JULY 2020

Annual Report of the Council of Inspectors General on Financial Oversight

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

Message from the Chair

We are in the midst of an unprecedented public health and economic crisis. In recent months, the novel Coronavirus (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 disruptions to their livelihoods. Regardless of the challenges, all of us are making adjustments in our lives. 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, 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 Inspectors Generals 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.

Looking back at the work completed in 2019 and 2020 for this annual reporting cycle, CIGFO continued its oversight role. In this role, it has, since 2011, established working groups that are comprised of staff from the CIGFO member Inspector General offices to conduct reviews of FSOC operations—CIGFO relies on these working groups to fulfill its mission. CIGFO issued a report by a Working Group convened in December 2018 that surveyed FSOC Federal members' efforts to support implementation of the Cybersecurity Information Sharing Act of 2015. CIGFO also issued a report by a Working Group convened in March 2019 that reported on management and performance challenges identified in 2018 across CIGFO agencies. These reports can be found in Appendix A and Appendix B.

In addition to CIGFO's oversight activities, it has performed monitoring activities including sharing financial regulatory information which enhanced Inspectors General knowledge and insight about specific issues related to members' current and future work. For example, during its quarterly meetings, CIGFO members discussed audits on bank enforcement actions, financial research activities, and 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.

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

/s/

Rich Delmar
Acting Chair, Council of Inspectors General on Financial Oversight
Deputy 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:

- National Cyber Investigative Joint Task Force – structure and core services of its Virtual Currency Team and an overview of what virtual currency is and its key attributes
- Federal Deposit Insurance Corporation Office of Inspector General – overview of fraud schemes associated with cyber-crimes and strategies to prevent them
- Intelligence Community Inspector General – results of an audit of the appropriate federal entities implementation of the Cybersecurity Information Sharing Act of 2015
- FSOC's interpretative guidance on nonbank financial designations
- Events related to whistleblower rights and protections
- Components of the economic stimulus included in the Coronavirus Aid, Relief, and Economic Security Act of 2020 and the oversight role of the Office of Inspector General community

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*

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

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

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

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

Background

Congress established 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.

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 2019:

- Enhancing Organizational Governance and Risk Management
- Enhancing Oversight of Cybersecurity at Supervised Financial Institutions
- Ensuring That an Effective Information Security Program Is in Place
- Adapting to Internal and External Developments While Refining the Regulatory and Supervisory Framework

Among other items, we identified two major management challenges for the Bureau that apply to the financial sector in 2019:

- Ensuring That an Effective Information Security Program Is in Place
- Continuing to Refine the Supervision and Enforcement Strategy

The Board Can Enhance Its Internal Enforcement Action Issuance and Termination Processes by Clarifying the Processes, Addressing Inefficiencies, and Improving Transparency, OIG Report 2019-SR-B-013, September 25, 2019

The Board seeks to ensure that the financial institutions under its authority employ safe and sound business practices and comply with all applicable federal laws and regulations. If the Board or a Reserve Bank identifies significant concerns with these institutions through the supervisory process or other means, supervision staff can use enforcement actions to compel an institution's management to address the issues. We assessed the efficiency and effectiveness of the Board's and the Reserve Banks' enforcement action issuance and termination processes and practices.

We found that the Board and the Reserve Banks have implemented some effective practices to support the enforcement action issuance and termination processes; however, we identified opportunities for the Board to enhance these processes. Specifically, we found that the Board can clarify certain aspects of these internal processes, such as the steps in these processes, the Board stakeholders' roles and responsibilities, and the Board members' involvement. In addition, we found that the Board can (1) improve the timeliness and efficiency of its enforcement

action issuance and termination processes and (2) increase transparency with respect to the status of ongoing enforcement actions.

Our report contains recommendations designed to enhance the efficiency and effectiveness of the Board's enforcement action issuance and termination processes. The Board concurred with our recommendations.

Leveraging Certain Strategies May Help the Board Timely Implement and Sustain Enterprisewide Workforce Planning, OIG Report 2019-MO-B-012, September 25, 2019

Workforce planning is the systematic process for identifying and addressing the gaps between an organization's workforce of today and its future human capital needs. The Board's Human Resources (HR) function developed a preliminary enterprisewide workforce planning process in 2017 and began an initial pilot program with one division and one functional area of another division in 2018, which it has since completed. HR also developed a workforce plan with a third division and intends to complete a fourth workforce plan in 2019. We conducted this evaluation to identify any specific operational challenges to the Board's efforts to implement workforce planning and related lessons learned from other organizations that may be applicable to the Board.

We found that although the Board has made initial progress in implementing enterprisewide workforce planning, it faces four operational challenges, which are common among other organizations in the private and public sectors: resources, data and information, time, and process ownership. Through benchmarking, we identified several strategies—having data-driven conversations, sufficient and trained resources, leadership support throughout the organization, and a clearly structured process—that may help the Board mitigate its operational challenges. The Board has begun to address some of its challenges with these mitigating strategies; however, additional efforts to more comprehensively use these strategies may help the Board more timely implement and sustain an enterprisewide workforce planning process.

We also noted that HR should consider partnering with relevant divisions to coordinate workforce planning with other processes. By incorporating workforce planning into its existing administrative processes, such as strategic planning and enterprise risk management, the Board can help to ensure that it has centralized the workforce information necessary to make informed decisions when addressing operational priorities.

Our report contains recommendations to help the Board timely implement and sustain enterprisewide workforce planning. The Board concurred with our recommendations.

The Board Should Finalize Guidance to Clearly Define Those Considered Senior Examiners and Subject to the Associated Postemployment Restriction, OIG Report 2020-SR-B-003, March 9, 2020

The Intelligence Reform and Terrorism Prevention Act of 2004 restricts senior examiners at Reserve Banks from working for depository institutions and depository institution holding companies they have supervised during 2 or more months of their final 12 months of employment. The penalties for violating this restriction may include an industrywide prohibition for up to 5 years and a civil monetary penalty of up to $250,000. To implement the act, the Board issued Supervision and Regulation Letter 16-16/Consumer Affairs Letter 16-7, Special Post-Employment Restriction for Senior Examiners (SR Letter 16-16). We assessed the effectiveness of controls designed to ensure compliance with the requirements outlined in SR Letter 16-16.

We found that the four Reserve Banks in our sample have issued policies and procedures to identify senior examiners, require that they be notified of their postemployment restriction, and require workpaper reviews as appropriate. These Reserve Banks took different approaches, however, to determining whom to designate as a senior examiner. The senior examiners we interviewed appeared to understand the postemployment restriction and the penalties for violating the restriction.

Although the Board found through a 2017 horizontal review that the Reserve Banks implemented the Board's postemployment restriction guidance, the review also found that the Reserve Banks did not always apply the senior

examiner definition in accordance with the guidance. Thus, the 2017 review team recommended that the Board issue additional guidance to clarify the definition of a senior examiner. As of November 2019, the Board had not finalized this guidance.

Our report contains a recommendation designed to enhance the consistency among Reserve Banks in determining which employees should be designated as senior examiners for the purpose of applying the postemployment restriction. The Board concurred with our recommendation.

The Board's Oversight of Its Designated Financial Market Utility Supervision Program Is Generally Effective, but Certain Program Aspects Can Be Improved, OIG Report 2020-FMIC-B-005, March 18, 2020

Title VIII of the Dodd-Frank Act was enacted to mitigate systemic risk in the financial system and promote financial stability, in part through enhanced supervision of designated financial market utilities (DFMUs), which are systems that transfer, clear, or settle payments and other transactions among financial institutions. A failure or disruption of a DFMU could affect the smooth functioning of financial markets or financial stability. Title VIII grants the Board enhanced authority to supervise the DFMUs for which it is the supervisory agency and to consult with other federal agencies when the Board is not the designated supervisory agency for a DFMU. We assessed the effectiveness of the Board's oversight of its DFMU supervision program.

The Board has implemented practices and processes (1) to ensure governance over the DFMU supervision program, (2) to collaborate with other supervisory agencies in accordance with authorities provided in the Dodd-Frank Act, and (3) to conduct reviews of material changes filed by DFMUs that meet the Board's responsibilities under title VIII of the Dodd-Frank Act. However, we identified opportunities for the Board to enhance these practices and processes. Specifically, we found that the Board should publish certain internal delegations of authority and define certain roles and responsibilities within the DFMU supervision program. We also found that the Board can enhance its processes for collaborating with other supervisory agencies. Lastly, we found that the Board can better prepare for emergency changes filed by the DFMUs for which it is the supervisory agency.

Our report contains recommendations designed to enhance the efficiency and effectiveness of the Board's governance over its DFMU supervision program, its collaboration with other supervisory agencies, and its processes for reviewing emergency changes filed by DFMUs. The Board concurred with our recommendations.

The Board Can Enhance Certain Aspects of Its Enforcement Action Monitoring Practices, OIG Report 2020-SR-B-006, March 18, 2020

The Board delegates to each Reserve Bank the authority to supervise certain financial institutions within its District, with oversight by the Board's Division of Supervision and Regulation. If the Board or a Reserve Bank identifies significant concerns through the supervisory process or other means, supervision staff can use various enforcement tools to compel the institution's management to address the issues. Each Reserve Bank is responsible for monitoring compliance with all enforcement actions and recommending termination or modification of the actions within its District's purview. We assessed the effectiveness of the Board's and the Reserve Banks' enforcement action monitoring practices, with a focus on supervised financial institutions within the community banking organization (CBO) and the large and foreign banking organization portfolios.

We found that the Reserve Banks in our sample have implemented some effective practices for monitoring enforcement actions; however, we identified opportunities for the Board to enhance certain aspects of these practices. Specifically, we found that the Reserve Banks in our sample use different information systems for monitoring enforcement actions against institutions in the CBO portfolio. We learned that the Board currently has an initiative underway to develop a common technology platform for supervisory activities across the Federal Reserve System for institutions with less than $100 billion in total assets, including CBOs. We also identified certain instances of Reserve Bank staff not posting supervised institutions' progress reports describing their enforcement action remediation efforts to the required system of record.

Our report contains a recommendation designed to enhance the effectiveness of the Board's enforcement action monitoring practices. The Board concurred with our recommendation.

The Board Can Further Enhance the Design and Implementation of Its Operating Budget Process, OIG Report 2020-FMIC-B-010, March 25, 2020

Although the Board is not subject to federal budget-related laws, it prepares an annual budget as part of its efforts to ensure appropriate stewardship and accountability. The Board's 2018 annual operating budget was $766.7 million and included 2,847 authorized positions. We assessed the design and implementation of the Board's processes for formulating and executing its annual operating budget.

The Board has made changes over the past several years to improve its budget process; the Board has acknowledged perennial underspending and is addressing it by focusing on slowing growth and spending more consistently with budget estimates. The Board can further enhance the design and implementation of its operating budget process by communicating its budget process in an overarching document, strengthening the connection between budget and strategy, and implementing an agencywide approach to executing the approved budget. Doing so may help the Board define a more predictable and repeatable process; prioritize funding and monitor progress against strategic goals; and allocate financial and human capital resources more effectively, including conducting tradeoffs across the agency.

Our report contains recommendations designed to help the Board enhance the design and implementation of its operating budget process. The Board concurred with our recommendations.

Bureau Efforts to Share Consumer Complaint Data Internally Are Generally Effective; Improvements Can Be Made to Enhance Training and Strengthen Access Approval, OIG Report 2019-FMIC-C-008, June 3, 2019

Consumers have submitted over 1.7 million complaints about financial products and services with the Bureau since 2011. The effective sharing of complaint information among its divisions can help the Bureau understand the problems consumers are experiencing in the financial marketplace and identify and prevent unfair practices. We examined (1) the extent to which Consumer Response's consumer complaint–sharing efforts help to inform the work of internal stakeholders and (2) Consumer Response's controls over internal access to shared complaint data, which can contain sensitive consumer information.

Overall, Consumer Response effectively shares consumer complaint data within the Bureau. To increase the incorporation of complaint data in the Bureau's work, Consumer Response can better educate users about the internal complaint-sharing tools. Consumer Response can also enhance access controls to ensure that access to complaint data is limited to only users who need such information to perform their job functions.

Our report contains recommendations designed to further enhance the effectiveness of Consumer Response's internal complaint-sharing efforts and to strengthen access controls over complaint data containing sensitive consumer information. The Bureau concurred with our recommendations.

The Bureau Can Improve the Effectiveness of Its Life Cycle Processes for FedRAMP, OIG Report 2019-IT-C-009, July 17, 2019

FedRAMP was established in 2011 to provide federal agencies with a cost-effective, risk-based approach for the adoption and use of cloud computing services. The Bureau uses five FedRAMP cloud systems to support various mission and business processes, and it plans to move to a cloud-only information technology (IT) infrastructure by 2022. To meet our FISMA requirements, we determined whether the Bureau has implemented an effective life cycle process for deploying and managing FedRAMP cloud systems, including ensuring that effective security controls are implemented.

We found that the Bureau has developed a life cycle process for deploying and managing security risks for Bureau systems, which include the FedRAMP cloud systems it uses. However, we found that the process is not yet effective in ensuring that (1) risks are comprehensively assessed prior to deploying new cloud systems, (2) continuous monitoring is performed to identify security control weaknesses after deployment, and (3) electronic media sanitization renders sensitive Bureau data unrecoverable when cloud systems are decommissioned.

Our report contains recommendations designed to strengthen the Bureau's life cycle processes for leveraging FedRAMP cloud systems in the areas of risk management, continuous monitoring, and electronic media sanitization. The Bureau concurred with our recommendations.

The Bureau's Office of Enforcement Has Centralized and Improved Its Final Order Follow-Up Activities, but Additional Resources and Guidance Are Needed, OIG Report 2020-SR-C-002, March 2, 2020

Section 1055(a)(1) of the Dodd-Frank Act provides the Bureau or a court the authority to issue final orders against any entity or person for violations of federal consumer financial law. In August 2017, the Bureau's Office of Enforcement created a compliance team to centralize the office's follow-up activities on final orders. As of April 2019, Enforcement was responsible for monitoring compliance with final orders that collectively contained more than 3,000 provisions. We assessed the effectiveness of Enforcement's processes for monitoring and conducting follow-up activities related to final orders.

Enforcement has implemented some effective practices to improve its follow-up on final orders; however, we identified additional opportunities for Enforcement to improve its final order follow-up activities and reporting. First, we determined that Enforcement encountered challenges completing follow-up activities within the time frames established by its compliance team for 5 of 12 orders we reviewed. In addition, the enforcement actions page on the Bureau's public website provided information on the status of public enforcement actions that was prone to misinterpretation, because the website did not define the status categories or describe the purpose of the status information. After we completed our fieldwork and shared preliminary observations with the Bureau, the agency revised the status categories and indicated that it intends to provide additional clarifying information on its website. Finally, Enforcement can establish comprehensive guidance addressing expectations for conducting and documenting follow-up activities to help promote consistency.

Our report contains recommendations to improve Enforcement's follow-up activities and reporting related to final orders. The Bureau concurred with our recommendations.

Ongoing Work

Evaluation of the Board Economic Divisions' Research Planning Processes

The Board's four economic research divisions—Research and Statistics, Monetary Affairs, International Finance, and Financial Stability—produce research that supports the formulation and conduct of policy in key mission areas and informs the Board's financial stability activities. We are assessing these divisions' processes to plan certain research activities and identifying any opportunities to enhance the processes' effectiveness.

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

We identified cybersecurity oversight at supervised financial institutions as a major management challenge for the Board on an annual basis from 2015 to 2019. In 2017, we issued a report focused on cybersecurity supervision of multiregional data processing servicers and financial market utilities, among other topics. For the second phase of our cybersecurity oversight activities, we are assessing the Board's cybersecurity supervision of the largest and most systemically important financial institutions—those institutions in the Board's Large Institution Supervision Coordinating Committee portfolio.

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 plan to evaluate the efficiency and effectiveness of the Board's and the Reserve Banks' consumer compliance examination and enforcement action processes.

Evaluation of the Board's Adoption of Cloud Computing Solutions

Federal agencies, including the Board, are increasingly implementing cloud computing–based systems to meet their business needs. Cloud computing refers to a model for enabling convenient, on-demand network access to a shared pool of configurable resources (for example, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. We are initiating a scoping phase to review the Board's planning and security management processes for adopting cloud computing systems. During the scoping phase for this evaluation, we will further develop our objectives, scope, and methodology.

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 initiating a scoping phase to review the Board's progress in implementing ERM, including supporting governance structures and processes to identify, assess, respond to, monitor, and communicate risks. During the scoping phase for this evaluation, we will further develop our objectives, scope, and methodology.

Security Control Review of the Board's National Information Center

The Federal Information Security Modernization Act of 2014 requires that each agency inspector general conduct an annual independent evaluation of its respective agency's information security program and practices, including testing controls for select systems. To meet these requirements, we have initiated a security control review of the Board's National Information Center, which is the central repository and authoritative source of supervision and regulation, banking organization structure, and supervisory data.

Review of the Bureau's Budget Process

The Dodd-Frank Act created the Bureau's unique funding structure, which is outside the congressional appropriations process. The funding structure requires the Board to transfer to the Bureau a quarterly sum "determined by the Director to be reasonably necessary to carry out the authorities of the Bureau under Federal consumer financial law, taking into account such other sums made available to the Bureau from the preceding year (or quarter of such year)." We are assessing the design and implementation of the controls over the Bureau's budget processes, as well as compliance with applicable laws and regulations. We are focusing on (1) the Bureau's budget formulation and execution processes, (2) the Bureau's process for requesting funds from the Board, and (3) the Board's process for transferring funds to the Bureau.

Evaluation of the Bureau's Approach to Supervising Nondepository Institutions

The Dodd-Frank Act provides the Bureau with the authority to supervise depository institutions with more than $10 billion in total assets and their affiliates as well as certain nondepository institutions, such as mortgage companies,

payday lenders, private education lenders, and larger participants in other markets as defined by rules issued by the Bureau. An objective of the Dodd-Frank Act is to ensure that federal consumer financial law is enforced consistently without regard to whether a financial service provider is a depository or a nondepository institution. We plan to assess the Bureau's approach to supervising nondepository institutions.

Evaluation of the Bureau's Quality Management Program for Supervision Activities

The Bureau's Division of Supervision, Enforcement and Fair Lending has a quality management program that performs internal reviews related to the division's supervision activities. We plan to assess the design and effectiveness of the quality management program for supervision activities.

Evaluation of the Bureau's Periodic Monitoring of Supervised Institutions

To supplement its onsite examinations of supervised institutions, the Bureau conducts periodic offsite monitoring of all the depository institutions within its supervisory jurisdiction and certain nondepository institutions, including credit reporting agencies. This evaluation is assessing the Bureau's approach to periodic monitoring, including its implementation of periodic monitoring across the agency's regional offices.

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, 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.

Review of CFTC's Data Governance Program: Integrated Surveillance System (May 2019)

OIG's Office of Audits completed and published the subject audit report that highlighted challenges in collecting, storing, and securing market sensitive data. We assessed the maturity of CFTC's Data Governance program and corresponding practices as applied to facilitate the maintenance of Integrated Surveillance System (ISS). Specifically, we evaluated ISS Data Governance program practices for (1) defining business requirements, (2) extracting, transferring, and loading data (ETL), (3) managing changes, (4) maintaining stakeholder value, and (5) securing data.

We found CFTC's program exhibited a low maturity level, displaying numerous weaknesses, opportunities, and threats. We also found that ISS is less useful today than it was twenty years ago. Given that ISS was developed in the late 1990s, and that CFTC's markets have grown exponentially since that time, some degree of obsolescence may be expected. However, we believe adherence to an effective Data Governance program throughout its lifespan would have guarded against ISS obsolescence impacting CFTC operations, as well as the security concerns we noted.

We made five recommendations to enhance data governance and address security concerns noted. Management agreed to and completed the following recommendations to:

- Formulate a data governance framework;
- Address stakeholder business requirements for ISS;
- Upgrade data transmission standards and enhance ETL (extracting, transferring, and loading data) practices; and
- Ensure security compliance for ISS and other legacy systems.

Federal Information Security Management Act Review: FY 2019 (December 2019)

The objective of this audit was to evaluate CFTC's information security program and practices as required by FISMA. As follow-up to our recommendation that CFTC upgrade transmission standards and enhance ETL (from Review of CFTC's Data Governance Program: Integrated Surveillance System, previously discussed), we also performed cyber testing of market data transmission. The scope of testing was limited to FTP servers, email servers, mobile devices, and the CFTC portal.

We rated CFTC's IT security program as "Effective" for FY2019. Our rating is consistent with our contracted cyber security specialists' conclusion that CFTC's security controls protecting the confidentiality and integrity of sensitive market data during transmission is healthy.

To optimize its information security program, we recommended that CFTC:

- Develop periodic functional data restore tests and schedule taking into account business system criticality; and

- Remediate two penetration test vulnerabilities identified as "High" by contracted cyber security specialists; remediate four identified as "Medium" and consider "Low" vulnerabilities for action.

Management disagreed with the classification of "high" vulnerabilities but nevertheless agreed to enhance its security posture. This report is not public.

Office of Inspector General
Federal Deposit Insurance Corporation

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

Background

The Federal Deposit Insurance Corporation (FDIC) was created by the Congress in 1933 as an independent agency to maintain stability in the nation's banking system by insuring deposits and independently regulating state-chartered, non-member banks. The FDIC insures more than $7.8 trillion in deposits in 5,177 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 3,330 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 2020, our Office published its assessment of the Top Management and Performance Challenges Facing the FDIC. This assessment was based on our extensive oversight work and research relating to reports by other oversight bodies, review of academic and other relevant literature, perspectives from Government agencies and officials, and information from private-sector entities.

In addition, we conducted significant investigations into criminal and administrative matters involving complex multi-million-dollar schemes of bank fraud, embezzlement, money laundering, and other crimes committed by corporate executives and bank insiders. Our cases reflect the cooperative efforts of other OIGs, U.S. Attorneys' Offices, FDIC Divisions and Offices, and others in the law enforcement community throughout the country. These working partnerships contribute to ensuring the continued safety and soundness of the nation's banks and help ensure integrity in the FDIC's programs and activities. Finally, over the past year, we continued to coordinate with our financial IG counterparts and others on issues of mutual interest, most recently on matters relating to the Coronavirus pandemic.

The FDIC OIG also participated in the CIGFO Working Group's Survey of the Financial Stability Oversight Council and its Federal Member Agencies' Efforts to Implement the Cybersecurity Act of 2015, issued on January 15, 2020, and CIGFO's issuance of the Top Management and Performance Challenges Facing Financial Sector Regulators, issued in July 2019.

Top Management and Performance Challenges Facing the Federal Deposit Insurance Corporation

Pursuant to the Reports Consolidation Act of 2000, the OIG identified the following Top Management and Performance Challenges facing the FDIC. This year, we identified nine areas representing the most significant challenges for the FDIC, a number of which have implications to the financial sector, and ways to improve financial oversight. The identification of these challenges helps the FDIC and other policymakers to identify the primary risks at the Agency, and provides guidance for our Office to focus its attention and work efforts, as shown in the following summaries of each of these challenges.

Keeping Pace with Emerging Financial Technologies: Emerging technologies promise potential benefits but also introduce risk. Increased digital interconnections with multiple avenues to access banking systems elevate cybersecurity risk because an incident at one digital juncture has the potential to infect the banking system. The FDIC's challenge is keeping pace with new technology and the associated risks to banks, third-party service providers, and the banking system.

Enhancing the FDIC's Information Technology (IT) Security Program: As of June 2018, the FDIC had 338 IT systems that collect, store, or process Personally Identifiable Information (PII) and sensitive information. The FDIC also has legacy systems that are becoming difficult and expensive to maintain. The FDIC is modernizing its technology and must maintain the security of information within its systems as the IT environment evolves.

Ensuring the FDIC's Readiness for Crises: The FDIC identified two important lessons learned following the recent financial crisis: (i) the importance of crisis readiness planning; and (ii) quickly addressing emerging supervisory risks. Best practices identify the principles and elements of effective preparedness that collectively provide a framework for crisis planning efforts. Adopting such a framework strengthens the FDIC's ability to respond to a crisis in a timely and effective manner.

Sharing Threat Information with Banks and Examiners: Federal Government agencies gather a substantial volume of information related to the safety and soundness of financial institutions in the United States. Bankers need to receive actionable information in order to respond to threats in a timely manner. FDIC examiners responsible for supervised institutions should be aware of threats directed toward those institutions to understand their impact and make necessary supervisory adjustments. FDIC policy makers should be aware of emerging threats to ensure that relevant threat information is disseminated to banks and examiners, and to be able to adjust examination policy and procedures, and supplement or modify the regulatory scheme.

Strengthening the Governance of the FDIC: The Federal Deposit Insurance Act vests the management of the FDIC in its Board of Directors. The FDIC Board delegates authority to FDIC senior leaders to fulfill the Agency's mission, including implementation of its Enterprise Risk Management program. The FDIC should ensure that it is identifying and managing risks, and making data-driven acquisition decisions.

Overseeing Human Resources: Within the next few years, the FDIC will need to navigate a potential wave of retirements, reverse attrition trends among its core examination workforce, and hire staff with skills to match technology innovation. Effective management of these challenges limits the impact of leadership and skill gaps, and the loss of institutional experience and knowledge due to retirements.

Keeping FDIC Facilities, Information, and Personnel Safe and Secure: The FDIC is responsible for protecting approximately 6,000 employees and 3,000 contract personnel who work at 94 FDIC-owned or leased facilities throughout the country. The FDIC also has significant responsibility for its systems containing PII and sensitive PII related to employees, contractors, bank management, and deposit holders. The challenge for the FDIC is to maintain appropriate processes to safeguard facilities, information, and personnel.

Administering the Acquisition Process: In 2018, the FDIC spent nearly $500 million on contracts, with the largest expenditures for IT and administrative support services. The FDIC currently oversees acquisitions on a contract-by-

contract basis—rather than on a portfolio-wide basis—and it does not have an effective contracting management information system to readily gather, analyze, and report portfolio-wide contract information across the Agency and does not maintain certain key data elements. FDIC contract oversight should also include consideration of supply chain risks.

Measuring Costs and Benefits of FDIC Regulations: The FDIC does not currently have a consistent process in place to determine when and how to conduct cost benefit analysis in order to ensure that the benefits of a regulation justify its costs. Further, the FDIC does not have criteria in place to distinguish among rules that are sufficiently "significant" to require cost benefit analysis. We also note that conducting retrospective cost benefit analyses on existing rules would help the FDIC ensure that its rules are currently effective and achieve their intended objectives and outcomes.

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

During the 12-month period ending March 31, 2020, the FDIC OIG issued 12 audit, evaluation, and other products and made 61 recommendations to strengthen controls in FDIC programs and operations. Our work covered diverse topics such as information security and cyber threats, supervisory activities, and the FDIC's rulemaking process, among others. Results of several of these reviews are presented below.

Preventing and Detecting Cyber Threats

Our Office audited the effectiveness of two security controls intended to prevent and detect cyber threats on the FDIC's network: Firewalls; and the Security Information and Event Management (SIEM) tool. The FDIC's firewalls and SIEM tool operate in concert with other network security controls as part of a defense-in-depth cybersecurity strategy.

The FDIC has deployed firewalls at the perimeter and interior of its network to control the flow of information into, within, and out of the network. These network firewalls use rules to enforce what traffic is permitted. The FDIC's SIEM tool operates to analyze network activity and detect indications of potential cyber threats that may have bypassed the firewalls and other security controls. The tool runs automated queries (known as "Use Cases") to identify events or patterns of activity that may indicate a cyber attack.

We identified weaknesses that limited the effectiveness of the FDIC's network firewalls and SIEM tool in preventing and detecting cyber threats, including:

- The majority of firewall rules were unnecessary. Also, many firewall rules did not have sufficient justification. Several factors contributed to these weaknesses, including an inadequate firewall policy and supporting procedures, and an ineffective process for periodically reviewing firewall rules to ensure their continued need.

- Firewalls did not comply with the FDIC's minimally acceptable system configuration requirements. In addition, the FDIC did not update its minimum configuration requirements in a timely manner to address new security configuration recommendations by the National Institute of Standards and Technology.

- The FDIC did not always require administrators to uniquely identify and authenticate when they accessed network firewalls.

We found that the FDIC properly set up the SIEM tool to collect audit log data from key network IT devices. In addition, the SIEM tool effectively formatted the data to allow for analysis of potential cyber threats. However, the FDIC did not have a written process to manage the ongoing identification, development, implementation, maintenance, and retirement of Use Cases for the SIEM tool.

We made 10 recommendations intended to strengthen the effectiveness of the FDIC's network firewalls and SIEM tool in preventing and detecting cyber threats. The FDIC concurred with our recommendations.

The Minority Depository Institution Program at the FDIC

Minority Depository Institutions play a vital role in assisting minority and underserved communities and are resources to foster the economic viability of these communities. We evaluated the FDIC's Minority Depository Institution (MDI) Program.

The FDIC considers an institution to be an MDI if it is a Federally-insured depository institution where a majority of a bank's voting stock is owned by minority individuals; or a majority of the institution's Board of Directors is minority and the institution serves a predominantly minority community.

The Financial Institutions Reform, Recovery, and Enforcement Act of 1989 (FIRREA) required the Secretary of the Treasury to consult with the FDIC on methods for best achieving the five statutory goals aimed at preserving and promoting MDIs. In keeping with the requirements of FIRREA, the FDIC adopted an MDI Policy Statement describing its interpretation of ways to preserve and promote MDIs and implement the goals.

We concluded that the FDIC achieved its program goals as outlined in the MDI Policy Statement. That is, the FDIC took actions to preserve and promote MDIs, and preserve the minority character of MDIs; provided technical assistance to MDIs; encouraged the creation of new MDIs; and provided MDI training sessions, education, and outreach efforts.

Notwithstanding these efforts, we found that the FDIC did not evaluate the effectiveness of key MDI Program activities. Specifically, the FDIC did not assess the effectiveness of its supervisory strategies and MDI technical assistance. We also determined that the FDIC should further assess the effectiveness of its MDI training sessions, education, and outreach, including the benefit and value that they provide.

The FDIC also did not define the types of activities that it considered to be MDI technical assistance, as distinct from training, education, and outreach events. Additionally, while the FDIC provided training, education, and outreach events, the MDI banks, FDIC Regional Coordinators for MDIs, and representatives from MDI trade associations requested that the FDIC provide more such events.

Our report contained five recommendations to improve the FDIC's MDI Program. FDIC management concurred with the recommendations.

Cost Benefit Analysis Process for Rulemaking

Through the Banking Act of 1933, Congress provided the FDIC with the authority to promulgate rules to fulfill the goals and objectives of the Agency. The Administrative Procedure Act defines a rule as the whole or part of an agency statement "designed to implement, interpret, or prescribe law or policy or describing the organization, procedure, or practice requirements of an agency." Rulemaking is the "agency process for formulating, amending, or repealing a rule."

Cost benefit analysis informs the agency and the public whether the benefits of a rule are likely to justify the costs, or determines which of various possible alternatives would be the most cost effective.

In our review, we found that the FDIC's cost benefit analysis process was not consistent with widely recognized best practices that we identified, as noted below:

- The FDIC had not established and documented a process to determine when and how to perform cost benefit analyses. As a result, the FDIC's process did not ensure the appropriate depth of analyses was performed; resulted in inconsistent analyses; and limited public awareness and transparency.

- The FDIC did not leverage the expertise of its Regulatory Analysis Section economists during initial rule development.
- The FDIC did not require the Chief Economist to review and concur on the cost benefit analyses performed, which is an important quality control.
- The FDIC was not always transparent in its disclosure of cost benefit analyses to the public. The FDIC did not publish why a cost benefit analysis was or was not performed; the reason for the depth of analysis performed; the scope and methodology used; and the analysis performed.
- The FDIC did not perform cost benefit analyses after final rule issuance. Absent such analyses, the FDIC may not identify duplicative, outdated, or overly burdensome rules in a timely manner and may not ensure that its rules are effective and have achieved their intended objectives and outcomes.

We made five recommendations designed to improve the FDIC's cost benefit analysis process. Management concurred with four recommendations and partially concurred with one recommendation.

