Top Management and Performance Challenges Facing Financial-Sector Regulatory Organizations

Council of Inspectors General on Financial Oversight

Approved July 2019

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

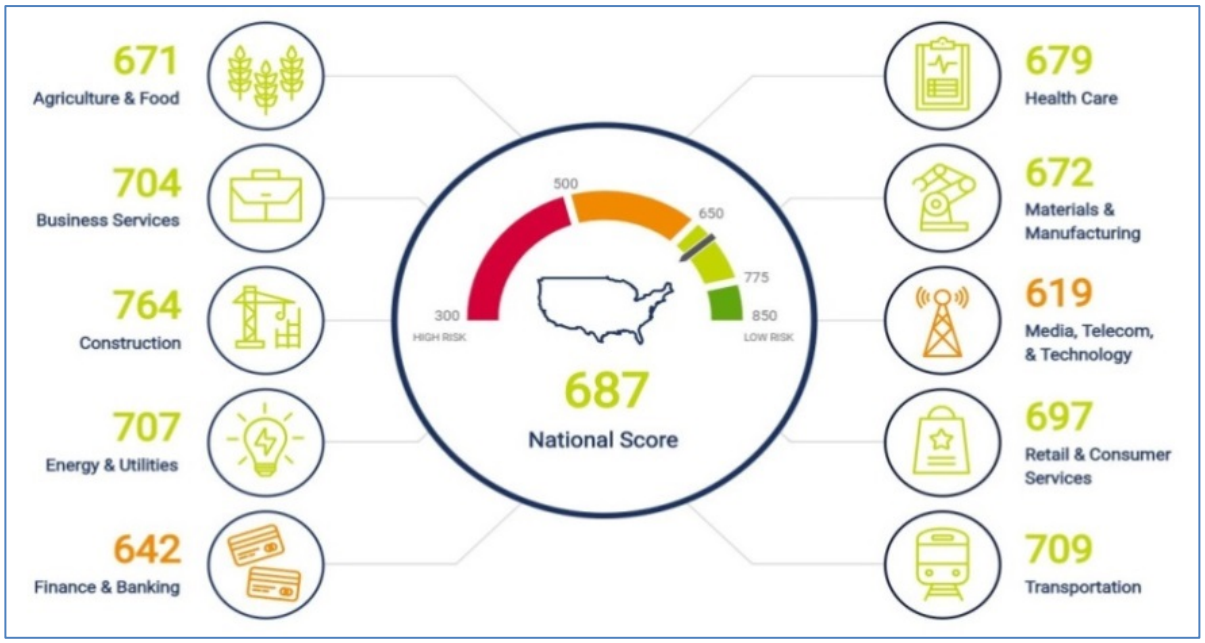
Cybersecurity continues to be a critical risk facing the financial sector. FSOC recognized in its December 2018 Annual Report that as financial institutions increase their reliance on technology, there is an increased risk that a cybersecurity event could have "severe negative consequences, potentially 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).

