Response Accountability Committee (PRAC) was established under the Coronavirus Aid, Relief, and Economic Security Act (CARES Act),[5] to promote transparency and ensure coordinated oversight of the government's spending and coronavirus response. Many of the CIGFO IGs serve on this important committee and provide their expertise in leading the PRAC's Financial Institutions Oversight Issue Group. CIGFO working group efforts generally adhere to the Government Auditing Standards, also known as the Yellow Book, and when applicable, conform to the quality standards developed by CIGIE. To learn more about CIGIE, visit www.ignet.gov/content/about-igs.

5. Public Law 116-136 (March 27, 2020).

Transition Issues Relating to CIGFO

Transition Issues Relating to CIGFO

Historically, because of their nonpartisan, independent status, IGs have remained in office when Presidential Administrations change. As a result, CIGFO, which is composed of IGs from the nine Financial-Sector Regulatory Organizations and the Special Inspector General for the Troubled Asset Relief Program, will remain largely unchanged preserving the knowledge and experience that is crucial to FSOC, CIGFO, and each IG's respective office.

Role of CIGFO in the Transition to a New Administration

Just as individual CIGFO member IGs can perform a valuable role during Presidential transitions at their respective agencies, CIGFO, as a collective body, can provide an equally valuable role in a transition. Based on its experience and unique perspective, CIGFO can be a valuable source of information about the key financial oversight issues that will confront the new Administration's management team.

In the past, the transition teams for many agencies have met individually with the IG of that agency for a briefing on the IG's ongoing and recently completed work, as well as the IG's view of the important issues within the agency that will confront the new Administration. It is useful for the transition teams to meet with the IG of that agency early in the transition process. Reflecting the IGs' independence and unique perspective on their agency, transition teams should meet with the IGs separate from their meetings with other management officials within the agency.

We suggest the transition teams review CIGFO's *Top Management and Performance Challenges Facing Financial-Sector Regulatory Organizations* (July 2019). This critical report consolidates the top management and performance challenges issued by the CIGFO members into a singular report identifying cross-cutting challenges facing multiple Financial-Sector Regulatory Organizations. Although Financial-Sector Regulatory Organizations have individual missions, this report emphasizes the importance of addressing challenges holistically through coordination and information sharing. Considering issues on a whole-of-Government approach versus a siloed, agency-by-agency basis allows for more effective and efficient means to address challenges through a coordinated approach.

This report will provide a useful overview to transition teams and new Administration appointees in understanding the scope of the issues they will confront in the financial sector and within the Financial-Sector Regulatory Organizations.

New Administration Officials' Interaction with CIGFO

Once the new Administration takes office, it is critical for CIGFO and FSOC's leadership to have regular and candid communications. After leadership of FSOC and their member agencies are appointed, it is important that they establish regular communications with CIGFO and the IGs of their respective agency.

These meetings will enable CIGFO to inform FSOC leadership about ongoing work, the results of completed work, and the status of open recommendations from working group reports and other

working group projects. CIGFO will also be able to answer questions about the processes and procedures it uses in its work. In addition, the FSOC members will be able to discuss their priorities and their views on future CIGFO reviews that could be valuable for agency programs. CIGFO can raise any impediments to its work or any areas that it believes need management attention for corrective action. On these and other issues, effective and regular communication between FSOC and CIGFO is important to establish an effective and candid relationship that fulfills the purposes of the Dodd-Frank Act.

Council of Inspectors General on Financial Oversight

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