Offsite Review Program

The Federal Deposit Insurance Act requires onsite examinations of FDIC-insured financial institutions at least once during each 12-month period. Between onsite examinations, an institution's financial condition may change. Therefore, the FDIC designed the Offsite Review Program to identify emerging supervisory concerns and potential problems between onsite examinations so that it could adjust supervisory strategies appropriately.

We evaluated whether (1) the Offsite Review Program identified highly rated institutions (those rated "1" and "2") with emerging supervisory concerns; (2) the Program resulted in the FDIC appropriately adjusting the supervisory strategies for these institutions in a timely manner; and (3) the adjusted supervisory strategies were effective.

We found that the Offsite Review Program identified 1- and 2-rated institutions with emerging supervisory concerns related to rapid growth, noncore funding, deteriorating financial trends, or those identified by Regional Offices. However, the FDIC should:

- Evaluate additional methods and new technologies to identify institutions with other types of emerging supervisory concerns. These could include concerns related to internal controls, credit administration, and management practices;
- Enhance the Offsite Review Procedures to provide detailed guidance for Case Managers regarding the offsite review process, such as determining the scope and methodology of offsite reviews; and
- Provide Case Managers with training to ensure consistent application of offsite review procedures.

When an emerging supervisory concern was identified for highly rated institutions, we found that the FDIC appropriately adjusted its supervisory strategy in a timely manner; and the adjusted supervisory strategies were effective.

We made three recommendations to improve the Program. Management agreed with all recommendations.

The FDIC's Information Security Program--2019

The OIG engaged a contract firm to evaluate the effectiveness of the FDIC's information security program and practices, as required by the Federal Information Security Modernization Act of 2014 (FISMA). 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.

Our 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. The six highest risk weaknesses are briefly described below.

Risk Management
The FDIC had not yet completed an inventory of risks facing the FDIC, or a Risk Profile to help manage and prioritize risk mitigation activities. The FDIC also needed to develop a method and strategy to classify risk ratings and risk profiles of applications and systems, and develop and communicate the FDIC's information security Risk Tolerance level and Risk Profile.

Network Firewalls
In a previous report, we found that many of the FDIC's network firewall rules that controlled the flow of inbound and outbound traffic lacked a documented justification and the majority were unnecessary. The FDIC took steps to address these weaknesses, but further actions are needed.

Privileged Account Management
Hackers and other adversaries target administrative accounts to perform malicious activity, such as exfiltrating sensitive information. Our report identified vulnerabilities related to these accounts that increased the risk of unauthorized network access or malicious activity.

Protection of Sensitive Information
We conducted unannounced walkthroughs of selected FDIC facilities and identified significant quantities of sensitive hard copy information stored in unlocked filing cabinets and boxes in building hallways. We also identified instances in which sensitive information stored on internal network shared drives was not restricted to authorized users.

Security and Privacy Awareness Training
FDIC employees and contractor personnel with network access must complete security and privacy awareness training within 1 week of employment, and annually thereafter. If not, their network access is revoked. We identified 29 network users who did not satisfy the FDIC's awareness training requirement but still had access to the network.

Security Control Assessments
Our report discusses instances that occurred in 2016 and 2017 in which security control assessors did not test the implementation of security controls, when warranted. Instead, assessors relied on narrative descriptions of controls in FDIC policies, procedures, and system security plans and/or interviews of FDIC or contractor personnel.

The FDIC was working to address six recommendations from prior FISMA audit reports to strengthen controls in the areas of risk management, contactor-provided services, Plans of Action and Milestones, and vulnerability and compliance scanning. This FISMA report contained three new recommendations to ensure employees and contractor personnel properly safeguard sensitive electronic and hardcopy information, and network users complete required security and privacy awareness training. The FDIC concurred with these three recommendations.

Ongoing audit and evaluation reviews at the end of the CIGFO annual reporting period were addressing such issues as the FDIC's readiness for crises, background investigations, enterprise risk management, allocation and retention of safety and soundness examination staff, and security of the FDIC's mobile devices, among others.

FDIC OIG Investigations Seek to Ensure Integrity in the Banking Sector

OIG investigations over the past months continued to complement our audit and evaluation work. Our investigative results over the 12 months ending March 31, 2020, included the following: 80 indictments; 40 arrests; 62 convictions; and potential monetary recoveries (fines, restitution, and asset forfeitures) of over $3.3 billion.

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 have been working to further develop our cyber capabilities to investigate computer crimes at banks. We also partner with other agencies, including the Small Business Administration, to identify fraud in the guaranteed loan portfolios of FDIC-supervised institutions. These investigations are important, as large-scale fraud schemes can significantly affect the financial industry and the financial condition of FDIC-insured institutions.

Importantly, at the end of March 2020, we were embarking on a number of initiatives related to the Coronavirus pandemic, including as a member of the Pandemic Response Accountability Committee, and by way of coordination with financial IG counterparts on CIGFO and with other IGs and federal law enforcement partners.

Former CEO and Chairman of Bankrupt Pharmaceutical Company Sentenced to 30 Years in Prison

Jack Kachkar, former Chief Executive Officer and Chairman of now bankrupt Inyx Inc., a multinational pharmaceutical company, was sentenced on July 2, 2019, to 30 years in prison, followed by 5 years of supervised release for his role in a $100 million scheme to defraud Westernbank of Puerto Rico. The losses from the scheme led to the eventual insolvency and collapse of Westernbank. Kachkar was also ordered to pay $103,490,005 in restitution to the FDIC, as receiver for Westernbank.

Evidence presented at trial showed that Kachkar orchestrated the scheme to defraud Westernbank by causing Inyx employees to make tens of millions of dollars-worth of fake customer invoices payable by customers in multiple countries, including the United Kingdom and Sweden. Those fake invoices were presented by the defendant to Westernbank to be valid. He also made false and fraudulent representations to Westernbank executives about purported and imminent repayments from lenders in other countries in order to convince Westernbank to continue lending money to Inyx.

Kachkar then made false and fraudulent representations to Westernbank executives stating that he had additional collateral, including mines in Mexico and Canada worth hundreds of millions of dollars, to persuade Westernbank to lend additional funds.

As a result of the scheme, Kachkar caused Westernbank to lend him approximately $142 million based on false and fraudulent invoices from customers. He used those funds for his own personal benefit.

Former Trader for Major Multinational Bank Convicted for Price Fixing and Bid Rigging in FX Market

On November 20, 2019, Akshay Aiyer, a former Executive Director at a major multinational bank, was convicted for his participation in an antitrust conspiracy to manipulate prices for emerging market currencies in the global foreign currency exchange (FX) market.

From at least October 2010 through at least January 2013, Aiyer conspired to fix prices and rig bids in Central and Eastern European, Middle Eastern and African (CEEMEA) currencies, which were generally traded against the U.S. dollar and the euro.

The defendant engaged in near-daily communications with his co-conspirators by phone, text, and through an exclusive electronic chat room to coordinate their trades of the CEEMEA currencies in the FX spot market. Aiyer and his co-conspirators also manipulated exchange rates by agreeing to withhold bids or offers to avoid moving the exchange rate in a direction adverse to open positions held by co-conspirators and by coordinating their trading to manipulate the rates in an effort to increase their profits.

By agreeing not to buy or sell at certain times, the conspiring traders protected each other's trading positions by withholding supply of or demand for currency and suppressing competition in the FX spot market for emerging market currencies.

The defendant and his co-conspirators took steps to conceal their actions by using code names, communicating on personal cell phones during work hours, and meeting in person to discuss particular customers and trading strategies.

Wells Fargo Agrees to Pay $3 Billion to Resolve Criminal and Civil Investigations into Sales Practices Involving the Opening of Millions of Accounts Without Customer Authorization

On February 21, 2020, Wells Fargo & Company and its subsidiary, Wells Fargo Bank, N.A., agreed to pay $3 billion to resolve their potential criminal and civil liability stemming from a practice between 2002 and 2016 of pressuring employees to meet unrealistic sales goals, through a "cross-sell strategy" to sell existing customers additional products. The pressure faced under this sales practice led to thousands of employees providing millions of accounts or products to customers under false pretenses or without consent, often through falsifying bank records and identity theft.

As part of its agreements with various U.S. Attorneys' Offices, the Commercial Litigation Branch of the Civil Division, and the Securities and Exchange Commission, Wells Fargo admitted that for years, it collected millions of dollars in fees and interest to which it was not entitled; harmed credit ratings of certain customers; and illegally misused customers' sensitive personal information, including customers' means of identification. The criminal investigation into false bank records and identity theft is being resolved with a deferred prosecution agreement in which Wells Fargo will not be prosecuted during the 3-year term of the agreement if it abides by certain conditions, including continuing to cooperate with further government investigations.

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

Office of Inspector General Federal Housing Finance Agency

Created by the Housing and Economic Recovery Act of 2008 (HERA), the Federal Housing Finance Agency (FHFA or Agency) supervises and regulates (1) the Federal National Mortgage Association (Fannie Mae) and the Federal Home Loan Mortgage Corporation (Freddie Mac) (together, the Enterprises), (2) the Federal Home Loan Banks (FHLBanks) (collectively, the regulated entities), and (3) the FHLBanks' fiscal agent, the Office of Finance. Since September 2008, FHFA has also served as conservator for the Enterprises. As of year-end 2019, the Enterprises collectively reported more than $5.7 trillion in assets. The FHLBanks collectively reported almost $1.1 trillion in assets.

Also created by HERA, the FHFA Office of Inspector General (OIG) conducts, supervises, and coordinates audits, evaluations, investigations, and other activities relating to the programs and operations of FHFA. OIG promotes economy, efficiency, and effectiveness and protects FHFA and the entities it regulates against fraud, waste, and abuse, contributing to the liquidity and stability of the nation's housing finance system. We accomplish this mission by providing independent, relevant, timely, and transparent oversight of the Agency to promote accountability, integrity, economy, and efficiency; advising the 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 12th year, are of unprecedented scope, scale, and complexity. FHFA's dual roles continue to present novel challenges. Consequently, OIG must structure its oversight program to examine FHFA's exercise of its dual responsibilities, which differ significantly from the typical federal financial regulator.

Our annual Audit, Evaluation, and Compliance Plan describes FHFA's and OIG's roles and missions; explains our risk-based methodology for developing this plan; provides insight into particular risks within five areas; and generally discusses areas where we will focus our audit, evaluation, and compliance resources.

On an annual basis, we assess FHFA's most serious management and performance challenges, which, if not addressed, could adversely affect FHFA's accomplishment of its mission. OIG continues to focus much of its oversight activities on identifying vulnerabilities in these areas and recommending positive, meaningful actions that the Agency could take to mitigate these risks and remediate identified deficiencies. 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

Under HERA, FHFA, as conservator, possesses all rights and powers of any stockholder, officer, or director of the Enterprises and is vested with express authority to operate the Enterprises and conduct their business activities. 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, 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.

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

OIG's body of work over the last five years has found that FHFA has limited its oversight of delegated matters largely to attendance at Enterprise internal management and board meetings as an observer and to discussions with Enterprise managers and directors. Read together, the findings in these reports demonstrate that, for the most part, FHFA, as conservator, has not assessed the reasonableness of Enterprise actions pursuant to delegated authority, including actions taken by the Enterprises to implement conservatorship directives, or the adequacy of director oversight of management actions. We have also found that 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.

As the Enterprises' conservator, FHFA is ultimately responsible for actions taken by the Enterprises, pursuant to authority it has delegated to them. FHFA's challenge, therefore, is to improve the quality of its oversight of matters it has delegated to the Enterprises for the duration of the conservatorships and ensure that its established processes are followed for non-delegated matters to promote reasoned decision-making.

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

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

FHFA has stated that its top priorities include "cement[ing] FHFA as a world-class regulator and [ ] restor[ing] Fannie Mae and Freddie Mac…to safe and sound condition by building capital to match their risk profiles." However, as demonstrated by 34 of our reports issued since October 2014, FHFA's existing supervision program for the Enterprises is materially deficient and its supervisory guidance falls short of the guidance issued by the Board of Governors of the Federal Reserve System, Office of the Comptroller of the Currency, and Federal Deposit Insurance Corporation.

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

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 (PII). Both the Enterprises and the FHLBanks have been the targets of cyberattacks.

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

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

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

The Enterprises rely heavily on counterparties and third parties to properly originate and service the mortgages the Enterprises purchase and third parties to provide operational support for a wide array of professional services. That reliance exposes the Enterprises to a number of risks, including the risk that a counterparty will not meet its contractual obligations, and the risk that a counterparty will engage in fraudulent conduct.

FHFA, however, lacks authority to supervise these counterparties and third parties. It reviews Enterprise management of their relationships with counterparties and third parties through its 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 risks related to their counterparties.

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

Conservatorship Operations

Compliance Review of FHFA's Process for Reviewing the Enterprises' Proposed FY 2019 and FY 2020 Annual Operating Budgets (COM-2020-003, issued March 13, 2020)

FHFA reviews and approves the Enterprises' proposed administrative operating budgets each year. In 2015, we made several recommendations to address deficiencies in FHFA's budget review process, including that FHFA "[r]evise the existing budget review process and staff the review process with employees who have the qualifications and experience needed for critical financial assessments of the proposed Enterprise budgets to permit FHFA to determine whether each Enterprise's budget aligns with FHFA's strategic direction and its safety and soundness priorities." FHFA committed to hire a financial analyst and to assign other employees "with relevant technical qualification and experience to support the budget review process." FHFA also committed that its Division of Conservatorship (DOC)[2] would "strategically consult" with other FHFA offices regarding proposed budgets. A review by our office found that FHFA met both commitments when reviewing the Enterprises' proposed FY 2019 and FY 2020 budgets.

Supervision of the Regulated Entities

FHFA Faces a Formidable Challenge: Remediating the Chronic and Pervasive Deficiencies in its Supervision Program Prior to Ending the Conservatorships of Fannie Mae and Freddie Mac (OIG-2020-002, issued March 30, 2020)

As HERA recognizes, FHFA's supervision of the Enterprises is of paramount importance to their safe and sound operation. Since October 2014, we have issued more than 40 reports on FHFA's supervision program for the Enterprises. Thirty-four of these reports, taken collectively, detailed chronic and pervasive deficiencies in the program itself, as well as in its execution. We have reported that DER has struggled to complete remediation of chronic and pervasive deficiencies in a timely manner, or has abandoned, not fully completed, or completed in form and not substance actions it undertook to remediate these deficiencies.

2 On January 30, 2020, FHFA's DOC was renamed the Division of Resolutions (DOR).

The FHFA Director announced that the Enterprises may emerge from conservatorship as early as 2021, and that FHFA is developing a "roadmap" by which to end those conservatorships. In written Congressional testimony, the Director stated that the Enterprises must be "well-regulated" before they can "responsibly" be released from conservatorship. He advised that FHFA's examination work must be "consistently rigorous, timely, and effective."

Effective February 3, 2020, the FHFA Director replaced the Deputy Director, DER, with a new Deputy Director and Associate Director of DER as part of an organizational "realignment." To assist this new leadership in rebuilding FHFA's supervision program for the Enterprises, we summarized the chronic and pervasive deficiencies that we have identified in previously published reports, by four programmatic elements:

Examination Guidance and Execution

- FHFA lacks clear and comprehensive examination guidance for supervision of the Enterprises and its guidance lacks the rigor of other federal financial regulators.
- FHFA failed to complete a significant number of targeted examinations planned for each year since 2012.

Adequately Sized Examiner Workforce with Necessary Qualifications and Training

- FHFA acknowledged in 2019 that it had not engaged in a systematic workforce planning process to determine whether it has the right staff size and skill mix to conduct its statutory supervisory responsibilities, despite its prior commitments in 2013 and 2014 to conduct such planning.
- Despite FHFA's recognition of the significant risks from the Enterprises' use of more than 100 "high-risk" models, it planned only a few targeted examinations of high-risk models (roughly 3% of those annually over six examination cycles) and completed a fraction of those examinations during the cycle for which they were planned. FHFA officials maintained that limited resources constricted FHFA's ability to examine more high-risk models.
- Notwithstanding its expenditure of $7.7 million over almost seven years, FHFA failed to establish a commissioned examiner program.
- These systemic failures by FHFA raise significant questions about its capacity to supervise the Enterprises.

Communication of Supervisory Findings

- FHFA failed to communicate Matters Requiring Attention (MRAs) directly to the Enterprises' boards of directors, even though these boards are responsible for ensuring that the MRAs are remediated.
- FHFA shared conclusions from its ongoing monitoring activities with the Enterprises' boards of directors before subjecting them to quality control review, creating a risk of communicating inaccurate information.

Quality Control

- Over the last eight years, FHFA has failed to establish a rigorous quality control function for its supervision program for the Enterprises.

Consequently, the challenge now facing FHFA is formidable. In its management response to our report, FHFA agreed that its supervision of the Enterprises is of paramount importance to their safe and sound operation and asserted

that management will continue to pursue the corrective actions to which it had previously committed. To remediate the deficiencies identified by us and by FHFA before the Enterprises are released from conservatorship, FHFA must accomplish a great deal in a relatively short period. Success will require a sustained, disciplined, and robust effort on the part of FHFA, led by an accountable senior executive.

Stakeholders should understand that, absent completion of meaningful remediation of deficiencies in its supervision program, FHFA may be unable to meet its statutory responsibilities to ensure the safe and sound operation of the Enterprises.

Information Technology Security

FHFA Should Enhance Supervision of its Regulated Entities' Cybersecurity Risk Management by Obtaining Consistent Cybersecurity Incident Data (EVL-2019-004, issued September 23, 2019)

Both the Enterprises and the FHLBanks have been the targets of cyber attacks. FHFA acknowledges that its regulated entities face significant cybersecurity risks and the Agency understands its responsibility to provide effective oversight of the Enterprises' management of cybersecurity risks. A 2015 Government Accountability Office (GAO) report on several federal financial regulators' oversight of cybersecurity threat mitigation by their regulated entities highlighted the value of centralized analysis of incident data, including trends analysis, and concluded that "[w]ithout collecting and analyzing data more consistently, regulators have not obtained information that could identify broader IT issues affecting their regulated entities, and better target their IT risk assessments." The GAO report also emphasized that "[c]ollecting trend information and analyses could further increase regulators' ability to identify patterns in problems across institutions, better target reviews, and better deploy the IT experts among their staff." We examined FHFA's requirements and practices for collecting and analyzing cybersecurity incident data between January 1, 2017, and April 30, 2019. Under existing FHFA guidance, the regulated entities are required to report specific cybersecurity incidents under limited circumstances. The regulated entities submitted only a handful of such reports to FHFA under this guidance during this time period.

To obtain information on additional cybersecurity incidents, DER has relied primarily on internal management reports that the Enterprises submit to FHFA. When comparing these internal reports, we found that Freddie Mac reported a significantly greater number of cybersecurity "events" and "incidents" than did Fannie Mae. Because each Enterprise defines cybersecurity events and incidents differently, DER lacked a consistently defined cybersecurity dataset on which to conduct trend analysis across the Enterprises. During 2019, DBR initiated a pilot program to collect and analyze data on each cybersecurity incident that occurs at each FHLBank and the Office of Finance to better understand the cybersecurity threat environment faced by them. DBR has developed a uniform template and definitions for the collection of standardized incident data. We found that FHFA does not have an agency-wide cybersecurity incident data analysis program based on a consistent dataset, and that the cyber-related incident data that DBR and DER collect from their regulated entities cannot be readily reconciled for comparison purposes. As a result, FHFA lacks sufficient information to conduct trend or other time-series analyses across its regulated entities and has not done so. We recommended that FHFA conduct inquiries and analyses to explain the large disparities in reported cybersecurity events and incidents between the Enterprises and evaluate the cybersecurity data it obtains from the regulated entities and revise, as appropriate, its existing cybersecurity reporting requirements.

Counterparties and Third Parties

Compliance Review of FHFA's Enterprise Non-Performing Loan Sales Program (COM-2020-002, issued February 26, 2020)

The Enterprises may sell non-performing loans (NPLs) to reduce the number of delinquent loans held in their retained portfolios and to transfer credit risk to the private sector. FHFA established multiple NPL program sales requirements, including post-sale reporting by NPL buyers to the Enterprises for a four-year period regarding borrower outcomes. After finding in 2017 that the Enterprises were not collecting all required information from NPL

buyers, we recommended that FHFA (1) determine the information necessary to ensure NPL program requirements are being met and update the reporting standards accordingly, and (2) direct the Enterprises to establish controls to prevent NPL buyers from abandoning vacant properties. In response, FHFA required the Enterprises to collect four additional data fields from NPL buyers and impose additional follow-up requirements on buyers for potentially vacant properties.

We initiated this compliance review to verify the Enterprises' compliance with these two corrective actions from June 2018 through November 2019. We found that Freddie Mac complied with the data collection requirements for the first corrective action but Fannie Mae did not. Fannie Mae provided us with its proposed plan to collect the data starting in 2020. Regarding the second corrective action, Fannie Mae reported that it is following up with NPL buyers on three potentially abandoned properties (out of 78,281 NPL sold) whereas Freddie Mac had not identified any such instances.

Examples of OIG Investigative Accomplishments

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

OI is the only federal law enforcement organization that specializes in deterring and detecting fraud perpetrated against the Enterprises, and its commitment to its mission is essential to the well-being of the secondary mortgage market. Collectively, Fannie Mae and Freddie Mac hold more than $5 trillion worth of mortgages on their balance sheets. Each year the Enterprises acquire millions of mortgages worth several hundreds of billions of dollars. The potential for fraud in these circumstances is significant. OI also investigates cases involving the eleven regional FHLBanks and, in some instances, cases involving banks that are members of the FHLBanks.

Civil Cases

Wells Fargo Agrees to Pay $3 Billion to Resolve Criminal and Civil Investigations into Sales Practices Involving the Opening of Millions of Accounts Without Customer Authorization

In February 2020, Wells Fargo & Co. and its subsidiary, Wells Fargo Bank, N.A., agreed to pay $3 billion to resolve three separate matters stemming from a years-long practice of pressuring employees to meet unrealistic sales goals – which led thousands of employees to provide millions of accounts or products to customers under false pretenses or without consent, often by creating false records or misusing customers' identities.

As part of the agreements, Wells Fargo admitted that it collected millions of dollars in fees and interest to which the company was not entitled, harmed the credit ratings of certain customers, and unlawfully misused customers' sensitive personal information.

The criminal investigation into false bank records and identity theft is being resolved with a deferred prosecution agreement in which Wells Fargo will not be prosecuted during the three-year term of the agreement if it abides by certain conditions, including continuing to cooperate with ongoing investigations. Wells Fargo also entered a civil settlement agreement under the Financial Institutions Reform, Recovery and Enforcement Act of 1989 (FIRREA) based on Wells Fargo's creation of false bank records. Wells Fargo also agreed to the U.S. Securities and Exchange Commission instituting a cease-and-desist proceeding finding violations of Section 10(b) of the Exchange Act and

Rule 10b-5 thereunder. The $3 billion payment resolves all three matters and includes a $500 million civil penalty to be distributed by the SEC to investors.

The 16-page statement of facts accompanying the deferred prosecution agreement and civil settlement agreement outlines a course of conduct over 15 years at Well Fargo's Community Bank, which was then the largest operating segment of Wells Fargo, consistently generating more than half of the company's revenue.

The top managers of the Community Bank were aware of the unlawful and unethical gaming practices as early as 2002. However, Community Bank senior leadership failed to take sufficient action to prevent and reduce the incidence of such conduct. Senior leadership of the Community Bank minimized the problems to Wells Fargo management and its board of directors, by casting the problem as driven by individual misconduct instead of the sales model itself. Community Bank senior leadership viewed negative sales quality and integrity as a necessary byproduct of the increased sales and as merely the cost of doing business.

Wells Fargo caused the FHLBank of Des Moines to make advances totaling $77 billion—more than it was entitled to receive—by fraudulently misstating its size and growth. Wells Fargo's misstatement had a negative effect on its value and stability, and caused the FHLBank of Des Moines both to downgrade Wells Fargo's rating and significantly reduce its advances.

Criminal Cases

Individuals Sentenced in $396 Million Fraud Scheme, Maryland

Between October 2019 and January 2020, three individuals were sentenced for their participation in a $396 million investment fraud scheme that operated from 2013 through September 2018.

According to court documents, Jay Ledford, a certified public accountant, started a company that purchased consumer debt portfolios—defaulted consumer debts owed to banks and others—which he sold to third party debt collectors. Ledford also solicited investors to supply capital to buy a portfolio or invest in his company. After learning of Ledford's financial success, Kevin Merrill formed his own debt collection business and obtained capital investors, but never purchased debt portfolios.

Beginning in 2013, Ledford, Merrill, and Cameron Jezierski perpetrated a Ponzi scheme which defrauded investors of more than $396 million. Specifically, Merrill and Ledford invited investors to join them in purchasing consumer debt portfolios. Ledford provided to Merrill fictitious sales agreements and other documents, including false tax returns, knowing that Merrill was using them to induce individuals to invest in his companies.

Ledford and Merrill falsely represented that the monies the conspirators paid to investors were "proceeds" from collections and/or flipping debt portfolios, when in fact, the proceeds were paid from funds provided by other investors. Merrill and Ledford provided monthly or quarterly reports to investors regarding the "purported progress of the portfolio and its recovery," which Ledford and Merrill created. The scheme to defraud took in over $396 million, and at the time of their arrests, the co-conspirators were attempting to obtain an additional $260 million from investors.

As part of the scheme, Merrill purchased a $10.5 million home in Naples, Florida, using a $4.5 million loan obtained from Florida Community Bank; that loan was pledged to the FHLBank of Atlanta. Additionally, Merrill obtained from an FHLBank member bank a $750,000 HELOC for a Maryland property he bought with stolen investor funds, and used the proceeds of this loan to continue the Ponzi scheme and pay investors.

For their roles in perpetrating this scheme, Ledford, Merrill, and Jezierski previously pled guilty to conspiracy to commit wire fraud. In addition to this charge, Ledford pled guilty to aggravated identity theft and a money-laundering transaction, and Merrill pled guilty to wire fraud.

Merrill was sentenced to 22 years in prison, 3 years of supervised release, and ordered to pay $189,166,116 in restitution. Ledford was sentenced to 14 years in prison, 3 years of supervised release, and ordered to pay $189,166,116 in restitution. Jezierski was sentenced to 24 months in prison, 2 years of supervised release, 1 year of home confinement, and ordered to pay $116,435 in forfeiture and $45,093,384 in restitution. The orders of restitution entered against Merrill, Ledford, and Jezierski are to be applied jointly and severally.

Trial Conviction of Business Owner and Guilty Plea of Participant in Multi-State Loan Modification Scheme with over 550 Victims, Kansas

In September 2019, Sarah Cordry was found guilty at trial on charges of conspiracy to commit mail and wire fraud, mail fraud, and wire fraud for her role in a loan modification/foreclosure rescue scheme.

Cordry, along with others, operated for-profit companies and devised a scheme to defraud homeowners with false promises of protecting them from foreclosure. Cordry and others conspired to fraudulently promise the victims to lower their interest rates, lower their monthly mortgage payments and help them obtain loan modifications. When victims received foreclosure notices, the co-conspirators told them not to worry about it. In some instances, the victims would stop making their monthly mortgage payments to their lenders and instead, make payments to companies controlled by the co-conspirators, who used the victims' monies for personal gain.

Over 550 victims have been identified in 24 states. The victims suffered over $1.2 million in direct monetary loss; this loss does not include additional fees paid by victims to their lenders or losses to the Enterprises and lenders caused by subsequent foreclosures.

In October 2019, Ruby Price was sentenced to one year and one day in prison, three years of supervised release, and ordered to pay over $1.3 million in restitution, jointly and severally, for her role this scheme. Price previously pled guilty to conspiracy to commit mail and wire fraud.

In addition, in April 2019, co-conspirator Tyler Korn was sentenced to 51 months in prison, three years of supervised release, and ordered to pay over $1.3 million in restitution, jointly and severally, for his role in this scheme. Korn previously pled guilty to conspiracy to commit mail and wire fraud.

FHLBank Executives Sentenced, Texas

During December 2019, the former FHLBank-Dallas President and CEO, as well as the former Chief Information Officer, were each sentenced to 60 months in prison, two years of supervised release, and ordered to pay restitution and attorney fees to the FHLBank of Dallas and its insurance carriers, totaling over $5 million.

Terence Smith, former FHLBank-Dallas President and CEO, and Nancy Parker, former Chief Information Officer, both previously pled guilty to conspiracy to make false statements to a Federal Home Loan Bank several days into their trial in a federal district court.

In their plea agreements, the pair admitted they submitted dozens of fraudulent expense reports to the FHLBank, claiming they had attended professional conferences they never visited—prompting the FHLBank to foot the bill for what was actually personal travel to Florida, California, and Nevada. They also admitted to repeatedly falsely reporting their number of unused vacation hours.

In November 2019, former FHLBank-Dallas Chief Financial Officer Michael Sims was sentenced to five years of probation and ordered to pay over $80,000 in restitution. Sims previously pled guilty to misprision of a felony.

The scheme cost the FHLBank more than $1.2 million—$780,000 in travel expenses, including airfare, limousine rides, concerts, vineyard tours, luxury hotel rooms, and lavish meals for Smith, Parker, Sims, and several colleagues, and $450,000 in unused vacation time reimbursements.

Fraud Scheme Operator Sentenced to 20 Years in Federal Prison and Co-Conspirators Plead Guilty for Conning Elderly Victims Out of Their Homes and Money, California

In September 2019, Michael Henschel was sentenced to 20 years in prison and three years of supervised release for running a multimillion-dollar real estate scheme that conned elderly people out of their homes, gouging them with fraudulent threats of litigation and extorting monthly payments for illegal foreclosure and eviction delay. Henschel previously pled guilty to mail fraud. In February 2020, Henschel was ordered to pay over $7.8 million in forfeiture of real property and nearly $4 million in restitution.

Henschel and his co-conspirators deceived vulnerable homeowners – typically elderly people in financial distress, some of whom spoke limited English. Henschel tricked the homeowners into signing fraudulent deeds on their properties with false promises that the deeds would help homeowners protect properties from creditors or enable them to get equity out of the properties. Unbeknownst to his victims, the deeds described fake loans that the homeowners were supposedly guaranteeing for third parties, and in signing the deeds, they were pledging their houses as collateral for these fake loans. Henschel used the fraudulent deeds to steal homes and money from the victims.

Henschel's criminal conduct devastated his victims, leaving some of them penniless. Many other victims had to face financial insecurity – even homelessness – in their old age as they struggled to pay for basic necessities such as food and clothing. Several victims lost homes that their families had owned for generations.

The real estate fraud scheme had two parts: one involving property theft and litigation extortion, and the other involving illegal foreclosure and eviction delay.

In the property theft and litigation extortion part of the scheme, Henschel filed fraudulent documents on titles to homeowners' properties and used these fraudulent filings to steal properties from some victims outright and to extort settlement payments from other victims in civil litigation. Henschel weaponized the state court litigation system against homeowners, using his specialized training and knowledge of the law (he attended law school but was never admitted to practice) to extort settlements from homeowners by dragging them through stressful lawsuits.

In the foreclosure rescue part of the scheme, Henschel and his co-conspirators used fraudulent filings to charge homeowners fees to delay foreclosure and eviction actions. Henschel and the others had homeowners sign fraudulent deeds that transferred interests to debtors in bankruptcy cases – but the bankruptcies were fraudulent and used solely as part of the fraudulent scheme, not as part of any genuine effort to restructure or eliminate debts.

Many of the fraudulent bankruptcies were filed in the names of fictional people and entities, and some involved stolen identities. Henschel and his co-conspirators sent fake deeds and fraudulent bankruptcy petitions to trustees to stop foreclosure sales. They delayed evictions in a similar way, mainly by filing fraudulent documents in state court unlawful detainer actions and then sending fraudulent documents to various county sheriff's offices.

Losses associated with this scheme are more than $17 million.