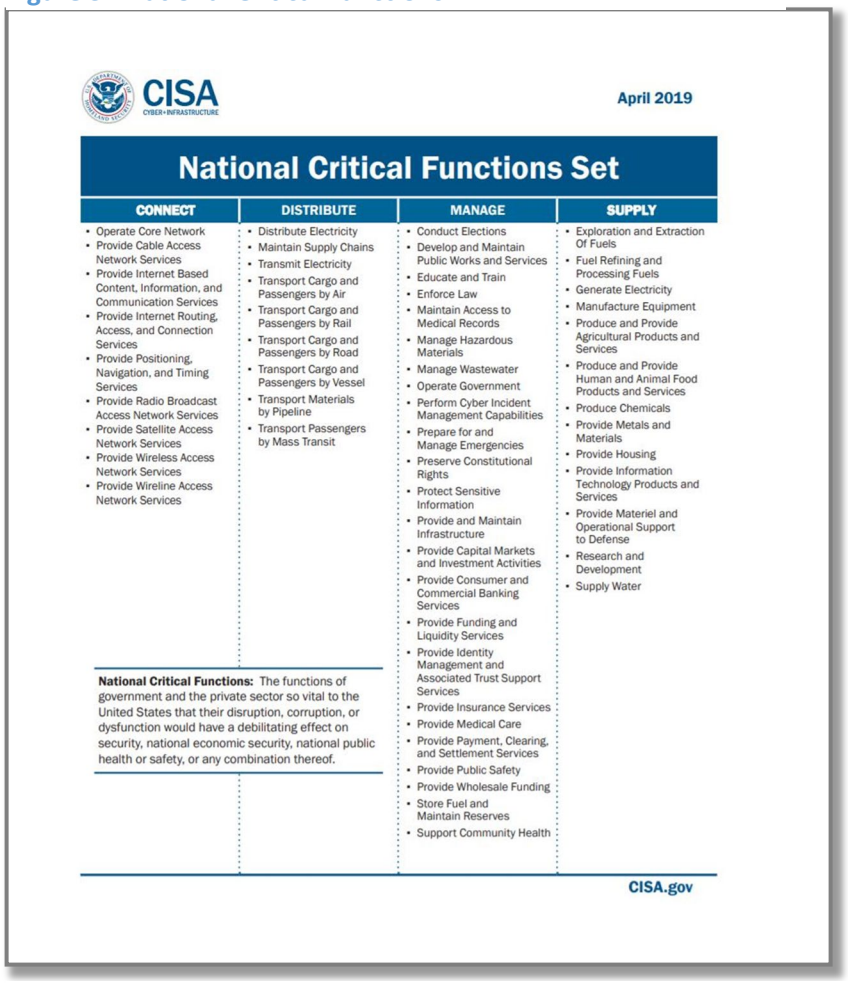
CHALLENGE 3 SHARING THREAT INFORMATION

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

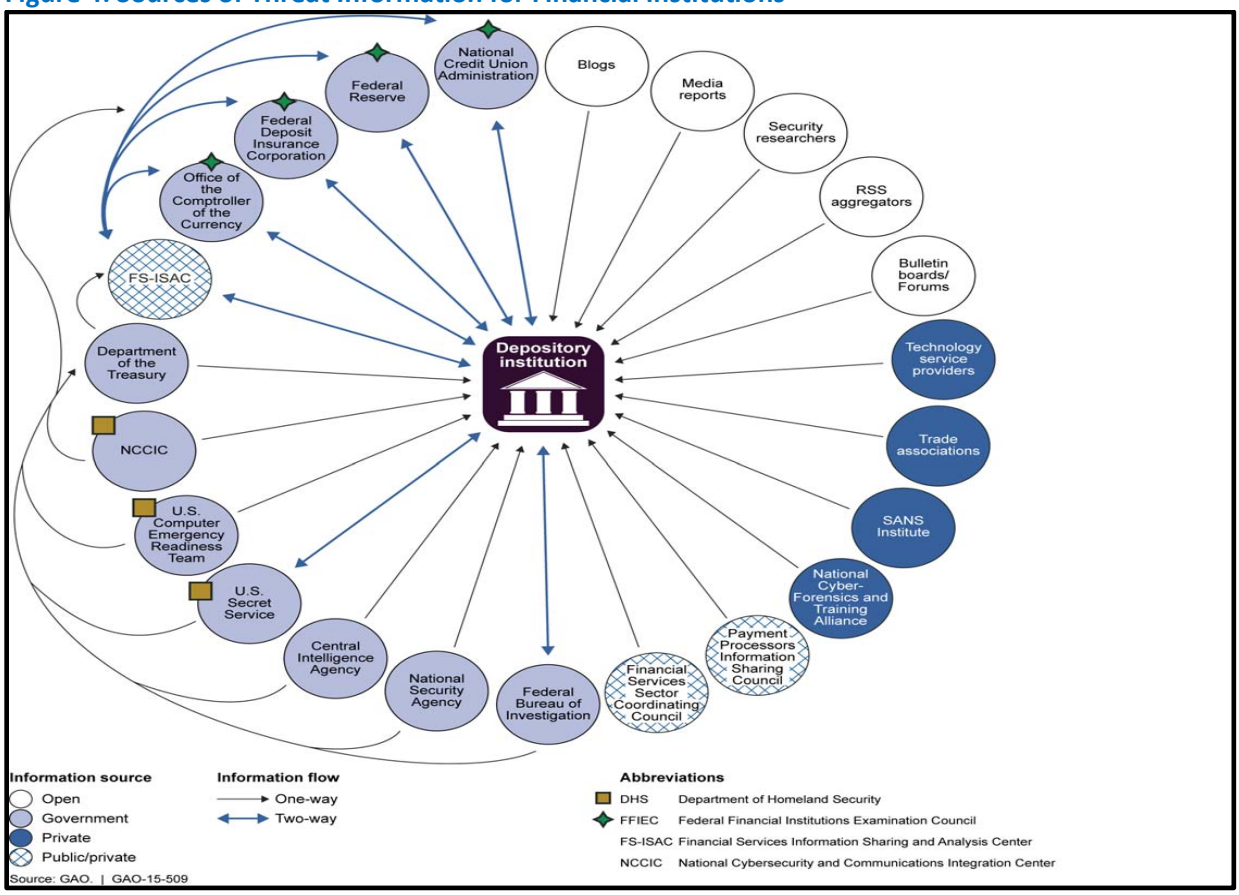


Source: Cybersecurity and Infrastructure Security Agency

[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

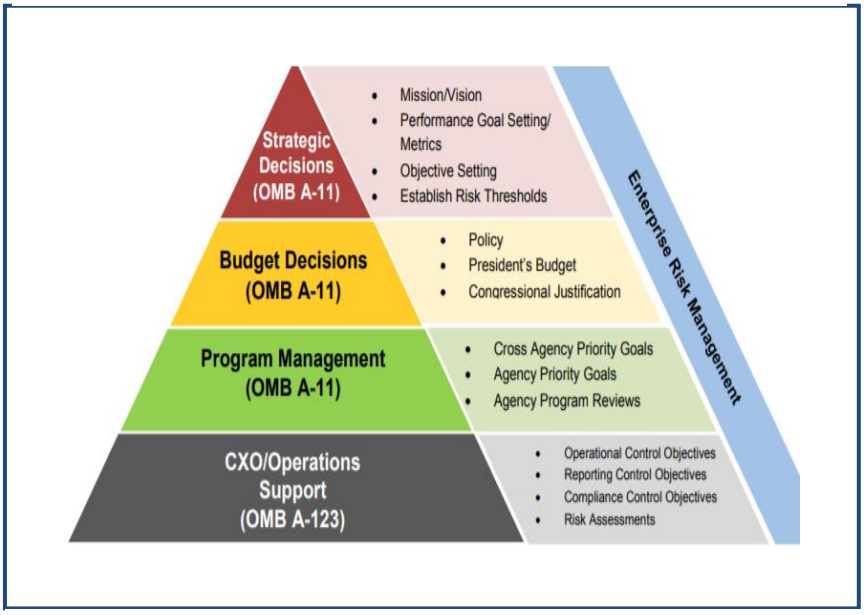
According to OMB Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control,* (OMB Circular A-123), Federal agencies face internal and external risks to achieving their missions, including "economic, operational, and organizational change factors, all of which 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.