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

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

Background

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

HUD has two component entities that have a major impact on the Nation's financial system: the Federal Housing Administration (FHA) and 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 the largest insurer of mortgages in the world, having insured more than 49.5 million single-family and nearly 67,000 multifamily and healthcare facility mortgages since its inception in 1934. As of September 2019, FHA managed more than 8.5 million insured mortgages valued at $1.3 trillion. FHA receives limited congressional funding and is primarily self-funded through mortgage insurance premiums.

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

Ginnie Mae has an outstanding portfolio of guaranteed MBS securities valued at nearly $2.1 trillion. A majority of the MBS securities consist of FHA-insured mortgages. Ginnie Mae offers the only MBS securities carrying the full faith and credit guaranty of the U.S. Government, which means that its investors are guaranteed payment of principal and accrued interest. If an issuer of MBS securities fails to make the required pass-through payment of principal and interest to investors, Ginnie Mae will advance the shortfall, seize the issuer Ginnie Mae portfolio and assume responsibility for servicing of the loans in those MBS pools.

HUD's Top Management Challenges

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

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

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

Challenges Presented by the COVID-19 Pandemic

HUD has been provided more than $12 billion to perform its responsibilities under Coronavirus Aid, Relief, and Economic Security Act (CARES Act) in the following areas: (1) rental assistance, (2) mortgage loan forbearance, (3) assistance for vulnerable populations, (4) assistance for communities' response, and (5) continued performance of its mission.

As of April 21, 2020, HUD reported publicly that 95 percent of HUD staff is working remotely to continue HUD's mission and implement new CARES Act responsibilities. HUD will need to ensure that it can continue to perform essential mission functions in light of these additional program obligations and operational limitations. HUD already experiences significant challenges in the areas of human capital and procurement, financial management, information systems technology, and monitoring and oversight, as outlined in our 2020 Top Management Challenges Report. All of the new work required by HUD under the CARES Act will amplify these challenges.

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

HUD has the responsibility to ensure quality, affordable homes for all. The most basic standards for HUD properties is that they be decent, safe, sanitary, and in good repair. HUD's challenge is to address the full spectrum of housing needs from emergency homelessness, low rent public housing, multifamily and scattered site rental assistance, to single-family homeownership. Economic and demographic factors, as well as aging rental housing stock, continue to contribute to the nation's severe shortage of safe and affordable housing. Continuous action is needed by HUD to ensure that the quality and quantity of safe and affordable housing matches demand.

Through the CARES Act, Congress provided HUD more than $2.6 billion in supplemental rental subsidies for tenants who have lost income and to ensure that landlords who provide subsidized housing and face significant increases in costs due to the coronavirus pandemic are not forced out of the affordable housing market. The CARES Act also protects tenants of covered properties from eviction for 120 days. HUD will be challenged to ensure that these grantees provide additional rental subsidies to tenants properly and in a timely manner and accurately track and report on the expenditure of these funds. It is unclear whether HUD has the ability to determine whether eligible renters are aware of and their landlords are complying with the moratorium.

HUD's Solutions to an Aging Rental Housing Stock

HUD's strategies to address affordable housing have necessarily become creative. To address an estimated $35 billion capital needs backlog shortfall in public housing, HUD's Rental Assistance Demonstration (RAD) program encourages public housing agencies (PHAs) to transition public housing units to a private-public partnership model. HUD developed RAD to give PHAs a tool to preserve and improve public housing properties and address the estimated $35 billion in capital needs nationwide. Congress has allowed up to 455,000 HUD assisted units to participate in the RAD program. OIG audited a number of PHAs in fiscal years 2018 and 2019 to assess their conversion to the RAD program, and has found some issue with implementation of the program. For example:

The Little Rock Housing Authority, Little Rock, AR, Did Not Fully Meet Rental Assistance Demonstration Program Requirements

OIG found that the PHA did not ensure timely completion of its conversions, properly account for predevelopment costs as required, and resolve a potential conflict of interest. The Authority also did not have effective procedures to ensure that costs were properly supported and allocated. As a result, it did not support $1.9 million in predevelopment costs or ensure that another $829,000 would be properly accounted for, allocated, and supported. Revisions and postponements of its RAD program conversion plans adversely affected rehabilitation costs by requiring the same or similar tasks to be amended, updated, or reworked multiple times. Further, the delays resulted in reduced occupancy in anticipation of rehabilitation of units and hindered the Authority's ability to provide decent, safe, and sanitary housing to current and prospective tenants. OIG made multiple recommendations to correct the identified deficiencies. (Audit Report: 2019-FW-1001).

OIG is continuing to conduct PHA RAD audits nationwide in fiscal year 2020.

Multifamily project owners who receive tenant subsidies from HUD are also using alternative financing vehicles such as Low Income Housing Tax Credits and Municipal Revenue Bonds to leverage capital for aging properties. This alternate financing process is largely outside HUD control under its existing regulatory scheme. The long-term effect of both these approaches remains unknown. OIG's work demonstrates some negative effects that can derive from these funding models, such as the possible reduction of affordable housing stock at the conclusion of the initial contract, de-federalization of program funds, and regulatory oversight limitations caused by the absence of regulatory agreements when HUD does not insure the mortgage.

The current pandemic also presents a challenge to the HUD-assisted rental stock. Shelter-in-place orders prevent all but emergency maintenance on the affordable housing portfolio. In addition, HUD allowed public housing agencies to waive or postpone certain program safeguards, such as onsite inspections. It is unclear what the impact of deferred inspection and maintenance will be on an already aging portfolio. OIG is continuing to monitor HUD's efforts to increase the availability of quality, affordable housing as HUD implements these strategies to address this challenge.

HUD Has Not Referred Troubled Public Housing Agencies as the Law and Regulations Require

The Office of Public and Indian Housing (PIH) operates HUD's public housing programs. Public housing's mission is to provide safe, decent, and affordable rental housing for eligible low-income families, the elderly, and persons with disabilities. PHAs own and operate the public housing developments in which such residents reside. Approximately 1 million households live in public housing units, managed by some 2,890 PHAs. PHAs are responsible for managing Federal aid and operating their housing developments in compliance with their annual contributions contract, a contract between the PHA and HUD which outlines the applicable regulations and procedural requirements that PHAs must abide by to receive Federal funding. If a PHA fails to address critical issues, the law and HUD's regulations require specific actions, which the OIG found HUD was not taking.

OIG found that PIH had not referred troubled PHAs to the Assistant Secretary for PIH to take them over as the law and regulations require. Without this referral mechanism, a PHA could remain troubled for an indefinite period while conditions stagnate or deteriorate. OIG identified 18 PHAs that remained troubled for more than 2 years without being referred. PIH is creating a process for referring troubled PHAs, but the draft process reviewed would provide

more options to the Assistant Secretary than the law and regulations allow and PIH cannot meet the statutory deadlines for referral of a troubled PHA without substantial changes to the assessment process or changes to the law and regulations. We found that PIH's staff training on substantial default and receivership suggests remedies that do not fully comply with the law and regulations. Finally, PIH has not submitted an annual troubled PHAs report to Congress for at least 11 years as the law requires, thereby missing an opportunity to strengthen the accountability and transparency of its recovery process. OIG offered five recommendations to help PIH ensure that it oversees troubled PHAs in an effective manner that aligns with the law and regulations, while fostering transparency with Congress. (Evaluations Report: 2019-OE-0001)

Protecting the Mortgage Insurance Programs

HUD is a significant actor in the housing finance market, providing insurance to private lenders through the FHA, and expanding market liquidity through Ginnie Mae. FHA provides government insurance/guarantees on single-family mortgages, home equity conversion mortgages (HECMs), apartment buildings, residential health facilities and hospitals. By committing the full faith and credit of the United States to repayment of lenders should the borrower default, HUD expands affordable homeownership, rental housing, and healthcare facilities.

HUD is challenged in protecting the FHA mortgage insurance fund, which as of fiscal year 2019 insured approximately 15 percent of all mortgages in the United States. Through the Mutual Mortgage Insurance (MMI) fund,[3] FHA insures participating lenders against losses when borrowers default on loans, which allows lenders to make loans to higher risk borrowers. From October 2018 through September 2019, the MMI fund paid out approximately 16 billion in reimbursements for defaulted loans. For those claims for which the lender conveyed the property to HUD and HUD resold the property, as of fiscal yearend 2019, HUD recovered only about 53 percent of the funds paid out.

Without sufficient controls, oversight, and effective rules, FHA's MMI fund is at risk of unnecessary losses. Further, if insurance fees collected from borrowers cannot support the fund, HUD may be required to draw on federal appropriated funds as it did after the financial crisis.

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 the insurance fund due to HECMs,
- increased risk to Ginnie Mae from its nonbank issuers, and
- challenges related to Ginnie Mae's shift toward an entirely digital mortgage life cycle.

Lack of Sufficient Safeguards in FHA's Mortgage Insurance Programs

Consistent with our approach in prior years, OIG continued focusing on the safeguards in place to protect FHA insurance programs in our fiscal year 2019 oversight work. For example:

FHA Insured at Least $13 Billion in Loans to Ineligible Borrowers With Delinquent Federal Tax Debt

OIG audited FHA-insured loans from fiscal year 2018 to determine whether FHA provided insurance on loans that were made to ineligible, delinquent Federal tax debtors. OIG worked with the Treasury Inspector General for Tax Administration to identify the number of FHA-insured loans made to borrowers with delinquent Federal tax debt. In fiscal year 2018, FHA insured more than 56,000 loans worth $13 billion, which were not eligible for insurance

3 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.

because they were made to borrowers with delinquent Federal tax debt. As a result, FHA did not achieve the Office of Management and Budget's principles for Federal credit programs, and the FHA insurance fund was exposed to greater risk. OIG recommended that FHA require lenders to obtain the borrowers' consent to verify the existence of delinquent Federal taxes with the Internal Revenue Service during loan origination and deny any applicant with delinquent Federal tax debt not meeting FHA requirements. By implementing our recommendations, FHA could potentially avoid insuring $13 billion in ineligible loans annually. (Audit Report: 2019-KC-0003)

FHA Improperly Paid Partial Claims That Did Not Reinstate The Delinquent Loans

OIG audited the FHA to ensure that delinquent loans were reinstated to a current state by the use of partial claim loss mitigation. OIG determined that FHA paid improper partial claims that did not reinstate the related delinquent loans because it did not have system tools to prevent these partial claims from being paid, or monitoring designed to detect the improper partial claims. By using a statistical projection, OIG estimated that FHA paid improper partial claims totaling $27.1 million between April 2017 and March 2018. In doing so, the FHA insurance fund was unnecessarily depleted by more than $27.1 million in partial claims, and unless FHA addressed the deficiencies, it could pay an additional $27.1 million over the next year for partial claims that fail to cure the loan delinquencies. OIG recommended that HUD (1) take corrective action against lenders for the improper partial claims that did not reinstate the delinquent loans and had not been repaid, (2) design controls to protect the insurance fund from improper partial claims that did not reinstate the loans, and (3) update applicable guidance. (Audit Report: 2019-KC-0001)

OIG continues to focus on protecting the FHA mortgage insurance programs. As an example, an ongoing audit focuses on whether FHA insured-loans met the underwriting requirements for special flood hazard areas. HUD requires the underwriter of a potential FHA-insured loan to determine whether the property is located in a special flood hazard area, as designated by the Federal Emergency Management Agency (FEMA). The underwriter is required to obtain a life of loan flood certification from FEMA if the subject property is in a special flood hazard area. OIG's concern is that if FHA insures the loan on a property that is in a special flood hazard area and it sustains flood damage but was not insured under the FEMA program, the FHA insurance fund could incur substantial losses if the borrower defaults on the mortgage. OIG expects to issue this report in fiscal year 2020.

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

Large Losses to the Insurance Fund Due to HECMs

Further, OIG remains concerned about the continued adverse impact that HECMs have on the FHA insurance fund. HECM is a reverse mortgage program that enables eligible homeowners age 62 and older to borrow funds using the equity in their homes. The HECM portfolio has had a longstanding negative impact on the insurance fund. However, the past year proved more favorable for the portfolio overall, despite HECM claims increasing from $6.15 billion in fiscal year 2018 to $9.56 billion in fiscal year 2019. Although still negative, the HECM capital position improved from negative $13.63 billion at the end of fiscal year 2018 to negative $5.92 billion for fiscal year 2019, a $7.71 billion improvement.

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. However, 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. OIG expects to issue this report in fiscal year 2020.

Increased Risk to Ginnie Mae from its Nonbank Issuers

HUD is also challenged by the significant increase in the number of nonbanks 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 are financial institutions that offer only mortgage-related services, and thus have no depositor base. They are also less regulated than banking institutions. Nonbanks must have sufficient liquidity to advance payments to investors even when a borrower does not pay, and/or advance funds to purchase the loan out of the pool. Ginnie Mae noted in its 2019 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 [mortgage servicing rights]."

Challenges Related to Ginnie Mae's Shift toward an Entirely Digital Mortgage Life Cycle

In addition, the mortgage industry is moving toward an entirely electronic loan process. Ginnie Mae intends to do the same, however, it is unclear what role FHA is playing regarding digital mortgages. However, HUD, particularly FHA, has well-known technology challenges. Change will require adding new platforms and security measures required for digital mortgages. Risks include information security, data transfers and platform integration, and system functionality, all of which could lead to fraudulent activities. Significantly, this would include digital promissory notes which are the legal evidence of a debt. For Ginnie Mae, as its issuers adopt e-notes in particular, it will need to ensure that it can demonstrate legal ownership of the note, should the issuer default. Because the paper note will not exist, Ginnie Mae will be required to demonstrate in bankruptcy court that the electronic record is the original note and is secure.

In its fiscal year 2018 annual report, Ginnie Mae noted its commitment to modifying the MBS program to permit the inclusion of mortgages that exist only in digital form. Ginnie Mae noted in its fiscal year 2019 annual report that it continued to develop and establish policies and infrastructure to incorporate digital mortgages into its existing business model. Ginnie Mae also reported its intention to launch a pilot project in fiscal year 2020 to test and refine its approach. In December 2019, Ginnie Mae published an initial draft of its Digital Collateral Guide, which contains the requirements that address the acceptability of digital promissory notes and other electronic documents for Ginnie Mae pools and loan packages, as well as participation in its digital collateral pilot. It solicited input from stakeholders about the requirements in the Guide, which was to serve as the governing document for the pilot. In fiscal year 2020, Ginnie Mae continues its venture into the securitization of digital mortgages. OIG will continue to monitor Ginnie Mae's progress with digital mortgages in fiscal year 2020 and will be working to ascertain FHA's role in the program.

Investigations of Alleged Fraud

OIG also helps protect the FHA insurance fund by conducting investigations of alleged fraud against the fund, and securing recoveries. OIG completed 85 single-family investigations of fraud against the FHA insurance fund during the calendar year ending on March 31, 2020. A majority of the investigations focused on loan origination fraud, for both forward and reverse mortgages. Recoveries from these cases totaled nearly $125 million (both criminal and civil recoveries). For example:

Quicken Loans, Inc., Settled Allegations of Failing To Comply With HUD's Federal Housing Administration Loan Requirements

OIG assisted the U.S. Department of Justice in the civil investigation of Quicken Loans, Inc. The investigation was of Quicken's origination, underwriting, endorsement, and related certifications of FHA-insured mortgage loans between September 1, 2007, and December 31, 2011. HUD's direct endorsement lender program authorizes private-sector mortgage lenders to approve mortgage loans for FHA insurance. Quicken participated in HUD's direct endorsement lender program. The United States contended that Quicken knowingly approved loans that violated FHA rules while falsely certifying compliance with those rules. Between 2007 and 2011, Quicken allegedly submitted claims for hundreds of improperly underwritten FHA-insured loans. Quicken entered into a settlement agreement with the Federal Government to pay $32.5 million. The settlement was reached through mediation. The settlement agreement was neither an admission of liability by Quicken nor a concession by the United States that its claims were not well founded. (Memorandum: 2019-CF-1805)

Father and Son Imprisoned for More Than 7 Years for Defrauding the HUD Real Estate Owned Program

A father and son, Sergio Garcia, Sr. and Sergio Garcia, Jr., were sentenced in U.S. District Court to a total of 88 months imprisonment and 3 years supervised release. The duo were also ordered to pay $500,454 in restitution, with $496,389 due to HUD and the rest due to the victims. The Garcias were sentenced following their earlier guilty pleas to conspiracy to commit mail fraud. The two conspired with others to contract with HUD to buy hundreds of HUD real estate owned (REO) homes across two states and sell them for a profit on the same day as purchased. The purchase contracts provided to HUD stated that they or one of their businesses were purchasing the properties as investors and would pay with cash or use other financing not involving FHA. The conspirators used fraudulent letters to show that they or their company had access to the funds needed to complete each purchase. Once under contract to purchase homes from HUD, the conspirators advertised the homes for subsequent resale and placed their own For Sale signs at the homes. When the conspirators could not find a subsequent purchaser to buy the homes, they allowed their purchase contracts with HUD to expire and filed false liens on the homes for the full purchase price, thus impeding HUD's ability to sell the homes to other interested buyers. The Garcias filed such false liens on 87 REOs, delaying HUD's sales of those homes and leading to a loss of value of almost $500,000 in the eventual sales. HUD OIG and the Federal Bureau of Investigation (FBI) conducted this investigation. (Hammond, IN)

Trio Ordered to Pay Restitution of More Than $3.4 Million

Ira Davis, a recruiter; Henry Florez, an investor; and Michael Rogers, a loan officer, were sentenced in U.S. District Court in relation to their earlier guilty pleas to bank fraud. The three were sentenced to a collective 36 months incarceration and 8 years supervised release and ordered to pay $3,465,627 in restitution to HUD. Over a course of 2 years, Davis, Florez, and Rogers submitted or caused to be submitted false representations to financial institutions regarding the sales price of properties, the source of the downpayments, and the amount of sales proceeds. This false information on real estate contracts, loan applications, and HUD-1 settlement statements allowed the trio to assist individuals in qualifying for FHA loans and purchasing 16 properties for which they otherwise would not have qualified. The loss to HUD for the loans was more than $3.4 million. HUD OIG conducted this investigation. (Chicago, IL**)**

Mortgage Industry Professional Sentenced to 46 Months in Prison

Dilcia Mercedes, a mortgage payment processor, was sentenced in U.S. District Court in connection to her earlier guilty plea to money laundering and unauthorized access of a computer with intent to defraud. Mercedes was sentenced to 46 months incarceration and ordered to pay $2,087,697 in restitution to the mortgage company and the mortgage company's insurer. For nearly 3 years, Mercedes monitored unclaimed customer escrow accounts, then diverted the unclaimed escrow payments by accessing the mortgage company's computer system and having the payments sent via wire transfers and ACH transfers to bank accounts and prepaid debit cards controlled by Mercedes and others. Mercedes exceeded her computer access authorization by using a coworker's computer login and password to approve the fund transfers then making false entries canceling borrower escrow checks to make it appear as though customers had requested the unclaimed funds be wire transferred to their bank accounts. A total of 1,543 mortgages were impacted by this scheme, of which 211 were FHA-insured. HUD OIG, the Internal Revenue Service Criminal Investigation Division, and the Federal Reserve Board OIG conducted this investigation. (Camden, NJ)

Bank and Lender Executives Forced to Repay More Than $60 Million

The president, chief executive officer, and chief business strategist and an in-house counsel of a mortgage lender and the chief executive officer of a savings bank were sentenced in U.S. District Court to a total of 4 years imprisonment followed by 17 years supervised release. The conspirators were also ordered to pay $60.3 million in restitution to Ginnie Mae, $1 million in restitution to the Internal Revenue Service, and $120,000 in forfeiture. The lender originated FHA-insured mortgages that were packaged and sold as Ginnie Mae-guaranteed MBS. The conspirators took part in a scheme whereby they misappropriated funds from the lender's warehouse line of credit to pay the lender's operating expenses rather than using the funds for the intended purpose of paying off the first mortgages of FHA-insured refinanced loans. Further, the conspirators caused the bank, a troubled savings bank, which acted as a warehouse lender to the mortgage lender, to engage in transactions that gave the appearance that the bank had improved its financial position when it had not. The scheme resulted in a $1.84 million loss to the savings bank. HUD OIG, the Special Inspector General for the Troubled Asset Relief Program, and the Federal Bureau of Investigation conducted this investigation. (Central Islip, NY)

Fake Law Group to Serve 11 Years in Prison for Loan Modification Scam

Three individuals were sentenced in State Superior Court to a total of 11 years imprisonment and ordered to pay more than $2.5 million in restitution. The scam artists were sentenced after each pleaded guilty to 64 felony charges of conspiracy, grand theft, money laundering, and unlawful loan modification advance fees for their role in a loan modification scam. The fraudsters established businesses claiming to be law firms and solicited individuals seeking lower mortgage payments via mail advertisements. The trio promised loan modifications and charged the homeowners upfront fees without rendering services. In some instances, the group was able to secure a loan modification but had the homeowners send the payments to its company instead of the lenders. The fraudsters then kept the payments instead of forwarding them to the mortgage servicers. In total, they victimized 387 borrowers, to include 46 with FHA-insured properties, and used more than $2.4 million in ill-gotten gains for their personal use. HUD OIG, the Federal Housing Finance Agency OIG, and the Orange County District Attorney's Office conducted this investigation. (Santa Ana, CA)

Purported Investors Sentenced for Fraudulent Home Sale Scheme

Two individuals purporting to be investors were sentenced in U.S. District Court in relation to their earlier guilty pleas to identity theft, wire fraud, mail fraud, bank fraud, and bankruptcy fraud. The two were sentenced to a cumulative 105 months imprisonment and ordered to pay restitution totaling $581,386, of which $80,136 was due to FHA. The two were involved in a scheme in which they would convince distressed homeowners to sign over the rights to their properties via quit claim deeds with the promise that the investors would make payments to the homeowners at a later date. The investors would then send a promissory note to the lenders holding the mortgages and file a fraudulent satisfaction of mortgage at the recorder's office to resell the properties. The investors performed this scheme on six properties, three of which were FHA insured. HUD OIG and the FBI conducted this investigation. (South Bend, IN)

CARES Act Challenges Facing HUD

Under the CARES Act, Congress has provided borrowers with single-family mortgages insured by FHA up to 180 days forbearance, with the right to request an additional 180 days. And Congress has provided up to 90 days forbearance to apartment building owners with FHA-insured mortgages. Because the vast majority of FHA-insured loans are securitized MBS, nonpayment on FHA mortgages due to forbearance impacts payments to MBS investors, which could have a negative impact on the residential securities market. HUD, through FHA and Ginnie Mae, is tasked with ensuring that borrowers are provided needed forbearance while also protecting the financial system destabilized by borrower nonpayment.

HUD faces pandemic related challenges on several fronts. Initially, HUD must ensure that borrowers protected by forbearance are aware of their rights. Ginnie Mae must act to preserve the stability in the residential securities market

by closely monitoring and addressing the risk that continued forbearance creates for its counterparties. While Ginnie Mae has established a temporary assistance program for the MBS it insures for issuers who are unable to make full payments to investors, Ginnie Mae acknowledges that this assistance does not include taxes and insurance payments, which lenders and issuers must advance on behalf of the nonpaying borrowers. The assistance also does not include servicer fees, which would have been included in the borrowers' payment. Further, Ginnie Mae has limited insight into the actions of other market actors, such as government-sponsored enterprises, and credit lines used by its issuers. Prolonged forbearance may create a risk of default of one or more of the Ginnie Mae issuers due to an inability to pay amounts due on their MBS.

As forbearances end, FHA will be required to track and monitor lender and borrower agreements to repay the forborne amounts. In many cases, servicers will be able to file a partial claim with HUD, allowing the servicer to recoup lost funds from HUD's insurance funds. HUD will need to track and monitor transactions for millions of loans. Partial claims due to forbearance will likely have a significant impact on FHA's mortgage insurance fund. Failure of borrowers to pay insurance premiums as part of their monthly payment will also strain the mortgage insurance fund.

HUD OIG will continue to provide oversight in this area.

Administering Disaster Recovery Assistance

HUD plays a key role in assisting individuals and communities recovering from disasters. Since 2001, Congress has appropriated more than $83 billion specifically for disaster recovery assistance. In 2017 and 2018 alone, Congress appropriated $35.8 billion for recovery from Hurricanes Harvey in Texas; Irma in Florida, Georgia, South Carolina, and the U.S. Virgin Islands; Maria in Puerto Rico and the Virgin Islands; and Nate in Mississippi. While disaster assistance will be an ongoing challenge for HUD, disaster recovery in Puerto Rico is particularly urgent, given the scope of the devastation, the geographical challenge involved in providing recovery assistance on an island, questions regarding Puerto Rico's capacity to handle funds, and the slow pace of funds being provided for recovery projects.

The complexity and range of challenges experienced when recovering from disasters makes HUD's programs to support disaster recovery inherently risky and susceptible to fraud. . Disaster recovery appropriation funds may take decades to spend, as their purpose is for long-term recovery, which includes rebuilding homes and communities. HUD's primary program for disaster recovery assistance is its Community Development Block Grant Disaster Recovery (CDBG-DR) program. Each disaster is funded through a supplemental appropriation separate from HUD's annual CDBG appropriation. Through the CDBG-DR program, HUD awards grants to States and units of local government for disaster recovery efforts, who work with subgrantees and contractors to implement recovery programs over several years. HUD's role is to rapidly begin funding jurisdictions, ensure that grantees have capacity to administer these funds through acceptable programs, and to balance the fluid nature of disaster recovery efforts with ensuring that the enormous amount of funds provided by HUD is being spent properly and effectively. Over the years, HUD has gained more experience and made progress in assisting communities recovering from disasters, but it continues to face these challenges in administering and overseeing these grants:

- ensuring that expenditures are eligible and supported,
- ensuring and certifying that grantees are following Federal procurement regulations,
- preventing fraud in disaster recovery assistance, and
- managing the multi-billion dollar CDBG-DR program through numerous federal register notices rather than codifying the program [4].

OIG has reported on HUD's challenges with CDBG-DR funding for 15 years, including fiscal year 2019. For example:

4 Codification of CDBG-DR would create a permanent statutory authority and regulations such as those that govern other disaster assistance programs.

The State of New York Did Not Ensure That Appraised Values Used by Its Disaster Program Were Supported and Appraisal Costs and Services Complied With Requirements

OIG audited the State of New York's Rising Buyout and Acquisition program to determine whether the State ensured that (1) the appraised fair market values used to determine award amounts under its program were supported and (2) appraisal costs for its program complied with applicable requirements and were for services performed in accordance with Federal, State, and industry standards. We concluded that the State did not ensure that (1) appraised fair market values used to determine award amounts under its program were supported and (2) appraisal costs complied with applicable requirements and were for services performed in accordance with applicable Federal, State, and industry standards. The State also did not ensure that it had a clear and enforceable agreement with the City of New York before relying on appraisal services provided by the City's contractor and did not ensure that the appraisal services were properly procured and performed. As a result, HUD and the State did not have assurance that more than $367.3 million paid to purchase properties was supported; more than $3.4 million disbursed for appraisal services was for costs that were reasonable, necessary, and adequately documented; and appraisal services were properly procured and performed. If the State improves controls over its program, it could ensure that up to $93.4 million not yet disbursed is put to better use. OIG recommended that HUD require the State to support the appraisal values of the properties purchased and strengthen controls to ensure that CDBG-DR funds used for appraisal services are for costs that are reasonable, necessary, supported, and for services that comply with applicable requirements. (Audit Report: 2019-NY-1002)

Grantees carry out the disaster recovery activities supported by CDBG-DR funding. The ability of these grantees to accomplish recovery from disasters and do so in an efficient and effective manner is critical to the recovery of the affected communities. To help HUD ensure that grantees have this ability, OIG conducts capacity reviews to determine whether these entities have the capability to administer their CDBG-DR grants in accordance with applicable regulations and requirements, particularly with regard to financial management, procurement, monitoring, and reporting. In fiscal year 2019, OIG conducted a capacity review of the Puerto Rico Department of Housing (PRDOH). HUD had awarded Puerto Rico $19.9 billion in disaster recovery funding, an unprecedented level of assistance.

The Puerto Rico Department of Housing, San Juan, PR, Should Strengthen Its Capacity To Administer Its Disaster Grants
OIG audited PRDOH to determine whether the PRDOH (1) had the capacity to administer its CDBG-DR grants in accordance with applicable regulations and requirements, and had in place financial and procurement policies and procedures that promoted the expenditure of funds and the acquisition of goods and services in accordance with Federal requirements. We concluded that the PRDOH should strengthen its financial and procurement capacity to administer its CDBG-DR grants in accordance with applicable regulations and requirements. Specifically, it could strengthen its capacity by improving its financial controls, improving its processes for preventing duplication of benefits, improving its procurement controls, and continuing to increase its staffing. Strengthening its capacity would help ensure that the PRDOH properly administers more than $19 billion in CDBG-DR funds in accordance with applicable requirements. In addition, the PRDOH did not follow Federal and its own procurement requirements when it acquired goods and services. As a result, HUD had no assurance that purchases totaling $416,511 were reasonable, necessary, and allowable. OIG recommended that HUD require the PRDOH to (1) develop adequate procedures for tracking monthly grant expenditures and reprogramming funds and program income, (2) review and update its policies and procedures to prevent duplication of benefits, (3) review and update its procurement policies and procedures, (4) continue to fill its vacancies, and (5) submit supporting documentation showing compliance with procurement requirements and that purchases totaling nearly $417,000 were reasonable and necessary costs or reimburse the program. (Audit Report: 2020-AT-1002)

OIG has planned and ongoing audits regarding grantee capacity and other areas of review for the State of North Carolina; State of Florida; City of Houston, TX; Harris County, TX; the U.S. Virgin Island's Housing Authority, among others, as well as additional audit work at PRDOH. We expect to begin reporting on these audits in fiscal year 2020.

Another area of significant overarching concern is that HUD has managed tens of billions in CDBG-DR funds for many years through a series of federal register notices rather than as a formal codified HUD program. OIG reported this concern in fiscal year 2018. A primary notice containing multiple requirements and waivers is issued for each disaster recovery supplemental appropriation. The primary notice largely repeats the same requirements and waivers from appropriation to appropriation. Thereafter, it is periodically updated by additional notices referring back to the original notices. Supplemental notices issued for more recent disasters may contain new standards that relate back to multiple prior disasters. In addition, some grantees manage multiple grants for different disasters. The number of notices continue to increase with each supplemental appropriation. As of May 2020, HUD had issued 77 notices for CDBG-DR covering $86.9 billion. Currently 75 of the notices are being used to oversee 109 active CDBG-DR grants totaling more than $81.4 billion.

HUD's process is cumbersome and confusing. It delays HUD allocations and forces grantees to cross-reference multiple notices to ensure they are following HUD requirements and waivers. CDBG-DR grantees also face additional challenges such as the need to coordinate the use of CDBG-DR funds with other disaster recovery programs that are initiated at different times and administered by other agencies. Since 2017, OIG has recommended that HUD codify this program to simplify the process and standards, and to speed up allocation. In March 2019, the Government Accountability Office found that, without permanent statutory authority and regulations such as those that govern other disaster assistance programs, CDBG-DR appropriations require HUD to customize grant requirements for each disaster in Federal Register notices—a time-consuming process that has delays the disbursement of funds. HUD officials have stated that permanently authorizing CDBG-DR would allow HUD to issue permanent regulations for disaster recovery and could help address grantee challenges. In May 2019, HUD's Secretary Carson testified that he would support codification, which he believed would be helpful. In fiscal year 2019, Congress proposed bills to codify CDBG-DR and OIG is hopeful that Congress will approve legislation requiring codification of the program, helping to speed up getting critical funding to those that have been impacted by disasters.

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

CARES Act Challenges Facing HUD

Under the CARES Act, Congress provided more than $5 billion to support local communities in responding to the pandemic through the CDBG program. Communities' pandemic response needs are new and extremely time sensitive, requiring HUD to develop new standards and issue CDBG funds with extraordinary speed. Further, the CARES Act more than doubles HUD's CDBG appropriation for fiscal year 2020 and adds different criteria for these funds. In audits dating back several years, OIG found that HUD was already challenged with monitoring this program and assessing risk.

HUD's efforts regarding other presidentially declared disaster relief efforts are ongoing. States are the initial grantees for disaster funding and must develop and oversee a network of local disaster relief entities. Many States are already severely taxed by pandemic efforts. As the United States enters hurricane season on June 1, HUD and its grantees may be challenged to respond in a timely manner to new disasters in addition to ongoing pandemic response activities.

Instituting Sound Financial Management

Over the last several years, HUD has progressed with its financial management governance; however, several areas remain unaddressed or require further improvements to fully address weaknesses and reach maturity of financial management processes. Specifically, HUD still experiences (1) weaknesses with financial management and internal controls; (2) risk mitigation responsibilities for enterprise risk management that are not fully assigned, and (3) antiquated financial management systems consisting of legacy systems and manual processes which contribute to our continued reporting on weaknesses in HUD's financial reporting processes. These continued weaknesses

increase the risk of a misstatement on HUD's financial statements. The progress made has allowed HUD to achieve a qualified audit opinion on its fiscal year 2019 consolidated financial statements; a notable improvement from the prior five years in which we were unable to provide an opinion on HUD's consolidated financial statements, resulting in a disclaimer of opinion.

However, one of HUD's component entities, Ginnie Mae, has also been unable to achieve an unmodified opinion and has received a disclaimer of opinion for the last six years. OIG has reported on Ginnie Mae's poor governance and a weak internal control framework in past years as the cause for the disclaimer of opinion. While Ginnie Mae has made progress in addressing these weaknesses, we encountered considerable challenges in auditing its fiscal year 2019 financial statements. Specifically, our work noted significant modeling concerns affecting Ginnie Mae's guaranty asset, guaranty liability, and allowance for loan losses. These issues concerned the appropriateness and reasonableness of the model methodologies, specifications, and model assumptions, which raised questions about the reliability of the significant accounting estimates produced by these models. Additionally, we were unable to audit the nonpooled loan assets due to documentation challenges to support balances for claims receivable and reimbursable costs, and insufficient time to complete necessary audit procedures for mortgage loans held for investment and acquired properties. These challenges related to 29 percent and 93 percent of Ginnie Mae's total assets and liabilities, respectively. Given the significance and pervasiveness of all of these limitations combined and our inability to perform all of the audit procedures that we considered necessary to reach and support a conclusion, we were unable to provide an opinion on Ginnie Mae's fiscal year 2019 financial statements.

While HUD has made progress in addressing weaknesses in its financial management environment, more progress is needed in targeted areas to strengthen public confidence in the government programs HUD administers and allow HUD's stakeholders to rely on HUD's financial position.

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,[5] the Community Development Revolving Loan Fund,[6] and the Central Liquidity Facility.[7]

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.

5 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.

6 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.

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

The agency's Office of National Examinations and Supervision (ONES) oversees examination and supervision issues related to consumer credit unions with $10 billion or more in assets and all corporate credit unions, which provide financial 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 federallyinsured credit unions nationwide. The insurance limit is $250,000 per depositor.

Credit Union Resources and Expansion

The 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

The 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.[8] The NCUA Inspector General (IG) is appointed by, reports to, and is under the general supervision of a three-member presidentially appointed Board. OIG staff consists of ten employees: the IG, the Deputy IG/Assistant IG for Audit, the Counsel to the IG/Assistant IG for Investigations, the Director of Investigations, five auditors, and an office manager. OIG promotes the economy, efficiency, and effectiveness of agency programs and operations, and detects and deters fraud, waste, and abuse, thereby supporting the NCUA's mission of facilitating the availability of credit union services to all eligible consumers through a regulatory environment that fosters a safe and sound credit union system. OIG supports this mission by conducting independent audits, investigations, and other activities, and by keeping the NCUA Board and the Congress fully and currently informed of its work.

Recent Work

Last year, we coordinated with our counterparts in CIGFO on issues of mutual interest, including on the Top Management and Performance Challenges Facing Financial-Sector Regulatory Organizations report that CIGFO issued in July 2019. This report reflected the collective input of the nine CIGFO Inspectors General that cybersecurity continued to be a critical risk facing the financial sector. The report included our observation that NCUA must acquire and deploy resources to enhance its cybersecurity oversight capabilities to maintain safety and soundness in the credit union industry.

We also participated in CIGFO's survey of FSOC and its federal voting member agencies' efforts to implement the Cybersecurity Information Sharing Act of 2015, the results of which CIGFO published in January 2020. The survey focused in part on the sharing of cyber threat information and related agency guidance. NCUA reported that it did not have the resources or mature capabilities to develop or sustain the development of procedures and policies, implement a repeatable process to efficiently analyze threat indicators, or to categorize and share the information with other entities. However, NCUA also reported that it has used indicators from other federal entities, although it did not disseminate indicators outside of NCUA. In addition, NCUA reported it used access controls, primarily two-factor authentication, to protect against threats.

We also conducted NCUA-specific work that could be instructive for the broader financial sector. First, in July 2019, we issued an audit report finding that the NCUA's Office of National Examinations and Supervision's examination program provided adequate oversight of credit union cybersecurity programs. This included, in 2018, implementing assessments of credit unions under its authority using the NCUA's Automated Cybersecurity Examination Tool (ACET). NCUA based ACET on the Federal Financial Institutions Examination Council's Cybersecurity Assessment Tool developed for voluntary use by banks and credit unions to help them identify their risks and determine their cybersecurity preparedness. NCUA also implemented a supplementary program offering credit unions a selection of voluntary cybersecurity assessments by independent third parties. After the audit, NCUA developed a long-term plan designed to better prepare the agency and credit unions to address cybersecurity threats, including ensuring that NCUA's systems and information are secure, implementing a new examination program focused on cybersecurity, and encouraging credit unions to develop their own cybersecurity plans that include strong security controls and actions to take in the event of a cyber attack and to ensure due diligence for their supply chains and third-party service providers.

Second, in December 2019, we issued an audit report regarding whether NCUA provided shared oversight of federally insured state-chartered credit unions (FISCUs) to assess their condition and address material risks that could negatively affect the NCUA's share insurance fund, and whether NCUA effectively monitored FISCUs using off-site monitoring tools and joint oversight processes with state supervisory authorities (SSAs). We determined that NCUA provided shared oversight of FISCUs and that it effectively monitored FISCUs using off-site monitoring tools.

8 5 U.S.C. app. § 8G.

However, we found that NCUA's regional offices did not have updated optional operating agreements with each individual SSA that defined roles and responsibilities, at even a high level, for joint on-site examinations of FISCUs; management needed to enhance its guidance to clarify reviews of FISCUs when NCUA examiners participated in joint examinations; and that supervisory examiners should consistently document their decisions on follow-up actions recommended by examiners after completing those reviews.

Third, in January 2020, in reviewing a revised NCUA instruction on the vetting and approval of changes in officials for newly chartered or troubled credit unions, OIG recommended that NCUA require a background investigation when a state-chartered credit union is converted into a federal credit union and when a foreign national is to become a credit union official, to be consistent with other financial regulators' practices. We further recommended that NCUA participate in financial regulators' sharing with one another prohibition orders and information about applicants or changed officials.

Finally, 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. Also in April, we provided information to the Council of the Inspectors General on Integrity and Efficiency's Pandemic Response Accountability Hotline about how to contact our office when it receives a complaint or feedback that relates to NCUA.

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

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

Background

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

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

The SEC's headquarters are in Washington, DC, and the agency has 11 regional offices located throughout the country. The agency's functional responsibilities are organized into 5 divisions and 25 offices, and the regional offices are primarily responsible for investigating and litigating potential violations of the securities laws. The regional offices also have examination staff to inspect regulated entities such as investment advisers, investment companies, and broker-dealers. In fiscal year 2019, the SEC employed 4,350 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.

SEC OIG Work Related to the Broader Financial Sector

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

Completed Work

The SEC's Office of Broker-Dealer Finances Provides Effective Oversight, But Opportunities To Improve Efficiency Exist, Report No. 559, February 26, 2020

The SEC prescribes broker-dealer net capital and risk assessment reporting requirements through various rules overseen by the Division of Trading and Markets' (TM) Office of Broker-Dealer Finances (OBDF). The largest broker-dealer firms can apply for and use an alternative net capital calculation for computing capital, if approved. Additionally, over-the-counter derivatives dealers can apply for and use value-at-risk and other statistical models to calculate capital once approved. OBDF monitors approved firms' monthly, quarterly, and annual filings and meets regularly with the firms' senior risk management staff. As of January 2020, there were five approved alternative net capital broker-dealer firms and three approved over-the-counter derivatives dealers. There were also 280 broker-dealers subject to risk assessment and material affiliate requirements.

We conducted this evaluation to assess the efficiency and effectiveness of TM's OBDF. Specifically, we sought to determine whether OBDF (1) provides effective oversight of broker-dealer compliance with capital and risk reporting requirements, in accordance with applicable rules and guidance, and (2) ensures efficient use of government resources to help achieve organizational goals and objectives.

We found that OBDF effectively monitors broker-dealer compliance with net capital and risk assessment rules and reporting requirements. Specifically, OBDF's sub-offices support its mission, and each suboffice has written policies and procedures with detailed processes that align with the organization's oversight requirements. Based on our review and testing of each sub-office's key processes and controls for oversight activities, we found that OBDF's processes were effective for overseeing broker-dealer net capital and risk reporting.

However, clarifications are needed in OBDF's Office of Broker-Dealer Inspections sub-office to reflect current practices and requirements. Specifically, certain updates to the Office of Broker-Dealer Inspections' written policies and procedures could strengthen controls over the inspection program, thereby improving efficiency.

We also obtained reasonable assurance of OBDF's efficient use of government resources, and we did not identify waste. However, we were unable to link OBDF's programs and resources to its goals and objectives because of the

lack of a unified, office-wide strategy. Also, OBDF did not make use of strategic planning, and did not have a formal succession plan. TM has drafted a strategic plan that includes goals for OBDF but, according to the TM Managing Executive, the final plan has been delayed because of the extensive rulemaking agenda. We reviewed TM's draft strategic plan and we discussed OBDF's strategic and succession planning with OBDF senior management who confirmed that, while there have been planning discussions, formal plans have not been established.

We issued our final report on February 26, 2020, and made three recommendations to address areas that can improve OBDF's oversight and efficiency, including recommendations to update its inspection policies and finalize needed rule updates and strategic plans. Management concurred with the recommendations, which will be closed upon completion and verification of corrective action. Because this report contains nonpublic information about the SEC's broker-dealer oversight program, we released a redacted version on our website at https://www.sec.gov/files/SECs-Office-of-Broker-Dealer-Finances-Provides-Effective-Oversight-but-opportunities.pdf.

Final Management Letter: Evaluation of the U.S. Securities and Exchange Commission's Delinquent Filings Program, December 17, 2019

The Delinquent Filings Program's (DFP) mission is to encourage reporting companies delinquent in filing periodic reports to become and stay current with the reporting requirements of the Securities Exchange Act of 1934 (the Exchange Act or Act) and to take action against those who do not. According to Division of Enforcement (ENF) officials, since 2004, DFP has generated about 5,000 revocation orders and 2,200 trading suspensions related to delinquent filers. Moreover, ENF's DFP employees worked through a backlog of about 2,000 delinquent filers and produce about 7 to 15 percent of all Commission actions each year.

To determine whether DFP's processes and internal controls were operating effectively, we conducted interviews; reviewed applicable laws, rules, regulations, and policies and procedures; and examined supporting documents for a sample of delinquent filers. We also surveyed ENF employees newly assigned to DFP. Generally, we found that DFP had adequate processes for identifying, tracking, and notifying delinquent filers and recommending related revocation orders and/or trading suspensions in accordance with applicable laws, rules, and regulations. Based on our testing, we also concluded that DFP adhered to its policies and procedures and maintained adequate documents to support its recommendations to the Commission. Finally, those employees who responded to our survey generally believed that they have received sufficient training and written guidance to fulfill their new DFP responsibilities. As a result, it appears that the DFP is well-positioned to continue pursuing its mission.

Nonetheless, two issues came to our attention that warrant management action. First, among other potential changes, the Division of Corporation Finance is assessing its ability to take a more active role in identifying companies that become delinquent or are likely to be delinquent, which could precede, overlap, and possibly impact the work conducted by ENF and the Division of Corporation Finance's Office of Enforcement Liaison. Second, delegating certain authority related to the Exchange Act could improve the efficiency of DFP.

We issued our final management letter on December 17, 2019, and made two recommendations. Management concurred with the recommendations, which will be closed upon completion and verification of corrective action.

Because this evaluation contains sensitive information, we released a redacted version on our website at https://www.sec.gov/files/Final-Mgmt-Ltr-Eval-of-the-SECs-Delinquent-Filings-Program.pdf.

Ongoing Work

Evaluation of the Office of Investor Education and Advocacy
The Federal securities laws task the SEC with a broad and diverse set of responsibilities, including engaging and interacting with the investing public through a variety of channels such as investor roundtables and education programs and alerts on the agency's SEC.gov website. The SEC's Office of Investor Education and Advocacy (OIEA), which each year has contact with millions of individuals, plays an important role in accomplishing the SEC's mission of protecting investors. Among other things, OIEA seeks to provide Main Street investors with the information they

need to make sound investment decisions and administers two programs to promote the SEC's mission. Specifically, OIEA's Office of Investor Assistance helps investors who contact the SEC with questions or complaints about perceived mishandling of their investments by investment professionals and others. In addition, OIEA's Office of Investor Education produces and distributes educational materials, leads educational seminars and investor-oriented events, and partners with other Federal agencies, state regulators, consumer groups, and self-regulatory organizations on financial literacy initiatives on behalf of the SEC in support of the agency's goals, the nation's Financial Literacy and Education Commission, and the National Strategy for Financial Literacy. OIEA's activities align with the SEC's strategic goal of enhancing outreach, education, and consultation efforts, including in ways that are reflective of the diversity of investors and businesses.

The OIG has initiated an evaluation of the SEC's OIEA. The overall objective of this evaluation will be 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.

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

Evaluation of the U.S. Securities and Exchange Commission's Tips, Complaints, and Referrals Program

The SEC's mission is to protect investors, maintain fair, orderly, and efficient markets, and facilitate capital formation. In pursuing its mission, the SEC encourages the public to file complaints or submit tips of 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 TCR). Each year, the SEC receives thousands of TCRs from members of the public, including industry professionals and attorneys, as well as referrals from self-regulatory organizations and exchanges, foreign and domestic Federal and local agencies, and law enforcement and other entities.

The OIG has initiated an evaluation of the SEC's TCR program. The overall objective of this evaluation will be to assess the SEC's management of the TCR program, including reviewing controls for collecting, triaging, and responding to credible allegations of violations of the Federal securities laws; safeguarding and maintaining TCR source materials, as required; and monitoring TCR program risks and trends.

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

Special Inspector General for the Troubled Asset Relief Program

Congress created The Special Inspector General for the Troubled Asset Relief Program (SIGTARP) in October 2008 in the Emergency Economic Stabilization Act (EESA), which authorized a $700 billion bailout and foreclosure assistance program known as TARP. TARP was the federal government's response to the 2008 financial crisis and resulting recession. Congress gave SIGTARP specific responsibilities to conduct investigations and audits over TARP, and to report quarterly on TARP. In 2009, Congress authorized SIGTARP to serve as a law enforcement office.

Background

SIGTARP is primarily a Federal law enforcement office protecting the interests of the American people by investigating illegal activity at financial institutions that received TARP funds, other TARP recipients in housing programs, and TARP-related scams. SIGTARP also conducts audits over TARP programs to identify waste, abuse, risk of fraud, ineffectiveness, mismanagement, and to recommend changes to open TARP programs that will save taxpayer dollars and prevent fraud, waste, and abuse.

All TARP programs are intended to promote financial stability. Treasury and Congress have extended TARP program multiple times. Currently, TARP programs are scheduled to continue through March 2024.

TARP is changing in response to COVID-19. In April 2020, SIGTARP recommended that Treasury put to better use unspent TARP dollars to be used for mortgage assistance for homeowners unemployed as a result of COVID-19. This would include those TARP funds that may not be spent in the future as well as those earmarked to be spent on less immediate problems, such as down payment assistance programs for new homebuyers. State finance agencies participating in TARP's Hardest Hit Fund have started reopening programs that were closed to new applicants to provide mortgage assistance for unemployed homeowners, which was the traditional use of the program.

SIGTARP protects the interests of Americans by combatting fraud, waste, and abuse related to the $442 billion that has been spent in TARP. Our focus on accountability of TARP recipients promotes confidence of the American people and markets that TARP dollars go where intended.

SIGTARP's Focus on Accountability of TARP Recipients Promotes Confidence

Restoring confidence was the goal of TARP. SIGTARP promotes confidence of Americans and markets that TARP dollars go where intended, by focusing on accountability of TARP recipients. SIGTARP investigations have resulted in 384 convicted (including 94 bankers and 79 of their co-conspirators). SIGTARP has a 97% DOJ conviction rate. Courts have sentenced to prison 302 defendants (including 77 bankers). Regulators banned 81 bankers. DOJ, the SEC and others brought enforcement actions against 24 banks/corporations. SIGTARP auditors identified more than $11 million wasted by state agencies on parties, lavish dinners, catered BBQs, gifts, boondoggle conferences, a Mercedes Benz, and more. SIGTARP focuses on recovering dollars lost to fraud and waste. More than $11 billion has been recovered

– a 31 times return on investment. Fiscal Year 2019 recoveries of $900 million are a 39 times return on investment from the Fiscal Year 2019 appropriated budget of $23 million. Already in Fiscal Year 2020, SIGTARP has recovered $81.6 million—a 3.7 times annual return on investment—in just six months, as compared to SIGTARP's entire FY 2020 appropriated budget of $22 million.

SIGTARP's Dedicated Law Enforcement/Auditors Reduced and Caught Crisis-Related Crime

Crisis-related crimes are crimes of opportunity. Expertise in TARP and bailed-out industries means we can see the same opportunities that criminals see. Our auditors identify fraud risk and vulnerabilities. Our investigators use an innovative intelligence-based strategy to find crime. SIGTARP caught 120 scammers convicted for defrauding nearly 30,000 homeowners nationwide seeking TARP foreclosure relief through TARP's HAMP program, which Treasury contracted with lenders to administer under Treasury's supervision. Courts sentenced 96 scammers to prison, including HOPE Services, later known as HAMP Services, who victimized more than 500 homeowners out of $2.5 million. TARP-funded demolitions became an opportunity for corruption and fraud. According to an indictment, Saigon Bank became an opportunity for a drug cartel to launder narcotics trafficking proceeds while the bank was in TARP.

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 works with the U.S. Department of Justice to hold accountable individuals and institutions that break the law. Our investigation into the largest financial crime in Delaware resulted in several Wilmington Trust bankers going to prison and recovered $270 million. We also caught bankers who personally profited from fraudulent loans and used TARP to hide their fraud.

Sigtarp Launches Financial Institutions Crimes & Fines Database

In December 2019, SIGTARP launched its Financial Institutions Crimes & Fines database, a public record of SIGTARP's law enforcement impact that has protected securities markets, the banking industry, investors, consumers, and taxpayers. The database, available at http://www.sigtarp.gov/database, gives the public a single point of access to information on nearly 400 criminally convicted defendants, 24 financial institutions/corporate enforcement actions, and civil fines from SIGTARP's law enforcement investigations. The database includes more than 300 defendants sentenced to prison, including 77 bankers, with 64 of the banker's co-conspirators, and 41 bank borrowers. Dozens of these bankers were senior executive officers, bank presidents, and chief financial officers at regional and community banks.

With the goal of deterring fraud and arming investors, markets, consumers, and companies with information they need to make informed financial decisions, SIGTARP has created an easy way to find the criminal convictions, civil judgments, and enforcement actions that have occurred as a result of SIGTARP investigations. While most of this information is publicly available, it is neither quick nor easy to access – limiting its effectiveness, particularly in a sea of information. Law enforcement can also use this database as a tool to identify past precedent and repeat offenders.

Proposal for a national financial fraud registry

On December 18, 2019, Special Inspector General Christy Goldsmith Romero proposed the creation of a national financial fraud registry (FFR), a modern data-driven approach to deterring fraud and protecting investors and consumers. The damage caused by financial fraud is so devastating that deterring fraudsters and protecting investors and consumers is a top priority of SIGTARP and other federal law enforcement offices. A centralized record of all crimes and fines related to financial fraud is a more effective and efficient way to achieve this important mission.

SIGTARP's pilot of its portion of the FFR – the Financial Institution Crimes & Fines Database – should serve as the first step in a coordinated approach by federal leaders to create a single public access point to information on fraud convictions and civil fines. Once established, each federal agency would register its convictions, sentencings, civil fines, and enforcement actions – a comprehensive record that the public can easily check before giving someone their money, their trust, and their business. Would-be fraudsters will not like that ease and accessibility, creating the powerful incentive to stop fraud plans that would result in their name in the registry. The federal government's comprehensive response to fraud would be transparent to the public. It would ease federal agencies' identification of repeat offenders.

Media coverage is the traditional method to let the public know how fraudsters are being held accountable, but it is not the most effective of efficient method. In a modern world with a sea of information, press releases from multiple agencies publicizing criminal fraud convictions and civil fraud fines can get lost. Media coverage is unreliable and often non-existent, even for major investigations. Deterrence suffers if the message of accountability is not received by would-be fraudsters. Many convictions and fines do not even get a press release – they are relegated to court and agency filings, read by few. Federal agencies supplement with executive speaking events and conferences that are limited to target audiences.

SIGTARP has seen firsthand through its investigations how fraud wrecks lives, businesses and communities. There is a more effective and efficient way for the federal government to arm people with the tools to protect themselves. Just as fraudsters have evolved their methods to take advantage of technology, so must law enforcement evolve our methods of deterrence and investor and consumer protection. The public does not care which federal agency investigates or prosecutes fraud. They do not want to have to search all corners of the internet for basic information about fraud. They care about not becoming a victim in the first place.

The most serious threat of fraud, waste, & abuse facing the government in TARP

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

(Program will continue to spend billions of TARP dollars until March 2024)

The largest open TARP program is the $23 billion Making Home Affordable (MHA) program and its signature program, the Home Affordable Modification Program (HAMP) that modifies mortgage (interest rates, term, etc.) for homeowners at risk of foreclosure to make mortgage payments more affordable and sustainable for homeowners. There are nearly 750,000 homeowners participating in all 50 states. California, Florida, New York, and Illinois each have more than 30,000 homeowners actively in HAMP.

SIGTARP conducts audits of the MHA program, and has an ongoing audit related to transparency of the program. In Fiscal Years 2018 and 2019, Treasury deobligated $4.3 billion from the program. In April 2020, SIGTARP recommended that any funds to be deobligated in the future be put to better use for unemployment mortgage assistance in TARP's Hardest Hit Fund given significant recent unemployment caused by COVID-19. This would be similar to Congress's action in the 2016 appropriations, which moved $2 billion from HAMP to the Hardest Hit Fund.

Treasury designed the program to have lenders administer the assistance. The sole reason why this program still exists is that lenders did not use speed in distributing this TARP foreclosure relief assistance during the housing crisis. For example, SIGTARP reported in 2015 that lenders (including banks that got TARP dollars in days) denied 70-80% of HAMP applicants, a total of four million people.

SIGTARP's top law enforcement priority is unlawful conduct by any of the banks and other financial institutions that received $21.1 billion or will continue to receive $2.4 billion for foreclosure prevention in TARP's MHA Program (data as of March 17, 2020). For example, our investigation uncovered that the floor at SunTrust buckled under the weight of unopened HAMP applications that SunTrust denied in mass and lied about to Treasury. The Department of Justice entered into a $320 million action, getting much of those dollars back to victim homeowners.

TARP spent $1.8 billion in Fiscal Year 2019, most of it by payments from Treasury to lenders in HAMP. For example, Treasury distributed $290 million to Ocwen Financial, $155 million to Select Portfolio Servicing (SPS), $131 million to Wells Fargo, $129 million to Nationstar, $101 million to JPMorgan Chase, $59 million to Bank of America, $19 million to Citigroup and more than $5 million each to National City Bank and CIT Bank. Treasury's payment of TARP to these financial institutions is not automatic, but instead requires that the financial institutions comply with the law and rules of the program. The administration of the program by financial institutions is under contract with Treasury, and subject to SIGTARP's oversight. Decisions that are illegal or violate program rules can result in harm to Treasury, homeowners, and taxpayers.

Significant payments of federal dollars to these lenders will continue through 2023, with the program ending in March 2024, unless extended. Through the first half of FY 2020, Treasury distributed $95.1 million to Ocwen Financial, $47.9 million to Wells Fargo, $24.6 million to Select Portfolio Servicing (SPS), $24.7 million to JPMorgan Chase, $21.3 million to Bank of America, $50.7 million to Nationstar, $8.1 million to Citigroup and $1.6 million to CIT Bank.

SIGTARP will continue to prioritize resources to counter this threat to ensure justice and safeguard Treasury, homeowners, and taxpayers. Despite criminal and civil enforcement actions and other wrongdoing against many of these financial institutions, Treasury has significantly scaled back its compliance reviews. The risk of fraud, waste, and abuse jeopardizes homeowners, communities, Treasury, the GSE's Fannie Mae and Freddie Mac, FHA, and Veterans Affairs agencies that participate in MHA. The billions Treasury has already paid in the program, and will pay in the future require significant oversight.

SIGTARP's Investigations

SIGTARP's work on financial institution fraud supports Justice Department prosecutions of individuals investigated by SIGTARP. The crime uncovered and investigated by SIGTARP hurt financial institutions.

SIGTARP's Select Investigative Results (April 1, 2019 to March 31, 2020)

Defendants Sentenced in Money Laundering Schemes in Operation Phantom Bank
In 2019-2020, a federal court sentenced four defendants to prison, and another defendant pleaded guilty, as part of a wide-ranging investigation into a series of schemes that involved narcotics trafficking and international money laundering. In total, 25 defendants have been charged across six indictments. At the center of the broad conspiracy is the lead defendant, Tu Chau "Bill" Lu, who was president and chief executive officer of TARP recipient Saigon National Bank from 2009 through January 2015. The indictments charge that Lu and five other defendants were members of a criminal organization involved in narcotics trafficking and international money laundering in countries that included the United States, China, Cambodia, Liechtenstein, Mexico, and Switzerland. The indictment alleges that Lu 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."

In the summer of 2019, a federal court sentenced Jimmy Sheng Lee and Wang Gao Wang to three year and two-year prison terms, respectively, for their roles in money laundering schemes. In separate schemes, both defendants conspired to provide cashier's checks in exchange for cash they believed was proceeds from drug activity. In exchange, the defendants believed they would receive a percentage of the funds laundered.

In October 2019, a federal court sentenced Raymond Tan to three years in prison for money laundering. Tan, along with his wife, Ruimin Zhao, and former East West Bank manager Vivian Tat, laundered cash through the bank. According to court documents and the evidence presented at trial, Tan and the other defendants led an informant into the bank's conference room where the informant provided $25,500 in cash that was then laundered into three "clean" cashier's checks issued through the account of a bank client. The informant was wearing a secret recording device and throughout the transaction the conspirators made statements demonstrating they knew money laundering was illegal.

Richard Cheung, who was convicted on a money laundering charge, was sentenced to one year and four months in prison. He conspired to provide cashier's checks in exchange for cash he believed was proceeds from drug trafficking. In a meeting with a confidential informant, Cheung requested assistance in moving cash out of mainland China because he was not satisfied with the speed and tax consequences of laundering money through casinos in Macau.

In February 2020, Mina Chau pleaded guilty to conspiracy to commit money laundering.

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.

Cooperating Defendant Sentenced to Time Served for Role in Massive Fraud Scheme that Contributed to Failure of TARP Recipient Sonoma Valley Bank That Resulted in a Complete Loss of $8.6 Million in TARP

In July 2019, a California federal court sentenced cooperating defendant James House to time served and three years of supervised release for his role in a massive fraud scheme that contributed to the failure of Sonoma Valley Bank and a complete loss to TARP of $8.6 million. As part of the sentencing, the court ordered House to pay $19,196,000 in restitution.

In August 2018, the court sentenced Sonoma Valley Bank CEO Sean Cutting and Chief Loan Officer Brian Melland to eight years and four months in prison, and attorney David Lonich to six years and eight months in prison, for a years-long, highly complex fraud scheme. On December 18, 2017, a federal jury convicted all three after trial. These bank officers conspired to make millions in illegal bank loans to "straw" borrowers, knowing that the loan proceeds would go to one bank borrower, real estate developer Bijan Madjlessi. In 2005, Madjlessi faced cash flow issues and the bank lent him money in excess of their legal loan limits through a series of straw borrowers. Bank CEO Cutting and Loan Officer Melland then tried to cover up the scheme by falsifying the bank's books and lying to bank regulators. During the fraud, the bank applied for TARP, with the CEO describing TARP as a "cookie jar" saying it only made sense for the bank to "take some."

James House became involved because, by 2009, Madjlessi had nearly $30 million in debt at Sonoma Valley Bank when one of his properties was foreclosed. To get the property back, Madjlessi conspired with House, to whom he owed hundreds of thousands of dollars for carpentry work. House agreed to act as a straw borrower, getting the loan from the bank in his name, and passing on almost all the proceeds to Madjlessi. In return, House was paid almost exactly what he was owed by Madjlessi. James House was the government's cooperating witness. When SIGTARP investigators approached House in 2011, his immediate reaction was to admit what he had done and offer to cooperate, which he did for more than eight years. He shot undercover video of Madjlessi and Lonich during which they described their plan and urged House to lie. House's crime was serious in that it directly contributed to the failure of the bank; however, House testified at trial for four days and received credit for his cooperation. After indictment, but prior to standing trial, Madjlessi died in a one car accident when his vehicle plunged over a cliff on Highway 1.

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

Federal Court Sentences Former Chief Financial Officer Craig On From Failed TARP Recipient United Commercial Bank

In October 2019, former United Commercial Bank (UCB) chief financial officer Craig On was sentenced by a federal court to two years probation and ordered to pay a $15,000 fine. On testified at the trial of UCB chief operating officer and chief credit officer, Ebrahim Shabudin, who was convicted at trial and sentenced to eight years and one month in prison.

After aggressive and risky loan-fueled growth, management of TARP recipient, UCB, fraudulently inflated the bank's financial performance by hundreds of millions of dollars. The bank later failed - one of the largest failures since the Great Depression - and $300 million in TARP funds was lost. During the crisis, in an attempt to have the bank appear to "break even," Shabudin and co-conspirators manipulated the bank's books and records, and issued false press releases, filings with examiners, and false financial statements. Then U.S. Attorney Melinda Haag said, "UCB is one of the largest criminal prosecutions brought by the U.S. Department of Justice of wrongdoing by bank officers arising out of the 2008 financial crisis."

As UBC's chief financial officer, On attested to the accuracy and completeness of financial information the bank provided to its accountants. While he knew that standard accounting practices required $67 million in potential losses to be disclosed, he purposely failed to have that information included in financial statements and lied when asked by the accountants if UCB had made full disclosures. On knew what he did was wrong but did it anyway because he thought disclosing the potential losses would cause the bank to collapse.

On was convicted of making a materially false and misleading statement to an accountant. He was also ordered by the Federal Deposit Insurance Corporation (FDIC) to pay a civil penalty of $150,000 and was banned from participating in the affairs of financial institutions. Shabudin was convicted of securities fraud and sentenced to eight years and one month in prison. He was also ordered by the FDIC to pay a civil penalty of $175,000 and was banned from participating in the affairs of financial institutions. Former senior vice president Thomas Yu, who also testified at Shabudin's trial, was convicted and sentenced to probation. The Justice Department deferred prosecution against Chris Chiem Lee, a manager at the bank. Lauren Tran, a vice president at the bank, had her guilty plea vacated due to cooperation.

SIGTARP was joined in the investigation by the FDIC Office of the Inspector General, the Inspector General for the Board of Governors of the Federal Reserve System, and the Federal Bureau of Investigation. The U.S. Attorney's Office for the Northern District of California prosecuted the case.

SIGTARP Agents Arrest Chief Executive Officer of TARP Recipient Noah Bank Who Was Indicted on Bribery and Fraud Charges

In May 2019, SIGTARP agents arrested Edward Shin, the chief executive officer of TARP recipient Noah Bank, a bank based in Pennsylvania. Shin was indicted on charges of Conspiracy to Commit Wire Fraud, Conspiracy to Commit Bank Bribery, Bank Bribery, and Theft, Embezzlement or Misapplication by Bank Officer. The charges were based on alleged conduct that began in 2009. Shin was indicted for allegedly soliciting and receiving bribes in connection with Small Business Administration guaranteed bank loans and commercial bank loans. Shin is charged with concealing that the loans were issued in violation of SBA rules. Shin allegedly siphoned off a portion of broker commissions on government guaranteed loans, even where there was no broker. Shin also allegedly caused the bank to issue a $950,000 SBA-guaranteed loan to a New York, New York business in which Shin had a secret interest. Allegedly, this loan later went into default resulting in a loss to the SBA of $611,491.

SIGTARP was joined in the investigation by Federal Deposit Insurance Corporation Office of Inspector General, Homeland Security Investigations, the Small Business Administration Office of the Inspector General, and the Federal Bureau of Investigation. The U.S. Attorney's Office for the Southern District of New York is prosecuting the case.

Former Bank Chief Lending Officer and Country Bank Loan Officer Sentenced to Prison for Fraud at Failed TARP Recipient Country Bank

On February 28, 2020, a federal court sentenced Dana Frye, the former executive vice president and chief lending officer of Country Bank of Aledo, Illinois to prison for five years. Frye was convicted of making false statements to the bank in October 2019. Andrew Frye, a loan officer at the bank who worked closely with his dad, Dana Frye, cooperated with prosecutors. Andrew Frye was convicted of loan fraud and sentenced to probation. As a condition of their sentences, both defendants are prohibited from ever working in the banking or financial industry again. The Fryes were arrested by SIGTARP special agents in October 2019.

While Dana Frye was working for Country Bank, he used his position to assist others in securing loans for various commercial real estate development projects without disclosing in bank records and loan applications that he stood to personally profit from the issuance of the loans. One such project was the development of a golf course in Sherrard, Ill., known as "Fyre Lake" that benefited from more than $20 million in loans from Country Bank.

Frye also helped secure loans to a number of real estate developments that retained Webgem, a management and account services company owned by Frye and his son. Frye did not disclose his interest in Webgem in bank records and loan documents submitted to Country Bank prior to the approval of these loans. Frye concealed his interest in these real estate developments and Webgem because he knew that Country Bank's policies prohibited loans to projects in which he had a financial interest.

In May 2009, Country Bank received a $4.1 million TARP bailout. In October 2011, Country Bank failed, leaving the FDIC with losses of more than $70 million. Other victims included Greenwoods State Bank, Burlington, Wis.; Blackhawk Bank & Trust, Milan, Ill.; and Citizens Bank of Mukwonago, Wisconsin; Blackhawk Bank & Trust, Milan, Illinois; and Citizens Bank of Mukwonago, Wisconsin. SIGTARP was joined in the investigation by the Federal Deposit Insurance Corporation Office of the Inspector General. The U.S. Attorney's Office for the Central District of Illinois is prosecuting the case.

Chief Executive Officer of TARP Recipient Cecil Bank Charged with Fraud

On February 20, 2020, SIGTARP special agents arrested Mary Halsey, the former president and chief executive officer of Cecil Bank of Elkton, Maryland, on federal charges of conspiracy to commit bank fraud, bank fraud, receipt of a bribe by a bank official, false statements in bank records, and false statements to a bank examiner. Treasury wrote off approximately $11 million from its TARP investment of Cecil Bank after the financial institution filed for bankruptcy in 2017.

According to the indictment, Halsey conspired with Daniel Whitehurst, who previously pleaded guilty to mail fraud, to defraud Cecil Bank related to a house in Elkton, Maryland, that had been foreclosed on and was owned by Cecil Bank. Halsey allegedly had the bank sell the house to Whitehurst for well below market value, not disclosing to the bank that Whitehurst was acquiring the house on her behalf and only acting as a straw buyer. She allegedly wired $75,000 to Whitehurst for the down payment, closing costs, and upgrades to the property that she requested. Later on, Halsey allegedly issued three checks to Whitehurst totaling $60,000 for improvements and monthly mortgage payments. The indictment alleges that, in return for Whitehurst acting as a straw buyer, Halsey assisted in the bank providing him a $650,000 bank line of credit.

Halsey allegedly also concealed the straw purchase of the property from a bank examiner. When asked about the sale of the home by a bank examiner for the Federal Reserve Bank of Richmond, Halsey allegedly falsely stated that she was "not totally familiar with [that] property" and that the bank had difficulty marketing the property and had not listed it with a realtor because of "issues with the county over the bonds outstanding."

SIGTARP was joined in the investigation by Federal Housing Finance Agency Office of the Inspector General, Federal Deposit Insurance Corporation Office of the Inspector General, and the Small Business Administration Office of the Inspector General. The U.S. Attorney for the District of Maryland is prosecuting the case.

SIGTARP has multiple investigations related to Cecil Bank. In April 2019, Mehul Khatiwala pleaded guilty to conspiracy to commit bank fraud and to three counts of bank fraud, in connection with a scheme to obtain by fraud loans from Cecil Bank to purchase hotels and a multifamily residential property, resulting in losses of more than $3.5 million. In June 2019, Zahid Aslam was sentenced to two and a half years in prison for making false statements to financial institutions, including Cecil Bank.

Nomura Securities International Inc. Trader's Conviction Upheld

On September 20, 2019, a federal appeals court for the Second Circuit upheld the conviction of Michael Gramins, a securities trader at Nomura. After a trial, in June 2017, a federal jury convicted Gramins of conspiracy to commit fraud related to Residential Mortgage Backed Securities (RMBS). Victims of the scheme charged in the indictment included funds through a TARP program that traded in RMBS. Subsequently to the jury verdict, the district court granted Gramin's motion for a new trial. The Court of Appeals reversed the district court and gave the district court instructions to reinstate the conviction. The court held that the materiality of Defendant's conduct brokering trades justified his conviction. SIGTARP was joined in the investigation by the Federal Bureau of Investigation. The United States Attorney for the District of Connecticut is prosecuting the case.

Securities and Exchange Commission Settled Charges that Nomura Securities International Inc. Misled Bond Customers for $25 Million

In July 2019, the Securities & Exchange Commission resolved civil charges against Nomura for failure to adequately supervise its traders in mortgage-backed securities. According to the SEC's order, Nomura traders misled customers about the prices at which Nomura had bought securities, with traders often pretending that they were still negotiating with a third-party seller when Nomura has, in fact, already bought a security. The SEC's orders further found that Nomura lacked compliance and surveillance procedures that were reasonably designed to prevent and detect this misconduct, which inflated the firm's profits at the customers' expense. Nomura was censured, will reimburse $24.9 million, which was the firm's profits on the trades tied to customer misrepresentations, pay a $1.5 million penalty, and improve its surveillance procedures and internal controls.

Federal Court Sentences CFO of Construction Company to Time Served and Supervised Release for Defrauding TARP Recipient Bank of Blue Valley

A federal court sentenced CFO of KC United, LLC Timothy Fitzgerald to time served and two years supervised release for defrauding Bank of Blue Valley by manipulating the company's finance records to falsify a profit, and falsifying a letter from an accountant. The bank relied on the falsified documents to extend loans, and lost more than $877,000 after KC United filed for bankruptcy. The bank's parent company received a $21.8 million TARP bailout. Treasury suffered a loss of approximately $500,000 on the TARP bailout, in addition to foregoing $4.9 million in missed dividend payments. SIGTARP was joined in the investigation by the Office of Inspector General for the U.S. Department of Labor, the U.S. Department of Labor Employee Benefits Security Administration, Internal Revenue Service Criminal Investigation Division, and the Federal Bureau of Investigation. The case was prosecuted by the U.S. Attorney's Office for the District of Kansas.

Federal Court Sentences Mortgage Company Executive to Three Years in Prison for Fraud Scheme Related to A Bank's Application for TARP

In July 2019, a federal court sentenced Lend America executive Michael Ashley to three years in prison for his role in a bank fraud conspiracy with Poppi Metaxas, the CEO of Gateway Bank to create the appearance that Gateway had improved its financial condition when it applied to TARP. In 2015, the court sentenced Metaxas to one year and six months in prison. The court ordered Ashley, who pled guilty in 2011, to pay $49 million in restitution and $800,000 in forfeiture.

In August 2008, Gateway Bank's regulator was conducting an examination when the bank applied for TARP in October 2008. While the application was pending, in November 2009, the bank examiner informed the bank that it was concerned about capital levels and toxic assets, and said that the bank needed to increase capital and reduce toxic assets. CEO Metaxas then engaged in a number of fraudulent schemes, including a conspiracy with Ashley at Lend America to make it look like the bank had reduced toxic assets. In March 2009, while the TARP application was pending, Metaxas caused Gateway to engaged in roundtrip transactions of $3.64 million in sham loan proceeds to Lend America, which Ashley transferred out of the bank to three entities he controlled, and back to the bank for a purported down payment for an asset sale. Metaxas proposed a $15 million sale of toxic assets to the bank's board,

concealing the source of the down payment, misleading the board. She later lied to bank regulators, all while the TARP application was pending. The bank then was not approved for TARP. In November 2009, Lend America failed, and Gateway wrote off the entire loan.

SIGTARP was joined in the investigation by the Federal Bureau of Investigation and the Department of Housing and Urban Development Office of Inspector General. The U.S. Attorney's Office for the Eastern District of New York prosecuted the case.

Federal Court Sentences Former Mirae Bank Executive to More than Five Years in Prison for Loan Fraud that Caused More Than $5.7 Million in Bank Losses

In May 2019, a federal court sentenced former Chief Marketing Officer Ataollah Aminpour at the now-defunct Mirae Bank to five years and 10 months in federal prison, after he pled guilty in December 2017 to his role in a scheme that caused the Koreatown-based lender to issue more than $15 million in fraudulent loans, and ultimately caused the bank to suffer more than $7.5 million losses. Aminpour specialized in providing financing for gas stations and car wash businesses with little or no down payment. He falsified bank loan applications to overstate the purchase price, leaving the bank under collateralized. Defendant Mohsen Hassanshahi purchased a gas station in 2006 and obtained 100% financing through Aminpour and Mirae Bank by submitting false financial statements. Hassanshahi also pled guilty and was sentenced to four years and five months in federal prison in August 2018.

FDIC and TARP recipient Wilshire Bank, which acquired Mirae Bank's assets from the FDIC, suffered more than $33 million in losses on the Aminpour-referred loans. The U.S. Treasury took in excess of a $3.5 million TARP loss on Wilshire Bank. SIGTARP was joined in the investigation by the Federal Deposit Insurance Corporation's Office of Inspector General, the Federal Bureau of Investigation, and the Federal Housing Finance Agency's Office of Inspector General. The U.S. Attorney's Office for the Central District of California prosecuted the case.

Federal Court Sentences Lawyer and Co-Conspirator to Prison for Participating in a Multimillion-Dollar Fraud Scheme, Including Those Seeking Assistance from HAMP

In July 2019, a federal court sentenced lawyer Rajesh Maddiwar to five years in prison, and sentenced Owen Reid to one year and one day in prison for a multimillion-dollar criminal scheme that defrauded New York homeowners in the Bronx, Brooklyn and Queens out of their homes, including those seeking mortgage modifications through TARP's HAMP program. In May 2015, Amir Meiri, Mario Alvarenga and Maddiwar were indicted. In December 2015, Owen Reid and two co-conspirators were indicted. SIGTARP agents participated in the arrest of Maddiwar, Reid, Alvarenga, Herzel Meiri and Samantha Boubert. The court sentenced Herzel Meiri and Amir Meiri, the owners of Launch Development, to 10 years in prison, and five years in prison.

From 2013 to 2015, Owen and co-conspirators, collectively called the Hillside Fraud Team, targeted distressed homeowners in the New York City area, including the Bronx, Brooklyn, and Queens. The Hillside Fraud Team sent mailers to owners of distressed properties on letterhead of the Homeowners Assistance Services of New York offering foreclosure prevention services. Reid and others trained and directed telemarketers to meet with the homeowners to appeal to the emotions of the homeowners. They developed a script that included in substance, a statement that a short sale would be a means for homeowners to lower their monthly payments and still remain in their home. Many homeowners – some of whom were elderly or in poor health – met with Reid or another member of the Hillside Fraud Team who advised them that they could assist with a loan modification. The homeowners were then told that a loan modification could not be completed, but they could sell the property to Launch Development, and then a relative could repurchase the property within 90 days, with the homeowner staying in the home.

There would then be a closing, where unbeknownst to the homeowner, they were selling their homes to a Hillside Business, often Launch Development. At the closing, the homeowner would meet with lawyer Maddiwar who told the homeowners that he would be their attorney. Maddiwar encouraged homeowners to sign documents that in some cases were blank. The homeowners did not know that they were selling their home to Launch Development for well below market value. A member of the Hillside Fraud Team typically appeared at the homeowner's residence

and demanded that the homeowner vacate the premises or commenced eviction proceedings. This fraud generated millions of dollars because they resold the houses at enormous profits. 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.

Jury Convicts Owner of U.S. Homeowners Relief of a Nationwide $3.5 Million Fraud Scheme Targeting More Than 250 Homeowners Seeking Loan Modifications, Including Under TARP's Making Home Affordable Program

In April 2019, after trial a federal jury convicted Aminullah Sarpas on 10 counts of conspiracy and mail fraud. In July 2014, SIGTARP agents and law enforcement partners arrested Sarpas who was a co-owner 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 his co-conspirators demanded upfront fees of up to $4,200 from homeowners in exchange for false promises of securing mortgage loan modifications on their behalf, touting a 97% success rate in securing modifications, and advertising money-back guarantees. The company's marketing materials implied they were affiliated with TARP's Making Home Affordable Program, making specific reference to the government website www.MakingHomeAffordable.gov and displaying 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; Corpus Christi, Texas. Two defendants pleaded guilty, including Paul Bain, a co-owner of the business who pleaded guilty in 2016, and Louis Saggiani, manager and chief accountant, who pleaded guilty in 2015. SIGTARP was joined in the investigation by the United States Postal Inspection Service and the Internal Revenue Service. The U.S. Attorney's Office for the Central District of California is prosecuting the case.

Defendants Sentenced In Nationwide $2.5 Million Scam that Victimized More than 500 Homeowners Related to HAMP Program

In late 2019 and early 2020, multiple defendants were sentenced to prison for their roles in a massive, nationwide scheme to defraud homeowners. In February 2020, Alan Jessie Chance was sentenced to one year in prison and three years' supervised release after he pleaded guilty to conspiracy to commit mail fraud. In November 2019, Chad Caldaronello was sentenced to three years and five months in prison, and Michael P. Paquette was sentenced to one year and three months in prison. In January 2020, Dennis Lake was sentenced to three years of probation and six months home confinement after he pleaded guilty to conspiracy to commit mail fraud.

The scheme, which took place in 2014 and 2015, started with sending mailers that appeared to be coming from an entity affiliated with the government to homeowners facing foreclosure. Chance and his co-conspirators operated under aliases and told homeowners they worked for HOPE Services, later changed to HAMP Services, which sounded similar to TARP's Home Affordable Modification Program. They falsely told victims they were part of a non-profit, government-affiliated agency, and that the homeowners were eligible for a loan modification without contacting any government agency or their lender. They told homeowners they were approved for a loan modification, and had to pay three trial payments that would be held in a trust account or escrow, but not to inform their lender about the trial payments. They obtained at least $2.5 million in trial payments from more than 500 victims nationwide spanning from their base of operation in California to points as far as Egg Harbor City, New Jersey and Mt. Airy, Maryland.

SIGTARP was joined in the investigation by the Federal Bureau of Investigation. The U.S. Attorney's Office for the Central District of California 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) and the Troubled Asset Relief Program (TARP), and keeps the Secretary of the Treasury and Congress fully informed. Treasury OIG is comprised of four divisions: (1) Office of Audit, (2) Office of Investigations, (3) Office of Counsel, and (4) Office of Management. Treasury OIG is headquartered in Washington, DC, and has an audit office in Boston, Massachusetts.

Treasury OIG has oversight responsibility for OCC. OCC is responsible for approximately 840 national banks, 303 federal savings associations, and 57 federal branches of foreign banks. The total assets under supervision are $12.8 trillion. Treasury OIG also oversees four offices created by the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank) which are (1) the Office of Financial Research (OFR), (2) the Federal Insurance Office, (3) the Office of Minority and Women Inclusion within Treasury's Departmental Offices (DO), and (4) the Office of Minority and Women Inclusion within OCC. Additionally, Treasury OIG oversees Treasury's role related to the financial solvency of the Federal National Mortgage Association 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 Management and Performance Challenges Related to Financial Regulation and Economic Recovery

In accordance with the Reports Consolidation Act of 2000, the Treasury Inspector General annually provides the Secretary of the Treasury with his perspective on the most serious management and performance challenges facing the Department. In a memorandum to the Secretary dated October 15, 2019, the Inspector General reported three management and performance challenges that were directed towards financial regulation and economic recovery. Those challenges are: Operating in an Uncertain Environment, Cyber Threats, and Anti-Money Laundering and Terrorist Financing/Bank Secrecy Act Enforcement.[9]

9 The Treasury Inspector General's memorandum included two other challenges not directly related to financial regulation and economic recovery: Efforts to Promote Spending Transparency and to Prevent and Detect Improper Payments, and Information Technology Acquisition and Project Management. The memorandum also discussed concerns about two matters: the coin redemption program at the United States Mint and managerial accounting.

Operating in an Uncertain Environment

We are mindful of external factors and future uncertainties that affect the Department's programs and operations. Among the most notable was the 35-day partial Federal government shutdown from December 22, 2018 through January 25, 2019 that affected all of government including Treasury. Like other components of Treasury subject to a lapse in appropriation, the Bureau of the Fiscal Service (Fiscal Service) developed its 2019 Lapse Plan as directed by the Office of Management and Budget (OMB). According to Fiscal Service officials, its 2019 Lapse Plan was based on assumptions that the shutdown would be of a short duration consistent with OMB's guidelines. Fiscal Service's 2019 Lapse Plan did not contemplate a shutdown of the nature and duration as that of the fiscal year 2019 shutdown. Given the central role that Fiscal Service serves in providing financial and administrative services government-wide and to the American public, management had to make adjustments to meet the bureau's obligations.

The Department continues to await discussions with OMB and Congress on the proposed changes included in OMB's comprehensive "Government–wide Reform Plan and Reorganization Recommendations" (Government–wide Reform Plan) to reorganize the Executive Branch.[10] Specific to Treasury, OMB proposed the transfer of alcohol and tobacco responsibilities from the Bureau of Alcohol, Tobacco, Firearms and Explosives within the Department of Justice to the Alcohol and Tobacco Tax and Trade Bureau (TTB) in order to leverage the expertise and resources of TTB. The plan also includes a proposal to privatize the United States Postal Service, which is estimated to be insolvent, yet continues to hold a $15 billion unfunded liability to the Treasury's Federal Financing Bank. Although no decisions have been made, Treasury started to prepare for the potential long-term restructuring of certain functions of offices/bureaus and expected budget cuts.

Treasury has had to manage the increasing demands placed on the Committee on Foreign Investments in the United States[11] (CFIUS), which is charged with reviewing transactions involving foreign investments in the United States to determine national security risks. There is an anticipated increase in both volume and complexity of transactions. 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 [12] modernized the review process, it also expanded CFIUS's jurisdiction to address growing concerns over certain investment structures that were not within CFIUS's 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. It will be a challenge onboarding personnel with the specialized skills to review complex investment structures as the security clearance process continues to be a contributing factor in recruiting highly skilled personnel that require access to programs and information systems dealing with national security.

The lengthy security clearance process continues to hamper the recruitment of cybersecurity personnel government-wide. Our previous audits of select Treasury bureaus found that the cause for many of our findings related to information systems' security measures involved a lack of resources and/or management oversight, which echoed the Government Accountability Office's (GAO) observations of agencies' impairments. In its April 3, 2019 letter to the Department regarding its top open recommendations, 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.[13] The security clearance process is still a culprit in the recruiting process and remained on GAO's 2019 high-risk list.[14]

To further complicate matters, Treasury must also operate in the repeated cycle of budget and debt ceiling stopgaps. Legislation was passed in February 2018 to suspend the statutory debt limit through March 1, 2019.[15] Because no long-term solution had been found, the U.S. debt limit was reinstated at $22 trillion on March 2, 2019. When the

10 OMB, *Delivering Government Solutions in the 21st Century, Reform Plan and Reorganization Recommendations* (June 2018)
11 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.
12 Public Law 115-232 (August 13, 2018).
13 GAO, *Treasury Priority Recommendations* (GAO-19-325SP; April 3, 2019)
14 GAO, *High-Risk Series, Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas* (GAO-19-157SP: March 2019)
15 Public Law 115-123 (February 8, 2018)

statutory debt limit was reinstated, Treasury immediately implemented extraordinary measures to prevent the United States from defaulting on its obligations. 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.[16] 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.

The impact of this challenge and the uncertainties require the Department 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 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 and subtle, they pose ongoing challenges for Treasury to fortify and safeguard its internal systems and operations along with the financial sector it oversees. 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, in addition to continuously evolving. 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. Ensuring the Nation's cybersecurity continues to be reported as a government-wide issue on GAO's 2019 high-risk list.

As the tools used to perpetrate cyber-attacks become easier to use and more widespread, the less technological knowledge and fewer resources that are needed to launch successful attacks of increasing sophistication. Such attacks include distributed denial of service attacks, phishing or whaling attacks, fraudulent wire payments, malicious spam (malspam), ransomware, and compromise of supply chains. There has been growing concern with foreign adversaries creating and exploiting vulnerabilities in information and communication technology and services. To secure the supply technology and services chain, an Executive Order was issued on May 15, 2019 that bans 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.[17] 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 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 in the near future.

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

As an ongoing challenge, Treasury will need to balance cybersecurity demands while modernizing and maintaining IT systems. To this end, Treasury must ensure that cyber security is fully integrated into its IT investment decisions.

16 Public Law 116-37 (August 2, 2019)
17 *Executive Order on Securing the Information and Communications Technology and Services Supply Chain* (May 15, 2019).

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 the 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. In 2018, the Office of Foreign Assets Control (OFAC) designated approximately 1,500 persons to the list of Specially Designated Nationals and Blocked Persons (SDN)[18] which is approximately 50 percent more than it has ever added to the list in any single year. Additionally, criminals and other bad actors evolve and continue to develop more sophisticated money laundering methods in an attempt to avoid detection.

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. In an effort to effectively implement U.S. policy and disrupt these financial networks, officials stated that TFI is moving towards a more collaborative approach to achieve its mission.

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 identified that the success of that system depends on the financial sector's confidence that those reports are adequately protected, but recent 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, we continue to consider anti-money laundering and combating terrorist financing programs and operations as inherently high-risk.

Completed and In-Progress Work on Financial Oversight

OFR's Hiring Practices

We initiated an audit of OFR's hiring practices. We reported that OFR's administration of the recruitment process for filling vacancies complied with applicable OPM, Treasury, OFR, and other federal requirements. As a result of the audit, we did not make any recommendations to OFR

18 SDN list includes individuals and entities designated in connection with activity involving sanctioned countries. It also lists individuals, groups, and entities such as terrorists and narcotics traffickers designated under sanctions programs that are not country-specific. Unless an exemption from regulation applies or OFAC authorizes a transaction under a license, all transactions by U.S. persons, including U.S. depository institutions, or transactions in or involving the United States are prohibited if they involve an individual or entity on the SDN list. U.S. persons must also block designated persons' property and interests in property within their possession or control.

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

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

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

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

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

We initiated an audit of OCC's supervisory impact on the practice of de-risking[19] 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.

Failed Bank Reviews

In 1991, Congress enacted the Federal Deposit Insurance Corporation Improvement Act (FDICIA) amending the Federal Deposit Insurance Act (FDIA). The amendments require that banking regulators take specified supervisory actions when they identify unsafe or unsound practices or conditions. Also added was a requirement that the Inspector General for the primary federal regulator of a failed financial institution conduct a material loss review when the estimated loss to the Deposit Insurance Fund is "material." FDIA, as amended by Dodd-Frank, defines the loss threshold amount to the Deposit Insurance Fund triggering a material loss review as a loss that exceeds $50 million for 2014 and thereafter (with a provision to temporarily raise the threshold to $75 million in certain circumstances). The act also requires a review of all bank failures with losses under these threshold amounts for the purposes of (1) ascertaining the grounds for appointing Federal Deposit Insurance Corporation (FDIC) as receiver and (2) determining whether any unusual circumstances exist that might warrant a more in-depth review of the loss. As part of the material loss review, OIG auditors determine the causes of the failure and assess the supervision of the institution, including the implementation of the prompt corrective action provisions of the act.[20] As appropriate, OIG auditors also make recommendations for preventing any such loss in the future.

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

20 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.

From 2007 through March 2020, FDIC and other banking regulators closed 543 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 initiated two non-material loss reviews of the failures of Resolute Bank, Maumee, Ohio which was closed on October 25, 2019 and City National Bank of New Jersey which was closed on November 1, 2019.

THIS PAGE IS INTENTIONALLY LEFT BLANK.

Approved July 2019

Top Management and Performance Challenges Facing Financial-Sector Regulatory Organizations

Council of Inspectors General on Financial Oversight

EXECUTIVE SUMMARY

Purpose

The purpose of this report is to consolidate and provide insight into cross-cutting management and performance challenges facing Financial-Sector Regulatory Organizations in 2019, as identified by members of CIGFO.

Approach

Following a review of 10 TMPC reports issued by CIGFO members, we synthesized the primary areas of concern facing Financial-Sector Regulatory Organizations. We sought to identify common insights within the financial sector.

CIGFO Members

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

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

The Inspectors General within CIGFO report annually on the Top Management and Performance Challenges (TMPC) facing their respective Financial-Sector Regulatory Organizations. This is CIGFO's second report reflecting the collective input from the Inspectors General in CIGFO and identifying cross-cutting Challenges facing multiple Financial-Sector Regulatory Organizations. This report reiterates the six challenges from our 2018 report and includes an additional challenge for 2019 – Improving Contract and Grant Management.

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

It is important to address the Challenges in this report because financial-sector activities – such as consumer and commercial banking, and funding, liquidity and insurance services – were identified by the Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, as National Critical Functions. Those functions are so vital to the United States that any disruption, corruption, or dysfunction would have a debilitating effect on U.S. security, the national economy, and/or public health and safety.

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.

By consolidating and reporting these Challenges, CIGFO aims to inform FSOC, regulatory organizations, Congress, and the American public of the cross-cutting Challenges facing the financial sector.

TABLE OF CONTENTS

BACKGROUND AND OBSERVATIONS

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

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

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

Figure 1: 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 Bureau of Consumer Financial Protection	▪ Board of Governors of the Federal Reserve System ▪ Bureau of Consumer Financial Protection
Federal Housing Finance Agency	Federal Housing Finance Agency
National Credit Union Administration	National Credit Union Administration
Securities and Exchange Commission	Securities and Exchange Commission
Special Inspector General for the Troubled Asset Relief Program	Department of the Treasury's Troubled Asset Relief Program

The Inspectors General within CIGFO, as well as the Inspectors General of other agencies, annually identify what they consider to be the TMPCs facing their agency. Each Inspector General's TMPCs generally appear in the host Agency's annual performance and accountability report under the Reports Consolidation Act of 2000.

On March 26, 2019, CIGFO approved a motion to compile a report identifying the top Challenges facing Financial-Sector Regulatory Organizations. The Federal Deposit Insurance Corporation (FDIC) Office of Inspector General (OIG) led the working group to conduct this analysis and compile this report.

This CIGFO report reflects the collective input from the nine CIGFO Member Inspectors General and identifies cross-cutting Challenges facing multiple Financial-Sector Regulatory Organizations. The report reiterates the six challenges from our September 2018 report, *Top Management and Performance Challenges Facing Financial Regulatory Organizations*, with an additional Challenge for 2019 – Improving Contract and Grant Management.

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

This report identifies significant financial-sector cybersecurity challenges. Financial-Sector Regulatory Organizations are faced with responsibilities to protect the information held by their respective agencies against cyber attacks, and to ensure that financial institutions and their third-party service providers have processes in place to mitigate cyber risks. Financial-Sector Regulatory Organizations must take a holistic, financial sector-wide view to address cybersecurity threats because a security incident for any participant has the possibility of infecting the entire financial sector.

Identifying threats, such as cyber risk and other vulnerabilities, requires the sharing of information among Government agencies and throughout the entire financial sector. Financial-Sector Regulatory Organizations face challenges to ensure effective gathering, analysis, and sharing of timely and actionable threat information. Absent such threat information, financial sector participants may not have a full understanding of the risks. This could result in informational gaps that can negatively impact risk mitigation and supervisory strategies and/or the financial sector. Financial-Sector Regulatory Organizations must also mitigate risks and stand ready when necessary to address threats that may escalate into a crisis. This report observes that Financial-Sector Regulatory Organizations must ensure that plans and resources are in place to address such crises.

Financial-Sector Regulatory Organizations also face Challenges to govern their internal operations. Controls should be in place to manage Financial-Sector Regulatory Organizations appropriately, including ensuring a sufficient workforce with skillsets to achieve organization missions. Further, controls should be in place to manage contract and grant funding so that organizations receive appropriate goods and services and grantees use funds as prescribed by statute and regulation.

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. By consolidating and reporting these Challenges, CIGFO aims to inform FSOC, regulatory organizations, Congress, and the American public of the cross-cutting Challenges facing the financial sector.

CHALLENGE 1 ENHANCING OVERSIGHT OF FINANCIAL INSTITUTION CYBERSECURITY

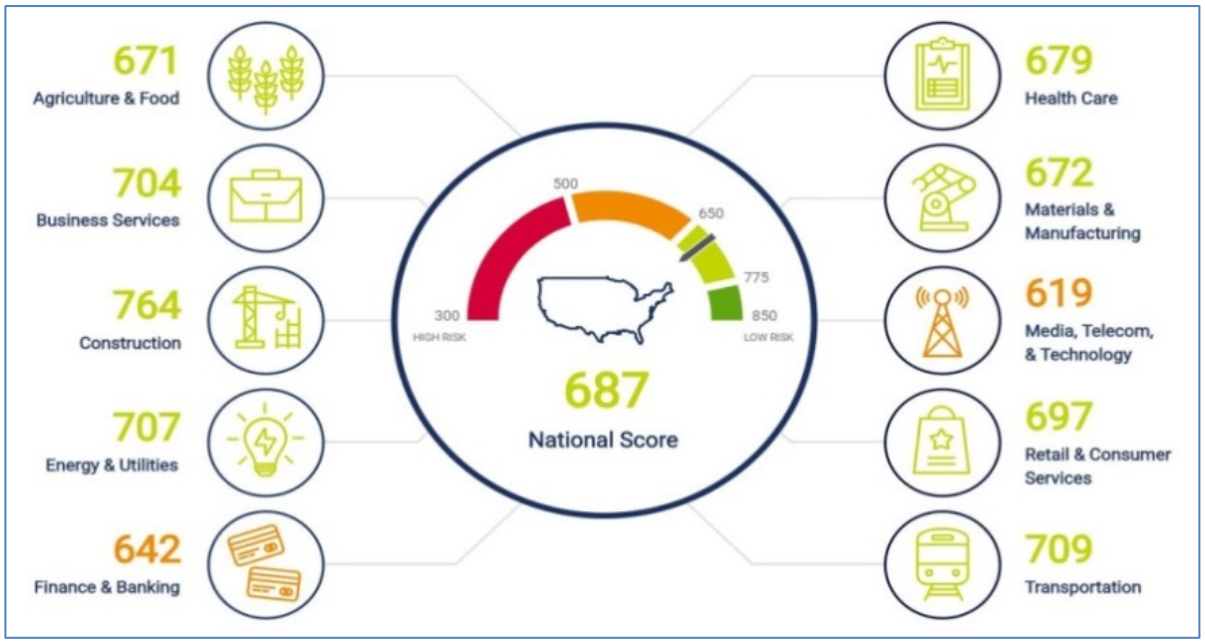
Cybersecurity continues to be a critical risk facing the financial sector. FSOC recognized in its December 2018 Annual Report that as financial institutions increase their reliance on technology, there is an increased risk that a cybersecurity event could have "severe negative consequences, potentially entailing systemic implications for the financial sector and the U.S. economy."[1] The Office of the Comptroller of the Currency (OCC) echoed this sentiment in its *Semiannual Risk Perspective* (Fall 2018), finding that cybersecurity threats "target operational vulnerabilities that could expose large quantities of personally identifiable information (PII)[2] and proprietary intellectual property, facilitate misappropriation of funds and data at the retail and wholesale levels, corrupt information, and disrupt business activities."[3]

In February 2018, the White House Council of Economic Advisors estimated that the United States economy loses between $57 and $109 billion per year to malicious cyber activity. Cyberattacks—such as distributed denial of service and ransomware—may be global in nature and have disrupted financial services in several countries around the world.[4] Verizon Communications' 2019 annual review of global data breaches across multiple sectors, including the financial sector, reported that there were more than 41,000 security incidents and 2,000 data breaches across 65 countries between April 2018 and April 2019.[5] This review also found that cyberattacks happen very quickly, with breaches occurring within seconds, and breach discovery taking months.

A 2018 study by the U.S. Chamber of Commerce and FICO (Fair Isaac Corporation) evaluated the cyber risk at 2,574 U.S. firms across 10 sectors, including the financial sector. This study provided cybersecurity ranking scores from 300 (high risk) to 850 (low risk) for each sector as well as a national average. The cyber risks faced by the finance and banking sector exceeded eight other sectors and the national average, as shown in Figure 2.

[1] The *Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010* established FSOC, which has responsibility for identifying risks and responding to emerging threats to financial stability. FSOC brings together the expertise of Federal financial regulators, an independent insurance expert, and state regulators.
[2] According to OMB Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, the term PII refers to information that can be used to distinguish or trace an individual's identity, such as their name, Social Security Number, biometric records, etc. alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.
[3] OCC *Semiannual Risk Perspective* (Fall 2018).
[4] World Bank Group, *Financial Sector's Cybersecurity: Regulations and Supervision* (2018).
[5] Verizon Communications Inc., *2019 Verizon Communications Data Breach Investigations Report*, 11th Edition (April 2019).

Figure 2: Cyber Risk Scores Across Ten Sectors



Source: U.S. Chamber of Commerce and FICO, *Assessment of Business Cybersecurity* (Q4 2018).

Supervisory Response to Cybersecurity Changes

Financial-Sector Regulatory Organizations are responsible for examining financial institutions to identify Information Technology (IT) risks. The *Interagency Guidelines Establishing Information Security Standards* for bank regulators states that an insured financial institution must "implement a comprehensive written information security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the institution and the nature and scope of its activities."[6] Most Financial-Sector Regulatory Organizations[7] conduct IT examinations using the Uniform Rating System for Information Technology created by the Federal Financial Institutions Examination Council (FFIEC).[8] The primary purpose of the rating system is to assess risks introduced by IT at institutions and service providers, and to identify those institutions requiring supervisory attention.[9] When examinations identify risks and weak management practices at institutions, regulators may use enforcement procedures to address such risks.

CIGFO members identified Challenges to keep pace with the changing cybersecurity landscape. The Federal Housing Finance Agency (FHFA) OIG identified that the FHFA will be challenged to design and implement supervisory activities for the financial institutions it supervises. Specifically, the FHFA must ensure that cybersecurity examination modules are updated in response to changes in the cybersecurity

[6] See 12 C.F.R. Part 364, Appendix B and 12 C.F.R. Part 748. The FDIC, OCC, and Board of Governors of the Federal Reserve issued the *Interagency Guidelines Establishing Information Security Standards*.
[7] The National Credit Union Administration does not use the Uniform Rating System for Information Technology.
[8] The FFIEC was established on March 10, 1979, pursuant to title X of the Financial Institutions Regulatory and Interest Rate Control Act of 1978, Public Law 95-630. The Council is an interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System, the FDIC, the National Credit Union Administration, the OCC, and the Bureau of Consumer Financial Protection and to make recommendations to promote uniformity in the supervision of financial institutions.
[9] FFIEC, *Uniform Rating System for Information Technology*, 64 Fed. Reg. 3109 (January 20, 1999).

environment. The FHFA must also recruit and retain a complement of examiners with the experience and expertise needed to conduct IT examinations, and ensure those examiners have ongoing training. Similarly, the Board of Governors of the Federal Reserve System (Federal Reserve Board) and Bureau of Consumer Financial Protection (Bureau) OIG noted that the Federal Reserve Board is challenged to ensure that supervised financial institutions manage and mitigate the risks and vulnerabilities of cyberattacks. The Federal Reserve Board should ensure that its supervisory approaches keep pace with evolving cybersecurity threats.

The FDIC OIG also identified cybersecurity as a significant challenge to FDIC-supervised institutions. The FDIC must ensure the effectiveness and efficiency of its IT examination work programs. One example would be using data to review and understand cybersecurity risks across all institutions. The FDIC is also challenged to have the appropriate number of IT examiners and to keep its examination staff skillsets up-to-date given the increasing complexity and sophistication of IT environments at banks. Similarly, the National Credit Union Administration (NCUA) OIG also noted cybersecurity as a continued and significant challenge to the stability and soundness of the credit union industry. The NCUA OIG believes the NCUA must acquire and deploy resources to enhance its oversight capabilities to maintain safety and soundness.

Financial Technology Cybersecurity Risk

Financial institutions face increased cybersecurity risk through interconnections with financial technology companies. The Group of Twenty's Financial Stability Board defined financial technology as "innovation that could result in new business models, applications, processes, or products with an associated material effect on financial markets and institutions and the provision of financial services."[10] Financial technology innovation includes, for example, mobile wallets, digital currencies, and digital financial advice.[11] The rapid pace of financial technology is being driven by capital investment, demand for speed and convenience, and digitization.[12] According to the Department of the Treasury (Treasury Department), from 2010 to 2017, more than 3,330 new technology companies were formed to serve the financial industry.[13] The Treasury Department also estimated that one-third of online U.S. consumers use at least two financial technology services—including financial planning, savings and investment, online borrowing, or some form of money transfer and payment.[14] Further, KPMG estimated that global investment in financial technology was $57.9 billion in just the first 6 months of 2018.[15]

---

[10] *Financial Stability Implications from FinTech, Supervisory and Regulatory Issues That Merit Authorities' Attention*, (June 27, 2017). The Financial Stability Board (FSB) was chartered by the Group of Twenty (G20) on September 25, 2009. The G20 Members include Argentina, Australia, Brazil, Canada, China, France, Germany, India, Indonesia, Italy, Japan, Republic of Korea, Mexico, Russia, Saudi Arabia, South Africa, Turkey, the United Kingdom, the United States, and the European Union (plus Hong Kong, Singapore, Spain, and Switzerland). The FSB charter aims to promote global financial stability by coordinating the development of regulatory, supervisory and other financial-sector policies and conducts outreach to non-member countries. The G20 members represent about two-thirds of the world's population, 85 percent of global gross domestic product, and over 75 percent of global trade.

[11] Basel Committee on Banking, *Sound Practices – Implications of Fintech Developments for Banks and Bank Supervisors* (February 2018).

[12] Department of the Treasury, *A Financial System that Creates Economic Opportunities: Nonbank Financials, Fintech, and Innovation* (July 2018); Basel Committee on Banking, *Sound Practices – Implications of Fintech Developments for Bank and Bank Supervisors* (February 2018).

[13] *A Financial System That Creates Economic Opportunities: Nonbank Financials, Fintech, and Innovation* (July 2018).

[14] *A Financial System That Creates Economic Opportunities: Nonbank Financials, Fintech, and Innovation* (July 2018).

[15] KPMG, *The Pulse of Fintech 2018: Biannual Global Analysis of Investment in Fintech* (July 2018). KPMG is a professional services company.

Financial technology companies are interconnected with IT systems at banks, yet these technology companies may not be subjected to regulatory requirements for safety and soundness and may not be examined by financial regulators. Certain banks reported that between 20 and 40 percent of online banking logins are attributable to financial technology companies, and many banks represented that they cannot distinguish among computer logins, as to whether they originate from consumers, data aggregators, or even malicious actors.[16] IT system interconnections may provide a pathway for a cybersecurity incident at a financial technology company to infect the banking system.

Additionally, when financial institutions have multiple financial technology services and relationships, they face ambiguity and uncertainty as to the applicability of certain privacy rules, the Bank Secrecy Act provisions and regulations, and Anti-Money Laundering standards. Banks and credit unions may be unsure as to whether they or the service provider must comply with rules, regulations, and requirements. Moreover, financial institutions face challenges to have sufficient skilled staff and capabilities to monitor these risks and operations of financial technology companies.

The FDIC OIG stated that the FDIC faces challenges to ensure that banks have proper governance and risk management practices around these technologies. The FDIC may need to increase training and adjust staffing to ensure that examiners have the skills to effectively supervise the risks involved with new technology. Further, the FDIC may need to modify examination policies and procedures that pre-date financial innovation to improve supervision of financial innovation risk. The NCUA OIG stated that the NCUA faces significant challenges with technology-driven changes in the financial landscape that could potentially impact the safety and soundness of the credit union system and the Share Insurance Fund. The NCUA OIG believes it is imperative that the NCUA's examination and supervision program continues to evolve with emerging financial technologies that represent not only risks, but also opportunities to the credit union system.

Mitigating Third-Party Service Provider Risk

Banks and credit unions frequently hire third-party Technology Service Providers (TSP) to perform operational functions on behalf of the financial institution—such as IT operations and business product lines. TSPs may further sub-contract services to other vendors. According to the OCC, banks are increasingly reliant upon TSPs and sub-contractors, and such dependence creates a high level of risk for the banking industry.[17] The OCC indicates that TSPs are increasingly targets for cybercrimes and espionage and may provide avenues for bad actors to exploit a bank's systems and operations. For example, on December 20, 2018, the Department of Justice announced that two Chinese nationals were charged with computer intrusion offenses harming more than 45 service providers whose clients included the banking and finance industry and the U.S. Government. The hackers targeted service providers in order to gain unauthorized access to the computer networks of their clients and steal intellectual property and confidential business information.[18]

---

[16] Lael Brainard, Member, Board of Governors of the Federal Reserve System, *Where Do Banks Fit in the Fintech Stack?* Remarks delivered at the Northwestern Kellogg Public-Private Interface Conference on "New Developments in Consumer Finance: Research & Practice" (April 29, 2017).

[17] The FFIEC described the term TSP to include "independent third parties, joint venture/limited liability corporations, and bank and credit union service corporations that provide processing services to financial institutions." Supervision of Technology Service Providers, FFIEC IT Examination Handbook InfoBase.

[18] Department of Justice Press Release, *Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information* (December 20, 2018).

A financial institution must manage the interconnections, system interfaces, and systems access of TSPs and sub-contractors and must implement appropriate controls.[19] Significant consolidation among TSPs caused large numbers of banks to rely on a few large service providers for core systems and operations support.[20] As a result, a cybersecurity incident at one TSP has the potential to affect multiple financial institutions.[21] A financial institution's Board of Directors and senior managers are responsible for the oversight of activities conducted by a TSP on their behalf to the same extent as if the activity were handled within the institution.[22]

The Federal Reserve Board and Bureau OIG identified the need for the Federal Reserve Board to enhance its oversight of firms that provide technology services to supervised institutions. Specifically, the Federal Reserve Board can enhance its oversight by implementing an improved governance structure and providing additional guidance to examination teams on the supervisory expectations for such firms. The FDIC OIG also noted challenges with FDIC-supervised institutions' oversight of the TSPs with whom they do business. The FDIC must ensure that supervised financial institutions assess TSP cybersecurity risks, including due diligence of cybersecurity contract terms.

Financial-Sector Regulatory Organizations play a vital role in addressing financial institutions' cybersecurity risk which, if left unchecked, could threaten the safety and soundness of institutions as well as the stability of the financial system. Financial-Sector Regulatory Organizations must ensure that IT examinations assess how financial institutions manage cybersecurity risks, including risks associated with TSPs and new financial technology, and address such risks through effective supervisory strategies.

[19] OCC *Semiannual Risk Perspective* (Spring 2018).
[20] OCC *Semiannual Risk Perspective* (Spring 2018).
[21] OCC *Semiannual Risk Perspective* (Spring 2018).
[22] Financial Institution Letter 44-2008, *Guidance for Managing Third-Party Risk* (June 6, 2008).

CHALLENGE 2 MANAGING AND SECURING INFORMATION TECHNOLOGY AT REGULATORY ORGANIZATIONS

In March 2019, the Government Accountability Office (GAO) identified securing Federal systems and information as a high-risk area in need of significant attention.[23] An Office of Management and Budget (OMB) and Department of Homeland Security (DHS) review of Federal cybersecurity capabilities at 96 civilian agencies across 76 metrics found that 74 percent (71 agencies) had cybersecurity programs that were either "At Risk" or "High Risk.[24] Further, the Government sector represented a total of 56 percent of the over 41,000 cybersecurity incidents identified by Verizon Communications in its 2019 annual review of global data breaches across multiple sectors.[25]

Financial-Sector Regulatory Organizations' IT systems house commercially valuable and market sensitive information. For example, the Securities and Exchange Commission (SEC) OIG reported that the SEC's e-Discovery program alone is approaching one petabyte of data.[26] Financial-Sector Regulatory Organizations may also house significant amounts of personally identifiable information for bank and credit union officials, depositors, and borrowers. Without proper safeguards, those IT systems are vulnerable to individuals and groups with malicious intentions who can intrude and use their access to obtain sensitive information, commit fraud and identify theft, disrupt operations, or launch attacks against other computer systems and networks. Further, interconnections among Financial-Sector Regulatory Organizations and other Federal and state government agencies or private-sector institutions increase the likelihood of contagion in which a cybersecurity incident occurring anywhere within the systems may negatively impact the entire financial system.[27]

Securing IT from Evolving Threats

According to the GAO, risks to Federal IT systems are increasing.[28] Threats to Federal IT systems include those from witting or unwitting employees as well as global threats from nation states.[29] Federal agencies must develop, document, and implement department- and agency-wide information security programs to protect information and information systems.[30] Federal agencies use a common framework developed by the National Institute of Standards and Technology to manage their cyber risk.[31]

---

[23] U.S. Government Accountability Office, *High-Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas*, GAO-19-157SP (March 2019).
[24] *Federal Cybersecurity Risk Determination Report and Action Plan* (May 2018). "At Risk" meant that some essential policies, processes, and tools were in place to mitigate overall cybersecurity risk, but significant gaps remained; while "High Risk" meant that fundamental cybersecurity policies, processes, and tools were either not in place or not deployed sufficiently.
[25] Verizon Communications Inc., *2019 Verizon Communications Data Breach Investigations Report*, 11th Edition (April 2019).
[26] One petabyte of data is roughly the equivalent to the amount that can be stored in about 20 million four-drawer filing cabinets. U.S. Government Accountability Office, *Military Base Realignments and Closures: The National Geospatial-Intelligence Agency's Technology Center Construction Project*, GAO-12-770R, (June 29, 2012).
[27] Financial Services Sector-Specific Plan 2015 issued jointly among the Department of the Treasury, Department of Homeland Security, and the Financial Services Sector Coordinating Council.
[28] GAO, Cybersecurity Challenges Facing the Nation – High Risk Issue.
[29] Worldwide Threat Assessment of the US Intelligence Community, January 29, 2019.
[30] Federal Information Security Modernization Act of 2014, Public Law No. 113-283.
[31] Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, May 11, 2017.

The Department of Housing and Urban Development (HUD) OIG recognized that HUD faces challenges in the management and oversight of its IT systems. HUD has demonstrated an inability to incorporate Federally mandated requirements and key practices into effective operational management of its IT systems. Persistent IT management challenges have affected HUD's ability to manage and oversee key programs. As a result, IT systems vulnerabilities that could lead to breaches exist within HUD's IT environment. Since 2007, HUD OIG has made 483 recommendations to HUD management to address IT challenges and 197 of those recommendations remain open or unresolved.

The FDIC OIG found that the FDIC must continue to strengthen its implementation of governance and security controls around its IT systems to ensure proper safeguarding of information. The FDIC OIG identified 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. For example, the FDIC had not fully defined or implemented an enterprise-wide and integrated approach to identifying, assessing, and addressing the full spectrum of internal and external risks, including those related to cybersecurity and the operation of information systems.

The Federal Reserve Board and Bureau OIG noted that the Federal Reserve Board's decentralized IT services results in an incomplete view of security risks facing the agency as a whole, which impacts the implementation of an effective information security program. The Federal Reserve Board also faces challenges in implementing agency-wide processes for managing vulnerabilities and software inventories. The Federal Reserve Board and Bureau OIG also found that the Bureau faces challenges in centralizing and automating processes to better manage insider risks; ensuring that automated feeds from all systems, including contractor-operated systems, feed into the Bureau's security information and event management tool; and aligning its information security program, policies, and procedures with the agency's evolving enterprise risk management program.

The Treasury Department OIG noted challenges with the mitigation of risks to the Treasury Department's IT systems posed by interconnection agreements with other Federal, State, and local agencies as well as third-party cloud service providers. Similarly, the FHFA OIG found that the FHFA needs to ensure that access to its internal and external online collaborative environment is restricted to those with a need for the information.

The SEC OIG also noted that the SEC must mature its IT security programs to minimize risks of unauthorized disclosure, modification, use, and disruption of the SEC's non-public information. Specifically, the SEC can improve its management of IT risks, including access, continuous monitoring, and incident management. Further, the SEC could better manage information security risks of outside expert services contractors who have access to sensitive, non-public information.

Modernizing IT Systems

Some Financial-Sector Regulatory Organizations are relying on systems that are outdated, cannot be adapted to handle increasingly complex tasks, and are no longer supported by vendors. According to the GAO, use of such systems increases the vulnerability of unauthorized access to the information within those systems.[32]

[32] U.S. Government Accountability Office, *Information Security: SEC Improved Control of Financial Systems but Needs to Take Additional Actions*, GAO-17-469 (July 2017).

HUD OIG reported that HUD is using aging technology for most of its operations – technology that was implemented dating back to 1974. Many of HUD's systems remain at risk of failure or exploitation because critical vendor fixes or updates are no longer available. That situation increases the risk of possible HUD data breaches. Further, HUD's legacy systems are very costly to maintain because of the specialized skills and support needed to operate them. Over the last 5 years, HUD spent on average 70 to 95 percent of its $280 million annual IT budget on operations and maintenance.

Similarly, the U.S. Commodity Futures Trading Commission (CFTC) OIG identified that the CFTC faces challenges because it has not formalized IT capital planning. Specifically, the CFTC has not established accountabilities to eliminate manual-intensive legacy systems, reduce high-cost IT functions, and adopt a modern IT infrastructure. CFTC OIG noted that IT modernization efforts could yield cost savings and technological efficiencies during periods of fiscal austerity.

The Treasury Department OIG also noted the impact of uncertain budgetary funding on the Treasury Department's IT modernization efforts. The Treasury Department is challenged to balance cybersecurity requirements with expenditures for the modernization and maintenance of existing Treasury Department IT systems.

Enhancing the IT Security Workforce

According to the GAO, "a key component of mitigating and responding to cyber threats is having a qualified, well-trained cybersecurity workforce."[33] The GAO has identified, however, that there are cybersecurity workforce skills gaps across the Federal Government.[34]

CIGFO members identified mission challenges related to cybersecurity skills gaps. The Treasury Department OIG found that many IT security measures lacked adequate cybersecurity resources and/or management oversight. Similarly, HUD OIG noted that the maintenance of many of HUD's systems requires specialized skills. HUD OIG further noted that turnover among senior leadership and resource constraints hindered the completion of three IT modernization projects totaling approximately $370 million.

Cybersecurity threats against Government agencies continue to increase. Financial-Sector Regulatory Organizations must remain vigilant in their efforts to institute necessary controls and properly protect the information entrusted to them.

[33] U.S. Government Accountability Office, *Cybersecurity Workforce: Agencies Need to Improve Baseline Assessments and Procedures for Coding Positions*, GAO-18-466 (June 2018).
[34] U.S. Government Accountability Office, *High-Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas*, GAO-19-157SP (March 2019).

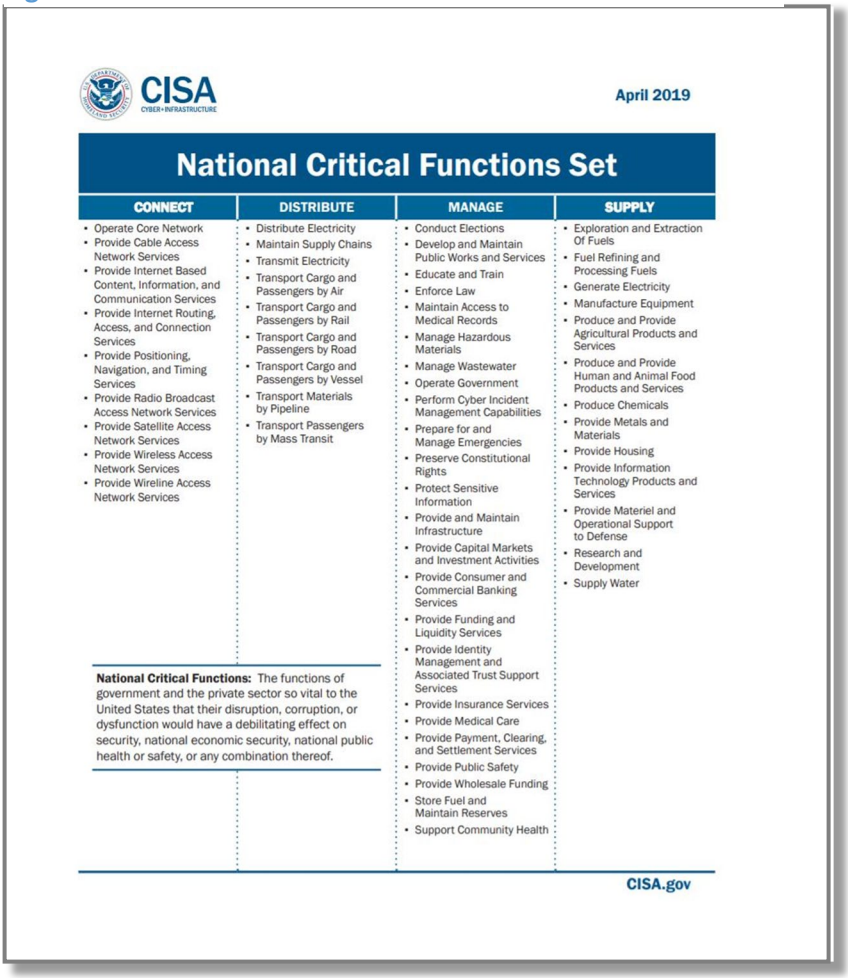
CHALLENGE 3 SHARING THREAT INFORMATION

On November 16, 2018, the President signed into law the Cybersecurity and Infrastructure Security Agency Act of 2018 (Act). The Act established the Cybersecurity and Infrastructure Security Agency (CISA) within the DHS to, among other things, make the United States cyber and physical infrastructure more secure by sharing information at all levels of Government and the private and non-profit sectors.[35]

On April 30, 2019, the CISA published a list of National Critical Functions, which were defined as, "[t]he functions of government and private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[36] The provision of consumer and commercial banking, funding and liquidity services, and insurance services were included on the list of National Critical Functions.[37] Rather than relying on prior, sector-specific or asset-based risk identification, the National Critical Functions construct looks across sectors to provide a holistic approach to capture risks and dependencies within and across sectors.[38] As shown in Figure 3, the National Critical Functions are presented in four overarching areas – connect, distribute, manage, and supply.

One key focus of the CISA and the National Critical Functions is collecting and sharing information, including

Figure 3: National Critical Functions

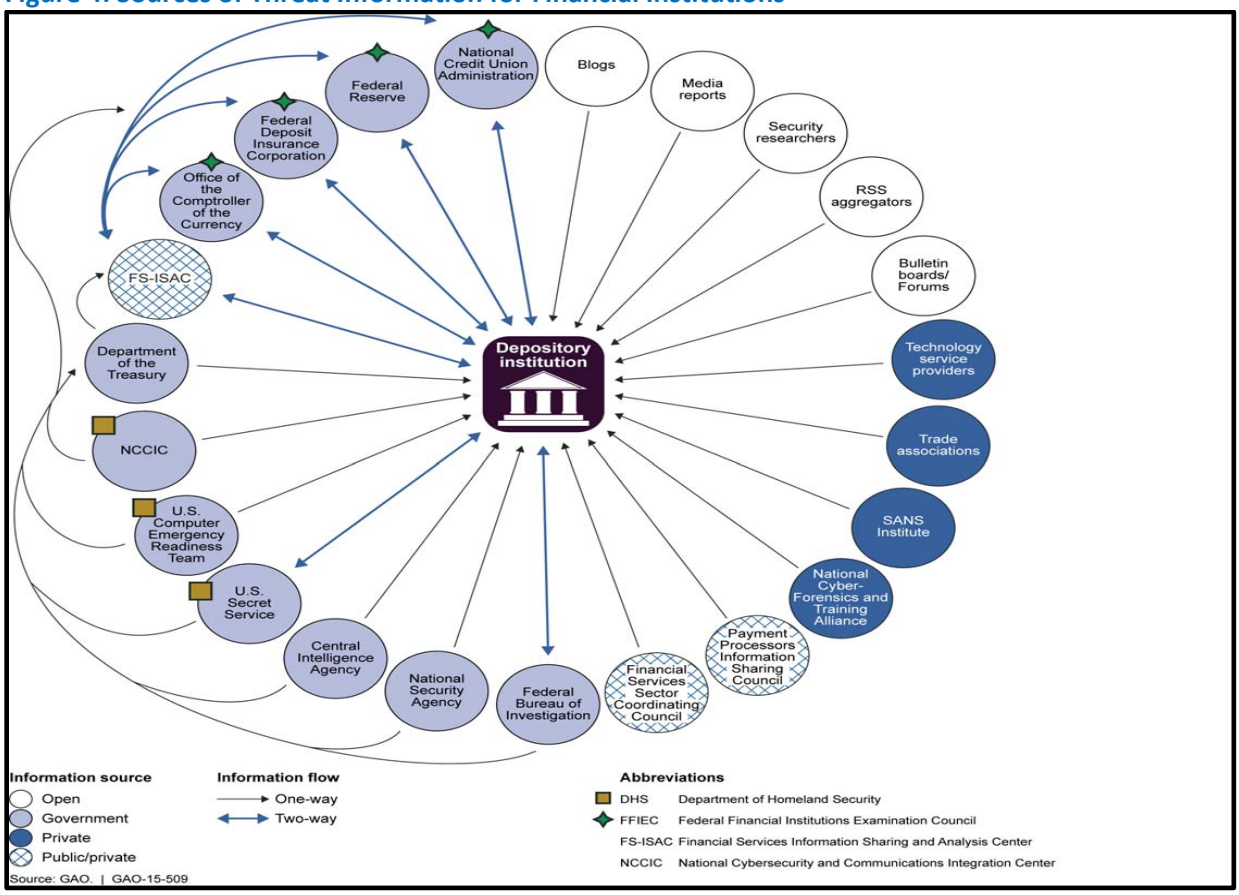


Source: Cybersecurity and Infrastructure Security Agency

[35] Cybersecurity and Infrastructure Security Act of 2017, House Report 115-454, 115th Congress, December 11, 2017.
[36] National Critical Functions – An Evolved Lens for Critical Infrastructure and Security Resilience, DHS Cybersecurity and Infrastructure Security Agency, April 30, 2019.
[37] National Critical Functions – An Evolved Lens for Critical Infrastructure and Security Resilience, DHS Cybersecurity and Infrastructure Security Agency, April 30, 2019.
[38] National Critical Functions – An Evolved Lens for Critical Infrastructure and Security Resilience, DHS Cybersecurity and Infrastructure Security Agency, April 30, 2019.

informing intelligence collection requirements.[39] FSOC noted, in its 2018 Annual Report, the critical importance to the financial sector of sharing timely and actionable threat information among the Federal Government and the private sector. FSOC stated that Federal agencies should consider how to share information and when possible "declassify (or downgrade classification) of information to the extent practicable, consistent with national security needs."[40] The GAO also identified various sources of threat information that could be shared with financial institutions. Figure 4 illustrates how the GAO captured threat information flows from multiple sources.

Figure 4: Sources of Threat Information for Financial Institutions



Sharing Threat Information Throughout the Financial Sector

Financial institutions must be prepared to address many threats, and Financial-Sector Regulatory Organizations must ensure through supervisory processes that financial institutions are ready to mitigate those risks. According to the FFIEC, financial institutions should have business continuity plans that "[a]nalyze threats based upon the impact to the institution, its customers, and the financial market

[39] National Critical Functions – An Evolved Lens For Critical Infrastructure Security and Resilience, Cybersecurity and Infrastructure Security Agency, National Risk Management Center, April 30, 2019.
[40] FSOC 2018 Annual Report.

it serves."[41] Further, the FFIEC notes that financial institutions should have "a means to collect data on potential threats that can assist management in its identification of information security risks."[42]

In November 2014, the FFIEC members encouraged financial institutions to join the Financial Services Information Sharing and Analysis Center (FS-ISAC), through its *Statement on Cybersecurity Threat and Vulnerability Monitoring and Sharing* (*Cybersecurity Sharing Statement*).[43] FS-ISAC is a group of 7,000 member organizations whose purpose is to share timely, relevant, and actionable security threat information. The *Cybersecurity Sharing Statement* also suggested using other resources such as the Federal Bureau of Investigation's (FBI) InfraGard,[44] U.S. Computer Emergency Readiness Team,[45] and Secret Service Electronic Crimes Task Force.[46] Threat awareness is important because financial institutions are links in the chain of financial services system interconnections; an incident involving one community bank has the potential to affect the broader financial sector.[47] Therefore, as part of the supervisory examination process, Financial-Sector Regulatory Organizations must ensure that supervised institutions can receive and access threat information, and that they have business continuity plans to address such threats.

The Treasury Department leads financial sector readiness efforts. The Treasury Department OIG recognized the Department's challenge to provide financial-sector leadership, ensure effective public-private coordination, and strengthen awareness and preparedness against cyber threats. The FDIC OIG identified challenges for the FDIC to ensure that relevant threat information is shared with its supervised institutions and examiners as needed, in a timely manner, to prompt responsive action to address the threats. Threat information provides FDIC examiners with context to evaluate banks' processes for risk identification and mitigation strategies.

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

According to the Director of the Financial Crimes Enforcement Network, "Financial institutions are often the first to detect and block illicit financing streams, combat financial crimes and related crimes and bad acts, and manage risk."[48] Providing the financial sector with information about illicit activity can help sector participants identify and report such activities; this assists law enforcement in disrupting money laundering and other financial crimes.[49] Such information is especially important with the use of virtual currencies to identify illicit actors who use virtual currency to "… facilitate criminal activity such as

[41] FFIEC, Business Continuity Planning Booklet, *Risk Assessment*, (Available on the FFIEC website).
[42] FFIEC IT Examination Handbook Infobase, Information Security Booklet, II, *Information Security Program Management* (Available on the FFIEC website).
[43] FFIEC, *Statement on Cybersecurity Threat and Vulnerability Monitoring and Sharing*.
[44] InfraGard is a web-based portal that provides collaboration between the FBI and the private sector to exchange information about critical infrastructure.
[45] US-CERT is a component of the Department of Homeland Security; its mission is to reduce the nation's risk of systemic cybersecurity and communications challenges.
[46] The Electronic Crimes Task Force is a nationwide network designed to support and assist state, local, and Federal law enforcement agencies in order to combat criminal activity involving the use of new technology.
[47] Departments of the Treasury and of Homeland Security, *Financial Services Sector-Specific Plan* (2015).
[48] Prepared remarks of Financial Crimes Enforcement Network Director Kenneth A. Blanco, SIFMA Anti-Money Laundering & Financial Crimes Conference, February 4, 2019.
[49] Prepared remarks of Financial Crimes Enforcement Network Director Kenneth A. Blanco, SIFMA Anti-Money Laundering & Financial Crimes Conference, February 4, 2019.

human trafficking, child exploitation, fraud, extortion, cybercrime, drug trafficking, money laundering, terrorist financing, and to support rogue regimes and facilitate sanctions evasion."[50]

The Treasury Department OIG reported challenges affecting the Department's ability to effectively gather and analyze intelligence information. Specifically, the Treasury Department must do more to collaborate and coordinate with other Federal agencies to identify and disrupt financial networks that support terrorist organizations. The Treasury Department also faces staffing challenges threatening its ability to ensure effective gathering and analysis of intelligence information. The Department requested approximately 100 new analyst positions for Fiscal Year 2019. Those positions are difficult to fill, however, because of required expertise and the length of time to process security clearance for such personnel.

Threat information can be considered by financial institutions and Financial-Sector Regulatory Organizations in developing and examining bank and credit union mitigation strategies and continuity plans. Absent such threat information, financial institutions and examiners may lack a full understanding of the risks facing banks and credit unions, and thus, risk mitigation and supervisory strategies might have gaps which could affect the safety and soundness of institutions.

[50] Financial Crimes Enforcement Network, *Advisory on Illicit Activity Involving Convertible Virtual Currency* (May 9, 2019).

CHALLENGE 4 ENSURING READINESS FOR CRISES

The financial sector is a vital component of the infrastructure of the United States. As noted by DHS, "large-scale power outages, recent natural disasters, and an increase in the number and sophistication of cyberattacks demonstrate the wide range of potential risks facing the sector."[51]

Financial-Sector Regulatory Organizations support the financial sector by identifying and mitigating potential systemic problems. When supervisory mitigation cannot stem risks or economic events overtake such efforts, Financial-Sector Regulatory Organizations, in conjunction with other Federal and state regulators, must be ready to stabilize financial markets and provide disaster aid.

Crisis readiness requires advanced preparation, regardless of whether the crisis results from financial disruption in the markets, economic turmoil, a cyber attack, natural disaster, or other event. "When the unexpected, enterprise-threatening crisis strikes, it is too late to begin the planning process. Events will quickly spin out of control, further adding to the loss of reputation and avoidable costs necessary to survive and recover with minimal damage."[52]

Figure 5: Crisis Management Preparedness Continuous Cycle

Source: Federal Emergency Management Agency

Although crises may be different in their cause or complexity, implementation of fundamental principles allows Financial-Sector Regulatory Organizations, to plan and prepare for such events. Figure 5 illustrates the Crisis Management Preparedness Cycle, which includes the following five components:[53]

- **Plan –** Supports effective operations by identifying objectives, describing organizational structures, assigning tasks to achieve objectives, identifying responsibilities to accomplish tasks, and contributing to the goals.
- **Organize –** Identifies necessary skillsets and technical capabilities.
- **Train –** Provides personnel with the knowledge, skills, and abilities to respond to a crisis.
- **Exercise –** Identifies strengths and weaknesses through an assessment of gaps and shortfalls with plans, policies, and procedures to respond to a crisis.

[51] Department of Homeland Security, CISA, Financial Services Sector available on the DHS website.
[52] Hastings Business Law Journal, *The Board's Responsibility for Crisis Governance* (Spring 2017).
[53] Federal Emergency Management Agency National Incident Management System.

- **Evaluate and Improve –** Compiles lessons learned, develops improvement plans, and tracks corrective actions to address gaps and deficiencies identified.

Preparing for Potential Financial Institution Disruptions and Failures

It has been more than a decade since Financial-Sector Regulatory Organizations were called upon to address the financial crisis. An FDIC study described the financial crisis as two interconnected and overlapping crises.[54] The first phase of the crisis involved systemic threats to the financial system as a whole through the failure of large financial and non-financial institutions during 2008-2009. The second overlapping phase involved a rapid increase in the number of smaller troubled and failed banks between 2008-2013. As noted by FDIC Chairman Jelena McWilliams on April 3, 2019, "[t]here were regulatory gaps leading up to the crisis—perhaps none more important than the inadequate planning for potential failure of the largest banks and their affiliates." [55] As described by Chairman McWilliams, the lessons learned from the crisis are that large and small banking institutions must be able to fail "without taxpayer bailouts and without undermining the market's ability to function." [56]

Financial-Sector Regulatory Organizations, in conjunction with other Federal and state regulators, must be prepared to mitigate financial institution risks and, when necessary, resolve failed banks and credit unions. The Dodd-Frank Act introduced significant changes since the crisis. The Dodd-Frank Act required that bank holding companies plan for potential resolution through bankruptcy. The Dodd-Frank Act also provided new resolution authority to orderly liquidate financial companies in extreme cases during severe financial crisis. In addition, the FDIC instituted regulations requiring that insured depository institutions with more than $50 billion in assets also prepare resolution plans addressing how the FDIC could resolve the institution under the Federal Deposit Insurance Act. These steps clarify resolution authority, but Financial-Sector Regulatory Organizations must be able to execute those resolutions.

The FDIC OIG identified challenges with the FDIC's readiness to fulfill its mission to manage receiverships. According to the FDIC, the events of the financial crisis unfolded more quickly than the FDIC expected and were more severe than the FDIC's planning efforts anticipated.[57] For example, in July 2008, the FDIC resolved IndyMac, the most expensive FDIC failure, estimated to cost about $12.3 billion, and in September 2008, Washington Mutual, the sixth-largest FDIC-insured institution, also failed. The FDIC had not planned for several large and small banks to fail at the same time, and these failures occurred at a quicker pace than in previous crises. The FDIC OIG stated that the FDIC is challenged to ensure that it has the ability to on-board the staff needed to address escalating crisis workloads. For example, during the crisis, the FDIC authorized funding for additional personnel but faced challenges expediting the hiring process to on-board needed staff.

Further, the FDIC faced challenges dealing with the increased volume of contracts required during the time of crisis. During the financial crisis, the FDIC awarded over 6,000 contracts totaling more than $8 billion. The size of the FDIC acquisition staff was initially insufficient, which resulted in delays to

[54] FDIC, *Crisis and Response, An FDIC History, 2008-2013* (November 30, 2017).
[55] FDIC Chairman Jelena McWilliams, Bank Resolution: A Global Perspective, International Banker (April 3, 2019).
[56] FDIC Chairman Jelena McWilliams, Bank Resolution: A Global Perspective, International Banker (April 3, 2019).
[57] FDIC, *Crisis and Response, An FDIC History, 2008-2013* (November 30, 2017).

modify existing contracts and award new contracts. The FDIC needed to rapidly hire and train personnel to oversee the contracts. The FDIC is also challenged to ensure that it has plans in place to react and respond quickly to a crisis, irrespective of its cause, nature, magnitude, or scope; ensure those plans are current and up-to-date; and incorporate lessons learned from past crises and the related bank failures.

The NCUA OIG also noted several challenges faced by the NCUA pertaining to risks to the safety and soundness of credit unions and the protection of the National Credit Union Share Insurance Fund which, similar to the Deposit Insurance Fund, insures credit union member accounts against losses up to $250,000.[58] These risks include: significant threats posed by cyberattacks, competitive challenges to credit unions posed by new technology-driven financial products; increasing competition in the financial services industry; and continuing consolidation among depository institutions. The NCUA needs to: strengthen the resiliency of the credit union systems and the agency; work with credit unions to manage risks of new financial products and services; and continue to monitor consolidation trends among depository institutions.

Preparing to Administer Disaster Aid

HUD plays a substantial role in national disaster recovery initiatives and often receives more disaster recovery funding than any other Federal agency. After a national disaster, Congress may authorize additional funding to HUD for the Community Development Block Grant Program (Community Development Grants) for significant unmet needs for long-term recovery.[59] Since 2001, Congress has awarded HUD more than $84.6 billion for disaster recovery. HUD awards Community Development Grants to state and local governments who, in turn, may grant money to state agencies, non-profit organizations, economic development agencies, citizens, and businesses. The state and local governments provide these funds for disaster relief, long-term recovery, restoration of infrastructure, housing, and economic revitalization.

HUD OIG noted that, by their nature, Community Development Grants pose a risk as they are provided at a time when a community is recovering from a disaster. HUD OIG identified that HUD's Community Development Grant requirements are not codified in the Federal Register. Instead, HUD issues multiple requirements and waivers for each disaster in Federal Register notices, which leads to confusion among program grantees. For example, HUD OIG noted that 59 grantees with 112 active Community Development Grants totaling more than $47.4 billion were required to follow 61 different Federal Register notices to manage the program. Further, HUD OIG identified continuing risks to HUD concerning the more than $18 billion in disaster recovery sent to Puerto Rico during a time when Puerto Rico was close to filing for bankruptcy.

HUD OIG also reported that HUD is challenged to ensure that grantees have the capacity to administer Community Development Grants and ensure the funds are used for eligible and supported items. Since 2006, HUD OIG has completed 120 audits and 6 evaluations of the Community Development Block Grant

[58] Created by Congress in 1970, NCUA administers the Share Insurance Fund and insures individual credit union member accounts against losses up to $250,000 and a member's interest in all joint accounts combined up to $250,000. The Deposit Insurance Fund is administered by the FDIC and insures account holder deposits in FDIC insured banks and provides funds to resolve failed banks.

[59] Community Development Block Grant Disaster Recovery Fact Sheet.

Program, identifying $477.4 million in ineligible costs, $906.5 million in unsupported costs, and $5.5 billion in funds that could be put to better use.

HUD also faces challenges to ensure that grantees follow Federal procurement regulations. HUD OIG identified that state disaster recovery programs may not align with Federal procurement requirements. As a result, products and services obtained through grant funds may not have been purchased competitively at fair and reasonable prices. HUD OIG also identified challenges in HUD's ability to expedite disaster assistance grants while also maintaining adequate safeguards to deter and detect fraud.

Additionally, HUD OIG found that Americans face challenges in attempting to receive assistance from HUD and other disaster relief agencies. Citizens face a circuitous path to receive disaster recovery assistance depending on how, when, and where they enter the disaster relief process. As a result, citizens may face significant delays in processing their applications for assistance, delays in receiving funding, and possible duplication of benefits.

Financial-Sector Regulatory Organizations protect the financial sector and American citizen when crises strike. Crises in the financial sector may come from many sources and at any time. Financial-Sector Regulatory Organizations must plan, prepare, train, exercise, and maintain readiness for scenarios that could lead to crises.

CHALLENGE 5 STRENGTHENING AGENCY GOVERNANCE

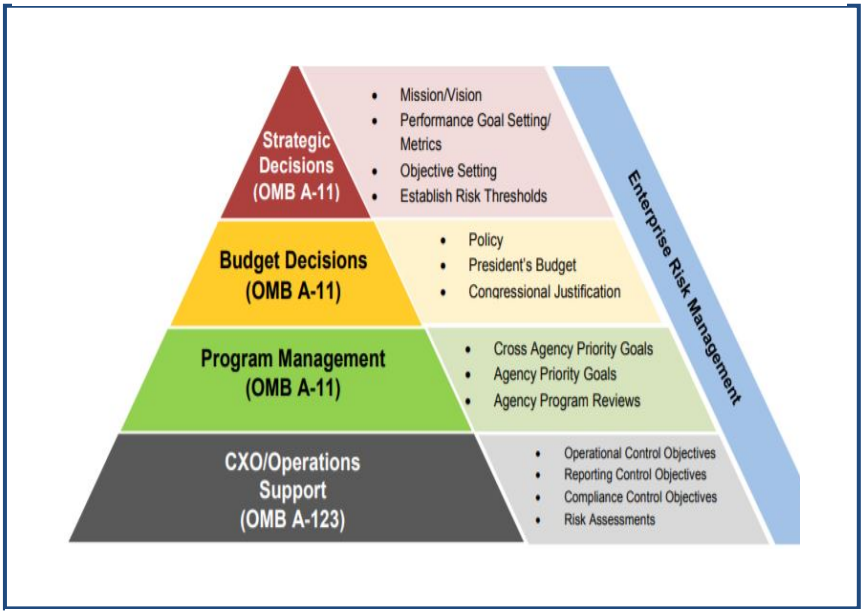
According to OMB Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control,* (OMB Circular A-123), Federal agencies face internal and external risks to achieving their missions, including "economic, operational, and organizational change factors, all of which would negatively impact an Agency's ability to meet goals and objectives if not resolved."[60] To address those risks, Federal leaders and managers generally must establish a governance structure to direct and oversee implementation of a risk management and internal control process.[61] Enterprise Risk Management (ERM) and internal controls are components of this governance framework. OMB defines ERM "as an enterprise-wide, strategically-aligned portfolio view of organizational challenges that provides better insight about how to most effectively prioritize resource allocations to ensure successful mission delivery."[62]

Establishing Enterprise Risk Management

ERM focuses specifically on the identification, assessment, and management of risk, and it should include these elements:

- A risk management governance structure;
- A methodology for developing a risk profile; and
- A process, guided by an organization's senior leadership, to consider risk appetite and risk tolerance levels that serves as a guide to establish strategy and select objectives.

Figure 6: Enterprise Risk Management Program



Source: CFO Playbook: Enterprise Risk Management for the U.S. Federal Government.

OMB urges agencies to adopt an enterprise-wide view of ERM—a "big picture" perspective— thus synthesizing the management of risks into the very fabric of the organization; it should not be viewed in "silos" among different divisions or offices. As shown in Figure 6, ERM should integrate risk management into the agency's processes for budgeting, including strategic planning, performance planning, and performance reporting practices.

[60] Office of Management and Budget Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control* (July 15, 2016).
[61] Office of Management and Budget Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control* (July 15, 2016).
[62] Office of Management and Budget Appendix A to OMB Circular A-123, *Management Reporting and Data Integrity Risk* (June 6, 2018).

The Federal Reserve Board and Bureau OIG found that the Federal Reserve Board has a complex governance system that creates challenges for the Governors to effectively carry out their roles and responsibilities and to have an enterprise-wide view of the management of certain administrative functions. For example, the Federal Reserve Board and Bureau OIG noted that Federal Reserve Board guidance does not set clear expectations for communication among Governors and between Governors and Division Directors. Such communication challenges may result in the Federal Reserve Board Governors being unaware of certain activities, and Board officials missing opportunities to leverage the Governors' knowledge and experience. In addition, the decentralization of information technology among Divisions does not allow for a complete view of IT security risks and impedes the ability to have an effective information security program. Additionally, the Federal Reserve Board Chief Human Capital Officer has had difficulty implementing enterprise-wide succession planning.

Similarly, the FDIC OIG identified challenges in the FDIC's implementation of its ERM program. Although the FDIC began ERM implementation efforts in 2010, the FDIC currently does not have an enterprise-wide and integrated approach to identifying, assessing, and addressing the full spectrum of internal and external risks. As a result, the FDIC faces difficulties integrating risk into its budget, strategic planning, performance reporting, and internal controls. In addition, FDIC Divisions and Offices are not able to evaluate risk determinations in the context of the agency's overall risk levels, tolerance, and profile. For example, the FDIC could not be sure that its resources were being allocated toward addressing the most significant risks in achieving strategic objectives.

Ensuring Effective Internal Controls

As described by the GAO, "a key factor in improving accountability in achieving an entity's mission is to implement an effective internal control system. An effective internal control system helps an entity adapt to shifting environments, evolving demands, changing risks, and new priorities."[63] OMB Circular A-123 emphasizes the need for agencies to coordinate risk management and strong and effective internal controls into existing business activities as an integral part of governing and managing an agency.

HUD OIG noted HUD's continuing struggle with effective oversight controls to monitor operations and programs. HUD faces challenges to effectively manage its programs that distribute about $48.2 billion annually to state and local government, organizations, and individuals through grants, subsidies, and other payments. For example, in 2018, HUD OIG reports identified more than $1.3 billion in ineligible, unsupported, unnecessary, or unreasonable costs. HUD OIG also noted that HUD's lack of compliance with the GAO's internal control standards has deprived HUD management of an important monitoring tool that can provide feedback on the effectiveness and efficiency of departmental operations.

FHFA OIG identified that internal control systems at Fannie Mae and Freddie Mac, which are under government conservatorship, fail to provide directors with accurate, timely, and sufficient information to enable them to exercise their oversight duties that are delegated to them by FHFA as conservator. Further, the FHFA OIG found that leadership changes in 2018 and 2019 may lead to a lack of attention to internal controls.

[63] U.S. Government Accountability Office, *Standards for Internal Control in the Federal Government*, GAO-14-704G, (September 2014).

Governance is an important tool for Financial-Sector Regulatory Organizations to ensure that they fulfill their missions and responsibilities to citizens and taxpayers. ERM and internal control programs synthesize the management of Financial-Sector Regulatory Organizations' risks into an organization's culture, so that these risks may be considered and incorporated into budget, strategic planning, performance reporting, and internal controls for the agency as a whole.

CHALLENGE 6 MANAGING HUMAN CAPITAL

Financial-Sector Regulatory Organizations rely on the skills of over 117,000 employees to ensure the safety and soundness of the U.S. financial system.[64] In March 2019, the GAO recognized strategic human capital management as a continuing Government-wide area of high risk.[65] The GAO noted the need for Federal agencies to "measure and address existing mission-critical skills gaps, and use workforce analytics to predict and mitigate future gaps so agencies can effectively carry out their missions."[66]

Succession Planning to Fill Leadership Gaps

Government-wide retirement eligibility in 2022 is estimated to be 31.6 percent of all permanent Federal employees.[67] According to the GAO, retirements could cause gaps in leadership and institutional knowledge and exacerbate existing skill gaps. According to the Office of Personnel Management (OPM), succession planning for such retirements forms an integral part of workforce planning and helps ensure an ongoing supply of qualified staff to fill leadership and other key positions.[68] Specifically, OPM requires that the head of each agency, in consultation with OPM, develop a comprehensive management succession program, based on the agency's workforce succession plans, to fill agency supervisory and managerial positions. Agency succession programs should be supported by employee training and development programs.

The Federal Reserve Board and Bureau OIG cited potential leadership and skills gaps as a result of a projected increase in numbers of Federal Reserve Board employees becoming eligible for retirement. Similarly, the FDIC OIG found that the percentage of FDIC employees eligible to retire more than doubles (2.3 times) over the next 5 years, increasing from 18 percent in 2018 to 42 percent in 2023. Further, the FDIC OIG identified potential leadership gaps resulting from the retirement eligibility of 66 percent of the Executive Management employees and another 57 percent of Managers between 2018 and 2022.

HUD OIG also identified that leadership gaps have affected HUD's management of its programs and operations. Specifically, constant turnover and extended vacancies in HUD's most important political and career executive positions led to poor management decisions and questionable execution of internal business functions. The SEC OIG also noted that, although the agency's multi-year strategic plan identified the need to strengthen human capital management, the SEC lacked a formal succession plan.

[64] CIGFO Working Group analysis of OPM Fedscope data as of March 2018 available at https://www.fedscope.opm.gov.
[65] U.S. Government Accountability Office, *High-Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas*, GAO-19-157SP (March 2019).
[66] U.S. Government Accountability Office, *High-Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas*, GAO-19-157SP (March 2019).
[67] U.S. Government Accountability Office, *High-Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas*, GAO-19-157SP (March 2019).
[68] 5 C.F.R. Part 412.

Skills Gap Identification and Mitigation

OPM's Human Capital Framework requires that agencies use comprehensive data analytic methods to monitor and address skills gaps and develop gap closure strategies.[69] CIGFO members identified challenges in the identification and mitigation of agency skill set gaps especially in response to new technologies. The Federal Reserve Board and Bureau OIG found that the Federal Reserve Board remains challenged to identify a diverse workforce with the necessary technical, managerial, and leadership skills. Continually evolving workforce expectations and a highly competitive environment for individuals with specialized skills presents challenges for the Federal Reserve Board. The FDIC OIG found that the FDIC was challenged to ensure that examination staff skill sets kept pace with the increasing complexity and sophistication of IT environments at banks as well as the introduction of new financial technology. The FDIC OIG also identified examiner skillset imbalances among FDIC regional offices. As a result, senior examiners may be required to travel more frequently in order to supervise less experienced staff and sign reports of examination.

The Federal Reserve Board and Bureau OIG stated that to address vacancies in the Bureau's workforce, the agency is reallocating staff resources through reassignments or detail opportunities. However, some of these vacancies are for highly specialized skillsets, and the Bureau may face challenges in identifying the necessary skillsets in its current workforce. The SEC OIG found that, although the SEC began a skill set assessment project in 2016, the SEC was delayed in implementing the project. Specifically, as of July 2018, the SEC had not completed competency assessment surveys or similar reviews to identify and close skill gaps within SEC divisions, offices, and regional offices.

Financial-Sector Regulatory Organizations' workforce plays a vital role in ensuring mission success. Mission success is contingent on each organization's management of human capital activities – workforce planning, recruitment, on-boarding, compensation, engagement, succession planning, and retirement programs – to allow for proactive responses to anticipated changes and maximize human capital efficiency and effectiveness.

[69] See OPM Human Capital Framework Structure and SEC OIG, *The SEC Made Progress But Work Remains to Address Human Capital Management Challenges and Align With the Human Capital Framework* (September 11, 2018), Report No. 549.

CHALLENGE 7 IMPROVING CONTRACT AND GRANT MANAGEMENT

The Administration recognized the importance of improving Federal Government acquisitions in finding that such acquisitions "often fail to achieve their goals because many Federal managers lack the program management and acquisition skills to successfully manage and integrate large and complex acquisitions into their projects."[70] In addition, the GAO found that Government contracting officials were carrying heavier workloads, and thus, it was more difficult for these officials to oversee complex contracts and ensure that contractors adhered to contract terms.

Grants are an important policy tool to provide funding to state and local governments, and nongovernmental entities for national priorities. According to the GAO, effective oversight and internal control is important to provide reasonable assurance to Federal managers and taxpayers that grants are awarded properly, grant recipients are eligible, and grants are used as intended according to laws and regulations.[71]

Strengthening Contract Oversight

According to the GAO's *Framework for Assessing the Acquisition Function at Federal Agencies*, agencies should effectively manage their acquisitions process in order to ensure that contract requirements are defined clearly and all aspects of contracts are fulfilled.[72] Agencies must properly oversee contractor performance and identify any deficiencies.

The Special Inspector General for the Troubled Asset Relief Program (SIGTARP) identified challenges to Treasury Department's oversight of Troubled Asset Relief Program (TARP) Funds. Over 150 banks or other institutions have or can receive $23 billion through agreements entered under the Making Home Affordable Program (MHA Program). The MHA Program pays TARP dollars when banks and institutions comply with rules and guidelines to modify mortgages to help struggling homeowners. SIGTARP found that despite enforcement actions and other wrongdoing of many financial institutions, the Treasury Department is significantly scaling back on MHA Program compliance reviews.

HUD OIG identified challenges with HUD's oversight of IT procurement. According to HUD's Chief Procurement Officer, fewer than five people were adequately trained and possessed the expertise to manage IT projects and contracts. HUD lacked well-documented and fully developed selection processes to ensure consistent application of selection criteria used for applicants for contracts. In addition, HUD did not have robust processes for contractor oversight and evaluating contractor performance against expected outcomes to ensure that its contractors met their obligations.

[70] The President's Management Agenda: Modernizing Government for the 21st Century.
[71] U.S. Government Accountability Office, *Grants Management: Observations on Challenges and Opportunities for Reform*, GAO-18-676T (July 25, 2018).
[72] U.S. Government Accountability Office, *Framework for Assessing the Acquisition Function at Federal Agencies*, GAO-05-218G (September 2005).

According to the FDIC OIG, the FDIC relies heavily on contractors for support of its mission, especially for IT and administrative support services. The FDIC OIG identified a number of contract challenges at the FDIC, including defining contract requirements, coordination between contracting and program office personnel, and establishing implementation milestones. For example, FDIC personnel did not fully understand and communicate the requirements to transition a nearly $25 million data management services contract from one contractor to another.

The Federal Reserve Board and Bureau OIG identified that the Bureau needed to strengthen controls for contract financing and management. Specifically, for one of its largest contracts, the Bureau did not comply with the *Federal Acquisition Regulation* requirements concerning contract financing requirements and documenting annual blanket purchase agreement reviews. Additionally, Bureau staff did not verify contractor expenses by obtaining and reviewing supporting source documents. The Federal Reserve Board and Bureau OIG also noted contracting challenges for the Federal Reserve Board's oversight of physical infrastructure changes. The Federal Reserve Board encountered significant delays, scope changes, and cost increases for renovations to its William McChesney Martin, Jr. building.

The SEC OIG identified challenges with the SEC's management and oversight of contracts. For example, the SEC OIG found that contract oversight personnel did not enforce contract requirements for experts performing work for the SEC. Further, contract oversight personnel had limited first-hand knowledge of the sufficiency of contract deliverables and therefore could not determine whether the invoices accurately reflected work performed.

Improving Grant Management

Grants are typically categorized as (1) categorical grants – which restrict funds to narrow, specific activities; (2) block grants – which are less restrictive funding for broader categories of activities; and (3) general purpose grants – which allow the greatest amount of discretion to be used for government purposes. Oversight and internal control of grants are important to ensure grants are used by eligible participants for allowable purposes.

SIGTARP identified challenges with the Treasury Department's oversight of TARP expenses charged by state housing finance agencies to administer the Hardest Hit Fund (HHF), a grant-like program. The Treasury Department's $9.6 billion for HHF provides funding to state housing finance agencies to assist unemployed homeowners and individuals whose mortgages are greater than their current home's value. SIGTARP has issued several reports on Treasury's lack of oversight for grantees. Between 2016 and 2017, SIGTARP identified $11 million in wasteful, abusive, and unnecessary funding by states for items such as gym memberships, parties, and country club events. Further, SIGTARP reported that there is no Federal requirement for states to use competition when spending funds on fees for consultants, accountants, and lawyers.

HUD OIG reported that HUD continues to struggle with effective program management of the nearly $50 billion in Federal funds that HUD passes to state and local governments, organizations, and individuals in the form of grants, subsidies, and other payments. Approximately 16 percent of HUD's

annual appropriations are provided as grants through the Office of Community Planning and Development. HUD OIG identified that 21 of their audits performed from 2014-2017 found that there was little or no monitoring of grantees. As a result, HUD did not have assurances that it correctly identified high-risk grantees or conducted adequate monitoring to mitigate risks.

Financial-Sector Regulatory Organizations rely on contracts and grants to perform their respective missions. Strong oversight and controls over contract and grant processes are critical to ensure proper stewardship over taxpayer funds.

CONCLUSION

This is the second report developed by CIGFO members to identify cross-cutting Challenges faced by Financial-Sector Regulatory Organizations. In this report, we continue to emphasize to policy makers the importance of considering a whole-of-Government approach to coordination and information sharing to address these Challenges.

Consistent with the mission of Inspectors General, this report helps inform the public by providing them with information about the important Challenges facing the financial sector to which most of the public is directly connected through bank or credit union accounts and mortgages. This report also informs CIGFO members in their identification of future Challenges and collaboration on reviews addressing cross-cutting Challenges facing the financial sector.

APPENDIX 1 ABBREVIATIONS AND ACRONYMS

Abbreviation and Acronym	Full Name
Bureau	Bureau of Consumer Financial Protection
CFTC	Commodity Futures Trading Commission
Challenges	The CIGFO Top Management and Performance Challenges identified in this report.
CIGFO	Council of Inspectors General on Financial Oversight
CISA	Cybersecurity and Infrastructure Security Agency
DHS	Department of Homeland Security
Dodd-Frank Act	The Dodd-Frank Wall Street Reform and Consumer Protection Act
ERM	Enterprise Risk Management
FBI	Federal Bureau of Investigation
FDIC	Federal Deposit Insurance Corporation
Federal Reserve Board	Board of Governors of the Federal Reserve System
FEMA	Federal Emergency Management Agency
FFIEC	Federal Financial Institutions Examination Council
FHFA	Federal Housing Finance Agency
Financial-Sector Regulatory Organizations	Federal Departments and Agencies overseen by CIGFO Inspectors General.
FISMA	Federal Information Security Modernization Act of 2014
FSB	Financial Stability Board
FS-ISAC	Financial Services Information Sharing and Analysis Center
FSOC	Financial Stability Oversight Council
GAO	U.S. Government Accountability Office
HHF	Hardest Hit Fund
HUD	Department of Housing and Urban Development
IT	Information Technology
MHA Program	Making Home Affordable Program
NCUA	National Credit Union Administration
NIST	National Institute of Standards and Technology
OCC	Office of the Comptroller of the Currency
OIG	Office of Inspector General
OMB	Office of Management and Budget
OPM	Office of Personnel Management
SEC	Securities and Exchange Commission
SIGTARP	Special Inspector General for the Troubled Asset Relief Program
TMPC	Top Management and Performance Challenges
Treasury Department	Department of the Treasury
TSP	Technology Service Provider

APPENDIX 2 METHODOLOGY

We reviewed 10 reports issued by the CIGFO members listed below that covered challenges identified in 2018.[73] Specifically, we reviewed every challenge reported in each TMPC report to identify common challenges reported by multiple CIGFO members. Through this process, we identified the most frequently reported challenges of CIGFO members by category, which resulted in seven challenges being identified. Once we established these categories, we reviewed individual challenges to determine whether we could also identify any common themes or key areas of concern.

Department of the Treasury

Federal Deposit Insurance Corporation

Commodity Futures Trading Commission

Bureau of Consumer Financial Protection

Department of Housing and Urban Development

Board of Governors of the Federal Reserve System

Federal Housing Finance Agency

National Credit Union Administration

Securities and Exchange Commission

Special Inspector General for the Troubled Asset Relief Program

[73] The Special Inspector General for the Troubled Asset Relief Program issues to the Treasury Department and has published its assessment of the most serious management and performance challenges and threats facing the Government in TARP in its Quarterly Report to Congress since October 2017.

THIS PAGE IS INTENTIONALLY LEFT BLANK.

January 2020

Survey of FSOC and its Federal Member Agencies' Efforts to Implement the Cybersecurity Act of 2015

Council of Inspectors General on Financial Oversight

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

THIS PAGE IS INTENTIONALLY LEFT BLANK.

Council of Inspectors General on Financial Oversight

January 15, 2020

MEMORANDUM FOR Steven T. Mnuchin
Chairman, Financial Stability Oversight Council

FROM: Richard K. Delmar
Acting Chair, Council of Inspectors General on Financial Oversight

SUBJECT: Survey Results— CIGFO Working Group's Survey of FSOC and its Federal Member Agencies' Efforts to Implement the Cybersecurity Act of 2015

With this memorandum, we hereby transmit the results of a Council of Inspectors General on Financial Oversight (CIGFO) Working Group survey of the Financial Stability Oversight Council's (FSOC) and its Federal voting member agencies' efforts to implement the information sharing provisions under Title I, the Cybersecurity Information Sharing Act (CISA) of the Cybersecurity Act of 2015. Section 107 of CISA, "Oversight of Government Activities," requires Inspectors General of "appropriate Federal entities,"[1] in consultation with the Intelligence Community Inspector General (IC IG) and CIGFO, to jointly report to Congress on the actions taken by the respective agencies over the most recent 2-year period to carry out the requirements of CISA. The first joint Inspectors General report was submitted to Congress in December 2017 (2017 joint IG report)[2] and the second joint report was issued in December 2019.

We undertook this survey to inform our reporting consultation role under Section 107, as well as provide FSOC and its Federal voting member agencies[3] with comparative information on how these agencies have implemented CISA.

We conducted the survey using a questionnaire based on the common question set created for the purpose of the 2017 joint IG report. In this regard, CISA Section

---

[1] The appropriate Federal entities are the Departments of Commerce, Defense, Energy, Homeland Security, Justice, the Treasury, and the Office of the Director of National Intelligence.

[2] *Joint Report on the Implementation of the Cybersecurity Information Sharing Act of 2015* (Office of the Inspector General of the Intelligence Community AUD 2017 005) (Dec. 19, 2017)

[3] The Federal voting members are the Secretary of the Treasury, Chairman of the Board of Governors of the Federal Reserve System, Comptroller of the Currency, Director of the Bureau of Consumer Financial Protection, Chairman of the U.S. Securities and Exchange Commission, Chairperson of the Federal Deposit Insurance Corporation, Chairperson of the Commodity Futures Trading Commission, Director of the Federal Housing Finance Agency, and the Chairman of the National Credit Union Administration.

107(b) requires that the joint report include certain information; the IC IG developed questions to gather that information. The CIGFO Working Group, led by the Department of the Treasury's (Treasury) Office of Inspector General (OIG), modified the common question set for the Federal financial sector survey audience. Our survey was not designed to assess Federal voting member agencies' compliance with CISA, and we make no such assessment in this memorandum.

We note that, while the Secretary of the Treasury is a Federal voting member of FSOC, Treasury was not included in this CIGFO Working Group survey. As one of the "appropriate federal entities" per CISA, Treasury's actions to carry out the requirements of CISA are reviewed separately by Treasury OIG. The results of Treasury OIG's reviews were included in the 2017 and 2019 joint IG reports to Congress. One of Treasury's bureaus, the Office of the Comptroller of the Currency (OCC), is a Federal voting member of FSOC and is included in this survey.

As part of this survey, in addition to the Federal voting members of FSOC, we interviewed officials from the FSOC Secretariat and Treasury's Office of Cybersecurity and Critical Infrastructure Protection (OCCIP) to gain an understanding of their role, if any, in implementing CISA. Treasury is a member of FSOC and OCCIP coordinates Treasury's efforts to enhance the security and resilience of financial sector critical infrastructure and reduce operational risk.

The following OIGs also participated in this Working Group: Board of Governors of the Federal Reserve System (Board) and the Bureau of Consumer Financial Protection (Bureau); Commodity Futures Trading Commission (CFTC); Federal Deposit Insurance Corporation (FDIC); Federal Housing Finance Agency (FHFA); National Credit Union Administration (NCUA); and U.S. Securities and Exchange Commission (SEC).

We conducted this survey from April 2019 through September 2019. The scope of our work covered the period of January 1, 2017 through March 31, 2019. As part of our survey, we reviewed applicable provisions of CISA and the agencies' responses to the common question set.

Background

In December 2015, CISA was signed into law to encourage the sharing of cyber threat information between the public and private sectors in a timely manner.[4] The act designated seven federal agencies to coordinate and develop government-wide,

[4] Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, div. N (Cybersecurity Act of 2015), Title I (Cybersecurity Information Sharing Act of 2015), 129 Stat. 2242, 2936-56 (2015) (codified at 6 U.S.C. §§ 1501-10).

publicly available policies, procedures, and guidance to assist federal and non-federal entities in their efforts to receive and share cyber threat indicators and defensive measures.[5] Among the policies issued was *Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government under the Cybersecurity Information Sharing Act of 2015* (February 16, 2016) which states:

> "Federal entities are encouraged to share [cyber threat indicators (CTIs)] and [defensive measures (DMs)] as broadly and as quickly as possible. Whether CTIs and DMs are classified, declassified or unclassified, federal entities should continuously identify and implement programs to share such CTIs and DMs with each other and with non-federal entities."[6]

I. Survey Results

The agencies provided responses to our questions on their implementation of CISA. Specifically, the responses addressed the:

A. Sufficiency of policies and procedures related to sharing CTIs[7] within the Federal Government;
B. Classification of CTIs and DMs,[8] and an accounting of the security clearances for the purpose of sharing with the private sector;
C. Actions taken based on CTIs or DMs shared with the Federal Government;
D. CTIs and DMs shared with federal entities containing information not directly related to a threat that is personal information; and
E. Any barriers to sharing information among federal entities.

A. Sufficiency of Policies and Procedures

The following questions were designed to gain an understanding of an agency's policies, procedures, and guidelines relating to the sharing of CTIs within the Federal Government and relevant entities, including those policies, procedures, and guidelines relating to the removal of information not directly related to a

[5] See footnote 1 for the list of these agencies.

[6] The policy document cautions that federal entities engaging in activities authorized by CISA "shall do so in full compliance with the Constitution and all other applicable laws of the United States, Executive Orders, and other Executive Branch directives, regulations, policies and procedures, court orders and all other legal, policy and oversight requirements." For example, the sharing of classified CTIs and DMs is with representatives of federal and non-federal entities that have appropriate security clearances.

[7] CTI – 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.

[8] DM – 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.

cybersecurity threat that is personal information of a specific individual or identifies a specific individual.

1. Does your agency have policies, procedures, and guidelines for:

   a) Sharing of CTIs within the Federal Government?
   b) Sharing CTIs with representatives of relevant entities (e.g., private entities, non-federal government agency, state/tribal/local government) as it pertains to the protection of classified information?
   c) Removal of information not directly related to a cybersecurity threat that is personal information of a specific individual or identifies a specific individual?
   d) Implementing security controls to protect against unauthorized access to CTIs or DMs?
   e) Notifying entities that received a CTI known to be in error?
   f) Notifying any U.S. person whose personal information is known to have been shared in violation of CISA?

2. To what extent have the policies, procedures, and guidelines for sharing CTIs been implemented?

3. Have there been any concerns or setbacks with regard to the implementation of the policies, procedures, and/or guidelines for sharing CTIs?

Table A.1 summarizes the agencies' responses to Questions 1a, 1b, 1c, 1e, 2 and 3.

Entity	Guidance for Sharing CTIs	Guidance for Sharing Classified Information w/ Relevant Entities	Guidance Addressing Removing PII[9] not related to CTIs	Guidance for Notifying Entities of CTIs Sent in Error	Guidance for Sharing CTIs Implemented	Concerns or Setbacks in Implementing Guidance for CTIs
Board	Yes	Yes	Yes	Yes	N/A	N/A
Bureau	Yes	N/A	Yes	Yes	Yes	No
CFTC	Yes	No[a]	Yes	Yes	Yes	No
FDIC	No	No	Yes	N/A	No	No
FHFA[b]	No	N/A	No	No	Yes	No
NCUA	No	No	Yes	No	No	Yes[c]
OCC	Yes	N/A	Yes	Yes	Yes	No
SEC	Yes	No	Yes	Yes	Yes	No

[a] CFTC has not developed specific policies, procedures, or guidelines for the sharing of CTIs with regulated entities. CFTC does not receive a significant amount of information regarding CTIs and the information received do not contain classified information.

[b] FHFA does not maintain policy/procedure documentation specific to sharing CTIs. However, FHFA answered that it implemented (1) information sharing agreements with certain Federal agencies and its regulated entities (Fannie Mae, Freddie Mac, and the Federal Home Loan Banks), and (2) procedures for controlling the release of PII outside the agency.

[c] NCUA reported that it does not have the resources or mature capabilities to develop or sustain the development of procedures and policies, implement a repeatable process to efficiently analyze threat indicators, or to categorize and share the information with other entities.

Table A.2 summarizes the agencies' responses to Question 1d.

Entity	Guidance for implementing security controls to protect against unauthorized access to CTIs or DMs.
Board	The Board has implemented controls to protect CTIs and DM and these controls are reviewed on a regular basis and continuously improved.

[9] PII – personally identifiable information – information that, when used alone or with other relevant data, can identify an individual.

Entity	Guidance for implementing security controls to protect against unauthorized access to CTIs or DMs.
Bureau	The Bureau's approach for applying protections for CTIs is consistent with appropriate controls for Federal Information Security Management Act (FISMA)[10] moderate systems as defined by applicable NIST[11] guidelines if external to a Bureau-owned system.
CFTC	The CFTC protects its sensitive information, including CTIs and DMs, by leveraging the NIST Cybersecurity Framework and Risk Management Framework in compliance with the FISMA.
FDIC	The FDIC uses the Anomali threat intelligence platform to store CTIs and leverages built-in, role-based access controls.
FHFA	FHFA does not have policies, procedures, or guidelines for implementing security controls to specifically protect against unauthorized access to CTIs. However, in practice, access to all cyber defense solutions, including vulnerability information, is restricted to members of FHFA's cybersecurity team and information technology engineers, as needed.
NCUA	OCIO[12] uses access controls for the protection of threat indicators. Most controls are two-factor authentication and are applied on the file shares, ticketing system and security tools.
OCC	Access controls for the security tools used by the OCC's internal cybersecurity operations to centralize and collocate open source intelligence and vendor-supplied threat and vulnerability information are set by internal agency logical access management policy and meet NIST SP 800-53 baseline security control requirements.
SEC	The SEC has documented its overarching policies pertaining to the implementation of access controls.

[10] FISMA – Federal Information Security Management Act of 2002 - U.S. legislation that defines a comprehensive framework for protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality and availability. FISMA was amended by the Federal Information Security Modernization Act of 2014.

[11] NIST – National Institute of Standards and Technology – Part of the U.S. Department of Commerce, its mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

[12] OCIO – Office of the Chief Information Officer

Table A.3 summarizes the agencies' responses to Question 1f.

Entity	Guidance for notifying any U.S. person whose personal information is known to have been shared in violation of CISA
Board	The Board has guidance pertaining to this topic.
Bureau	The Bureau noted that it is not aware of any instance where a U.S. person's personal information has been shared in violation of CISA, and should this occur, the Bureau's Privacy Office would coordinate the notification.
CFTC	CFTC has in place an Incident Response Plan that addresses the notification process of affected individuals in case of a PII compromise.
FDIC	FDIC does not have policies, procedures or guidelines specific to notifying U.S. persons of information shared in violation of CISA.
FHFA	PII maintained by FHFA that is lost, compromised or disclosed to an unauthorized individual is addressed by the FHFA in accordance with its policy for addressing and reporting PII breaches.
NCUA	NCUA has an overarching breach policy which (a) establishes internal and external notification procedures and required actions when a breach of PII occurs; and (b) includes policy specific to breaches affecting NCUA employees, contractors and the public.
OCC	The OCC internal cybersecurity operations limit such sharing to technical details. As no information about individuals is included in such reporting, no additional policy or procedures are required to address such notifications.
SEC	SEC has a plan that defines the roles and responsibilities of agency employees, managers, and contractors, including subcontractors, regarding the suspected or confirmed breach of PII. The plan also provides processes, procedures and associated tasks required by the Office of Management and Budget, applicable laws, and regulations.

B. Classification and Accounting

The following questions were designed to gain an understanding on whether CTIs or DMs identified by or shared with agencies have been properly classified and whether there is accountability over the number of security clearances authorized by the Federal Government for the purpose of sharing CTIs or DMs with the private sector:

1. Has your agency shared CTIs and DMs with the private sector?
2. Did your agency classify (i.e., a national security classification of confidential, secret, or top secret) the CTIs and DMs shared with the private sector?
3. How did your agency determine whether the shared CTIs and DMs were properly classified?
4. How does your agency account for the number of security clearances authorized for sharing CTIs and DMs with the private sector?

Sharing and Classifying Cyber Threat Information.

Table B.1 summarizes the agencies' responses to Questions 1, 2 and 4.

Entity	Sharing CTIs and DMs with Private Sector	Classifying of Shared DMs and CTIs	Accountability of Authorized Security Clearances for sharing DMs and CTIs
Board	Yes	No	Yes
Bureau	No	N/A	N/A
CFTC	Yes	No	N/A
FDIC	No	N/A	N/A
FHFA	No	N/A	N/A
NCUA	No	N/A	N/A
OCC	No	N/A	N/A
SEC	Yes	No	Yes

For the three agencies that indicated they share CTIs and/or DMs with the private sector but did not indicate classifying this information, they provided the following explanations:

- The Board reported that classified CTIs and DMs are shared with the Federal Reserve Banks and unclassified open source CTIs could be shared with the private sector through the Emergency Communication System. The Board also reported that it does not have classification authority.

- CFTC reported that the information it receives from the Cyber Information Group (CIG)[13] Circular is not classified.
- SEC reported that it does not have original classification authority and has not shared CTIs or DMs with a national security classification.

Additionally, FDIC reported that it has not shared classified CTIs or DMs and does not have classifying authority. FHFA reported that it only shares CTIs and DMs with its regulated entities. FHFA does not consider the regulated entities to be the private sector; they are government-sponsored enterprises. NCUA reported it does not have classification authority.

Accounting for Security Clearances. The agency responses varied as to how they accounted for the number of security clearances authorized for sharing CTIs and DMs with the private sector. Specifically, they responded as follows:

- The Board stated that all requests for security clearances at the Federal Reserve Banks sponsored by the Board are reviewed and approved by appropriate Board staff.
- The Bureau and OCC reported that they have not shared CTIs or DMs with the private sector.
- CFTC reported it does not provide clearances for CTIs because the information received is not classified.
- FDIC reported that it has not sponsored security clearances for the private sector.
- FHFA reported the question is not applicable.
- NCUA reported that its OCIO has not shared indicators or DMs with the private sector on a classified or unclassified level.
- SEC reported that its Office of Support Operations manages the issuance and tracking of clearances issued to agency personnel. Clearances are issued pursuant to agency and federal guidance. SEC does not share classified information with the private sector.

C. Actions Taken

The following questions were designed to gain an understanding of the actions taken by the agencies in response to CTIs or DMs shared between the agencies and other federal agencies:

[13] CIG – Treasury's Financial Sector CIG was established within Treasury's Office of Cybersecurity and Critical Infrastructure Protection in 2013. CIG monitors and analyzes all source information on cyber threats and vulnerabilities to the financial sector; provides timely, actionable cyber threat information to the sector; and solicits feedback and information requirements from the sector.

Subsequent Uses and Dissemination

1. Has your agency used and disseminated CTIs and DMs shared by other federal agencies?
2. Did your agency use or disseminate the shared CTIs and DMs appropriately?
3. How did your agency determine if the use and dissemination of shared CTIs and DMs was appropriate?
4. Has your agency shared CTIs and DMs with other federal agencies?
5. Did your agency share the CTIs and DMs in a timely and adequate manner with appropriate entities or, if appropriate, make them publicly available?
6. Have other federal entities shared CTIs and DMs with your agency in a timely, adequate, and appropriate manner?
7. How did your agency determine timeliness, adequacy and appropriateness of sharing the information?
8. How many CTIs and DMs from non-federal entities did the Department of Homeland Security (DHS) relay to your agency?

Six of the eight Federal voting member agencies – the Board, Bureau, CFTC, FDIC, OCC and SEC – reported using and disseminating CTIs and DMs shared by other federal agencies. FHFA and NCUA responses varied as to the use or dissemination of CTIs or DMs shared by other federal agencies. All eight Federal voting member agencies reported that they have used and disseminated the shared CTIs and DMs appropriately.

Table C.1 summarizes the agencies' responses to Question 1.

Entity	Responses to "Has your agency used and disseminated CTIs and DMs shared by other federal agencies?"
Board	CTIs and DMs received from other federal agencies are shared with the Federal Reserve Banks when appropriate.
Bureau	The Bureau receives threat indicators from DHS, the Federal Bureau of Investigation (FBI), and other federal agencies. When needed to apply protective controls, the Bureau shares a small subset of indicator information with its Managed Internet Service Provider for the purpose of applying DMs as defined in CISA. When Traffic Light Protocol[14] markings are affixed to indicator information, the Bureau adheres to the control markings.

[14] Traffic Light Protocol - TLP is a set of designations used to ensure that sensitive information is shared with the appropriate audience. It employs four colors to indicate expected sharing boundaries to be applied by the recipient(s).

Entity	Responses to "Has your agency used and disseminated CTIs and DMs shared by other federal agencies?"
CFTC	Yes, about five or six times a year, CFTC receives a CIG Circular from OIA.[15] The CIG Circulars do not contain any classified information. Two Divisions within the CFTC, the Division of Market Oversight and the Division of Clearing and Risk, determine whether they would be relevant for entities regulated by the CFTC. If the CIG Circular is relevant, the CFTC will email the Circular to appropriate contacts at the regulated entities.
FDIC	Yes, FDIC has used CTIs and DMs shared by other agencies.
FHFA	Yes, but only those provided by US-CERT[16] and the FBIIC[17]. FHFA has not received CTIs and DMs directly from other federal agencies.
NCUA	OCIO has used indicators from other federal agencies but does not disseminate indicators outside of NCUA.
OCC	Yes
SEC	Yes, the SEC has used cyber threat indicators and defensive measures shared by other Federal agencies such as CISA/DHS and the Federal Bureau of Investigation (FBI).

Table C.2 summarizes the agencies' responses to Question 3.

Entity	Responses to "How did your agency determine if the use and dissemination of shared CTIs and DMs was appropriate?"
Board	Board staff work with the Federal Reserve Banks to evaluate and assess their specific needs for CTIs and DMs, and limit access to responsive material.
Bureau	The Bureau follows its standard procedures for indicator handling.
CFTC	CIG Circulars include a traffic light protocol establishing the extent to which information can be shared and the CFTC follows that protocol in disseminating information in the Circulars.

[15] OIA – Office of Intelligence and Analysis is part of Treasury's Office of Terrorism and Financial Intelligence. It advances national security and protects financial integrity by informing Treasury decisions with timely, relevant, and accurate intelligence and analysis.

[16] US-CERT – United States Computer Emergency Readiness Team – a partnership between DHS and the public and private sectors, established to protect the nation's internet infrastructure.

[17] FBIIC – Financial and Banking Information Infrastructure Committee – coordinates the efforts of Federal and State financial regulators to address critical infrastructure issues, including preparation for and response to cyber or physical attacks against the financial system or indirect attacks or events that may affect the sector. The FBIIC consists of 18 member organizations from across the financial regulatory community, both federal and state and is chaired by a designee of the Secretary of the Treasury.

Entity	Responses to "How did your agency determine if the use and dissemination of shared CTIs and DMs was appropriate?"
FDIC	The use of shared CTI was based on the automated confidence scoring and the nature of specific indicators. They were deployed to appropriate defensive and protective controls.
FHFA	FHFA shares CTIs with its regulated entities and other Federal agencies as needed and follows dissemination instructions received with the CTI.
NCUA	OCIO adheres to the traffic light protocol established by DHS.
OCC	OCC internal cybersecurity operations has established procedures that are consistent with US-CERT requirements and guidance appearing in NIST Special Publication 800-150, *Guide to Cyber Threat Information Sharing*.
SEC	SEC was able to determine that the use of shared CTIs and DMs were appropriate by utilizing SOC[18] policies and procedures as well as guidance issued by DHS.

Table C.3 summarizes the agencies' responses to Question 4.

Entity	Responses to "Has your agency shared CTIs and DMs with other federal agencies?"
Board	Yes, the Board noted that it shares CTIs and DMs with US-CERT and the Federal Reserve Banks.
Bureau	Yes, the Bureau shares indicators directly with the DHS National Cybersecurity and Communications Integration Center using the STIX[19] 2.0 taxonomy.
CFTC	Yes, the CFTC shares the CTIs with DHS CISA, which in turn will share the relevant information with Federal agencies.
FDIC	FDIC has not shared CTIs or DMs with other Federal agencies.
FHFA	Yes, but only to US-CERT.
NCUA	OCIO does not disseminate indicators outside of NCUA.

[18] SOC – Security Operations Center – a command center facility for a team of information technology professionals with expertise in information security that is responsible for monitoring, analyzing, and protecting an organization from cyber-attacks.

[19] STIX - Structured Threat Information Expression – a standardized XML programming language for conveying data about cybersecurity threats in a common language that can be easily understood by humans and security technologies.

Entity	Responses to "Has your agency shared CTIs and DMs with other federal agencies?"
OCC	OCC internal cybersecurity operations has shared indicators with Treasury's Government Security Operations Center.
SEC	Yes, the SEC has previously shared cyber threat indicators and defensive measures with other Federal agencies.

Table C.4 summarizes the agencies' responses to Question 5.

Entity	Responses to "Did your agency share the CTIs and DMs in a timely and adequate manner with appropriate entities or, if appropriate, make them publicly available?"
Board	Yes
Bureau	Yes, the Bureau shared all indicators associated with incidents within the timeframes defined in the Federal Incident Reporting Guidelines.
CFTC	The CFTC SOC reports incidents and shares CTIs and DMs with DHS US-CERT in accordance with established DHS time reporting guidelines. CFTC does not share information it receives from DHS outside of the agency. Also, CFTC does not make information from CIG Circulars publicly available. Rather, CFTC makes relevant information from CIG Circulars available to regulated entities in a prompt manner.
FDIC	FDIC has not shared CTIs or DMs with other Federal agencies.
FHFA	Yes, with US-CERT; FHFA does not make CTIs and DMs publicly available.
NCUA	Not applicable, as OCIO does not disseminate indicators outside of NCUA.
OCC	OCC internal cybersecurity operations followed its established procedures for this information sharing. This information was not shared publicly.
SEC	The SEC has previously shared cyber threat indicators in a timely manner with appropriate entities.

Table C.5 summarizes agencies' responses to Question 6.

Entity	Responses to "Have other federal entities shared CTIs and DMs with your agency in a timely, adequate, and appropriate manner?"
Board	In general, yes.

Entity	Responses to "Have other federal entities shared CTIs and DMs with your agency in a timely, adequate, and appropriate manner?"
Bureau	Yes, the Bureau is a participant in the DHS Automated Indicator Sharing[20] (AIS) program.
CFTC	Yes
FDIC	By our estimation, data is shared in a timely manner. However, appropriateness is undermined by a large volume of indicators that alert on actors performing reconnaissance activity against the FDIC's outer bastion of network devices. The volume of indicators seems to adequately address various threat vectors, specifically those vectors for which the FDIC has a means to detect.
FHFA	FHFA has no way to make such a determination.
NCUA	Yes. OCIO receives indicators and DMs through the HSIN[21] portal, weekly Federal SOC calls, and bulletins from other federal entities as they are released.
OCC	Yes
SEC	Yes

Table C.6 summarizes agencies' responses to Question 7.

Entity	Responses to "How did your agency determine timeliness, adequacy and appropriateness of sharing the information?"
Board	There are no explicit metrics or measurement techniques for timeliness of information sharing.
Bureau	The AIS program provides the fastest available mechanism for unclassified indicator dissemination.
CFTC	The agency does not determine timeliness. Rather, the agency evaluates information received from either DHS or Treasury's OIA and assesses relevance to either the agency or to regulated entities.

[20] Automated Indicator Sharing – DHS' free capability that enables the exchange of CTIs between the Federal Government and the private sector at machine speed.

[21] HSIN - Homeland Security Information Network – is DHS' official system for trusted sharing of Sensitive but Unclassified information between federal, state, local, territorial, tribal, international and private sector partners.

Entity	Responses to "How did your agency determine timeliness, adequacy and appropriateness of sharing the information?"
FDIC	By our estimation, data is shared in a timely manner. However, appropriateness is undermined by a large volume of indicators that alert on actors performing reconnaissance activity against the FDIC's outer bastion of network devices. The volume of indicators seems to adequately address various threat vectors, specifically those vectors for which the FDIC has a means to detect.
FHFA	Not Applicable.
NCUA	OCIO has used indicators from other federal agencies, but does not disseminate indicators outside of NCUA. OCIO has not measured timeliness, adequacy and appropriateness of indicators from other federal agencies.
OCC	OCC's internal cybersecurity operations follow directions established in US-CERT federal incident notifications guidelines with regard to timely, adequate, and appropriate information sharing.
SEC	SEC evaluates the timeliness, adequacy, and appropriateness of the information shared on a case-by-case basis.

Table C.7 summarizes agencies' responses to Question 8.

Entity	Responses to "How many CTIs and DMs from non-federal entities did the DHS relay to your agency?"
Board	DHS did not relay any CTIs or DMs.
Bureau	As of June 2019, the Bureau had CTIs provided by DHS in its Threat Intelligence Platform. The Bureau did not receive the origin report for many of these indicators, so it is unclear how many were provided by non-Federal entities.
CFTC	Based on the information received from DHS and Treasury's OIA, CFTC is not able to determine whether CTIs conveyed by DHS are from non-federal entities.
FDIC	Undetermined. FDIC does not receive breakdowns of the original source of CTIs or DMs.
FHFA	This is a question for DHS.
NCUA	OCIO has received approximately 500 bulletins and advisories since January 1, 2019. It is difficult to determine non-federal vs federal agencies due to DHS not attributing CTIs or DMs to a specific agency or private entity.

Entity	Responses to "How many CTIs and DMs from non-federal entities did the DHS relay to your agency?"
OCC	DHS routinely relays such indicators and measures from non-federal entities through their semi-weekly conference calls and its situational awareness submissions to FS-ISAC,[22] which are sent out to both federal and local government agencies.
SEC	SEC regularly receives CTIs and DMs issued by DHS as part of DHS information sharing initiatives and regular report issuances.

D. Information Not Directly Related to a Cybersecurity Threat

The following questions were designed to gain an understanding of whether any information that is personal information of a specific individual was shared by a federal or non-federal entity with the agencies in contravention of law or guidelines required by CISA:

1. Did any federal or non-federal entity share information with your agency that was not directly related to a cybersecurity threat that is personal information of a specific individual or information identifying a specific individual in violation of CISA?
2. Please include a description of the violation.
3. To your knowledge, has your agency's sharing of CTIs and DMs within the Federal Government or with non-federal entities had an effect on the privacy and civil liberties of specific individuals?
4. What was the effect on privacy and civil liberties of specific individuals?
5. How did your agency quantitatively and qualitatively assess the effect?
6. Did your agency receive any notices regarding a failure to remove information that was not directly related to a cybersecurity threat and were any of those notices related to personal information of a specific individual or information that identified a specific individual?
7. How many notices did your agency receive?
8. Did your agency issue any notices regarding a failure to remove information that was not directly related to a cybersecurity threat and were any of those notices related to personal information of a specific individual or information that identified a specific individual?
9. How many notices did your agency issue?

[22] FS-ISAC – Financial Services Information Sharing and Analysis Center – is an industry consortium dedicated to reducing cyber-risk in the global financial system. It was created in response to the US Presidential Decision Directive 63, which was issued in 1998 and updated in 2003 by the Homeland Security Presidential Decision Directive 7.

10. Do you believe the steps taken by your agency to reduce adverse effects from the activities carried out under this title on the privacy and civil liberties of U.S. persons were adequate?
11. How did your agency determine adequacy of the steps taken?

All Federal voting member agencies reported that they had not shared information not directly related to a cybersecurity threat that was personal in nature or had an effect on the privacy and civil liberties of individuals. Further, they had not issued or received any notices regarding failure to remove information not directly related to a cybersecurity threat or personally identifiable information. As a result, the agencies' responses to all other related questions were either no or not applicable.

E. Barriers

The following questions were designed to obtain each agency's perspective on any barriers to the sharing of CTIs or DMs among federal entities and non-federal entities:

1. Has your agency identified any barriers that adversely affected the sharing of CTIs and DMs among federal entities and non-federal entities?
2. Please describe the barriers and the effect the barriers have on the sharing of CTIs and DMs.

Barriers to Sharing Cyber Threat Information. Three of the eight Federal voting member agencies – the Board, the Bureau, and NCUA – reported barriers to sharing cyber threat information. The Board shared that intelligence providers should continue to weigh the need to highly classify actionable information as this limits the ability to widely share such information. The Board also noted that the need to have Secure Compartmentalized Information clearances for all recipients limits the ability to implement actionable intelligence quickly and efficiently. The Bureau stated that, in general, the AIS program worked as intended. However, it was difficult to get responses from the DHS Cyber Liaison team regarding technical specifics on options available to leverage deeper analysis on shared indicators (for example, how to take advantage of shared DHS LookingGlass[23] services). NCUA reported that OCIO does not have the resources, fiscal funds, or technical capabilities to implement a sharing of CTIs and DM program.

For the remaining five Federal voting member agencies:

- CFTC, FHFA, OCC and SEC did not report any barriers.
- FDIC reported that it has not shared CTIs or DMs with other federal or non-federal entities.

[23] LookingGlass is a contractor used by DHS to provide a variety of platforms and services to meet a range of cyber intelligence needs.

II. Office of Cybersecurity and Critical Infrastructure Protection

Located within Treasury's Office of Domestic Finance, OCCIP works closely with financial sector firms, industry groups, and government partners to share information about cybersecurity and physical threats and vulnerabilities, encourage the use of baseline protections and best practices, and respond to and recover from significant incidents affecting the sector. OCCIP executes the responsibilities assigned to Treasury as the Sector Specific Agency for the Financial Services Sector by Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience*, and Executive Order 13636, *Improving Critical Infrastructure Cybersecurity* (February 12, 2013).

An OCCIP official told us that they actively work to bring awareness of CISA to the financial sector and work with government agencies to better understand CISA and its utility to firms. To facilitate this information sharing, OCCIP collaborates across organizations and with financial services sector groups such as the Financial and Banking Information Infrastructure Committee (regulators), the Financial Services Sector Coordinating Council, Financial Services Sector Government Coordinating Council, and the Financial Services Information Sharing and Analysis Center. OCCIP encourages firms to share actionable information (e.g., Indicators of Compromise) under the protections afforded under CISA, in accordance with other laws and applicable regulations consistent with their overall risk management strategy. However, as Treasury is not a regulator, OCCIP does not enforce compliance with CISA. (Given the existing degree of regulation and number of regulators of the sector, this is not an authority sought by Treasury.) Rather, OCCIP works to raise awareness of the benefits of voluntary cybersecurity information sharing under CISA by and with individual firms and the sector, as a whole; to date, it has not received any information sharing that has been explicitly linked to CISA.

III. Financial Stability Oversight Council Secretariat

FSOC Secretariat is a dedicated policy office within Treasury that assists in coordinating the work of the FSOC among its members and member agencies. An FSOC Secretariat official told us the Secretariat's role is to support FSOC activities by performing research, ensuring compliance with FSOC policies (bylaws), and providing administrative support (budget).

The FSOC Secretariat official also told us that FSOC's role in CISA is limited. The topic of cybersecurity had been discussed at meetings and in FSOC's annual reports, but CISA, the statute itself, had been rarely discussed. CISA was last

mentioned in FSOC's 2016 Annual Report.[24] FSOC Secretariat focuses on bringing regulatory attention of cybersecurity to private and government entities and providing recommendations. To date, the FSOC has not received any information explicitly related to CISA.

[24] In that report, FSOC noted that the Cybersecurity Act of 2015, which includes CISA, provides a foundation for further advances in cybersecurity-related information sharing. FSOC recommended that Treasury, the Departments of Homeland Security, Justice, and Defense, and financial regulators strongly support efforts to implement this legislation, including coordinating their associated processes with the financial services sector, consistent with processes established by the law.

Abbreviations

AIS	Automated Indicator Sharing
Board	Board of Governors of the Federal Reserve System
Bureau	Bureau of Consumer Financial Protection
CFTC	Commodity Futures Trading Commission
CIG	Cyber Intelligence Group
CIGFO	Council of Inspectors General on Financial Oversight
CISA	Cybersecurity Information Sharing Act of 2015
CTI	Cyber threat indicator
DHS	Department of Homeland Security
DM	Defensive measures
FBI	Federal Bureau of Investigation
FBIIC	Financial and Banking Information Infrastructure Committee
FDIC	Federal Deposit Insurance Corporation
FISMA	Federal Information Security Management Act of 2002
FHFA	Federal Housing Finance Agency
FS-ISAC	Financial Services Information Sharing Analysis Center
FSOC	Financial Stability Oversight Council
HSIN	Homeland Security Information Network
IC IG	Intelligence Community Inspector General
NCUA	National Credit Union Administration

Abbreviations (continued)

NIST	National Institute of Standards and Technology
OCC	Office of the Comptroller of the Currency
OCCIP	Office of Cybersecurity and Critical Infrastructure Protection
OCIO	Office of the Chief Information Officer
OIA	Office of Intelligence and Analysis
OIG	Office of Inspector General
PII	Personally identifiable information
SEC	U.S. Securities and Exchange Commission
SOC	Security Operations Center
STIX	Structured Threat Information Expression
Treasury	Department of the Treasury
US-CERT	United States Computer Emergency Readiness Team

THIS PAGE IS INTENTIONALLY LEFT BLANK.