SEPTEMBER 2018

Top Management and Performance Challenges Facing Financial Regulatory Organizations

Approved September 13, 2018

EXECUTIVE SUMMARY

Purpose

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

Approach

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

CIGFO Members

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

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

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

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

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

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

TABLE OF CONTENTS

BACKGROUND AND OBSERVATIONS

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

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

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

Table 1 - CIGFO Membership & Oversight

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

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

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

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

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

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

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

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

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

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

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

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

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

CHALLENGE 1 ENHANCING OVERSIGHT OF FINANCIAL INSTITUTION CYBERSECURITY

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

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

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

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

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

Cybersecurity Examinations

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

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

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

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

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

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

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

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

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

Vulnerabilities in Interconnections with Third-Party Service Providers

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

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

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

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

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

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

CHALLENGE 2 MANAGING AND SECURING INFORMATION TECHNOLOGY AT REGULATORY ORGANIZATIONS

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

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

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

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

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

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

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

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

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

IT Security Risk Management

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

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

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

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

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

[23] Public Law No. 113-283.

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

Obsolete IT

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

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

Shortage of IT Security Professionals

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

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

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

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

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

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

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

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

CHALLENGE 3 SHARING THREAT INFORMATION

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

Sharing Threat Information with Financial Institutions and Examiners

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

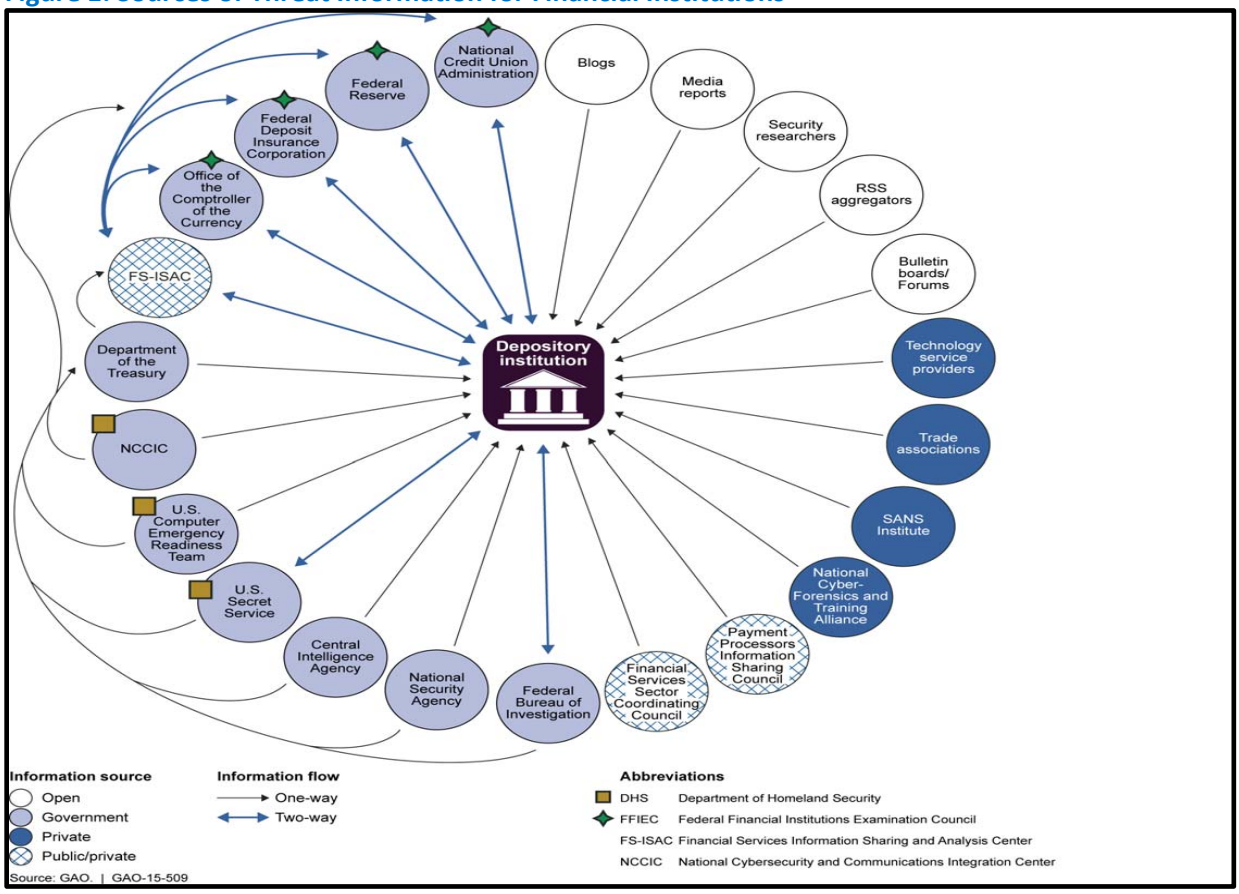
[28] In 2006, the Department of Homeland Security developed the National Infrastructure Protection Plan (NIPP); one portion of the NIPP relates to the financial sector – the *Banking and Finance Critical Infrastructure and Key Resources Sector-Specific Plan (Financial Sector-Specific Plan)*. The plans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

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

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

[31] FSOC 2017 Annual Report.

Figure 1: Sources of Threat Information for Financial Institutions



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

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

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

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

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

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

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

---

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

CHALLENGE 4 READINESS FOR CRISES

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

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

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

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

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

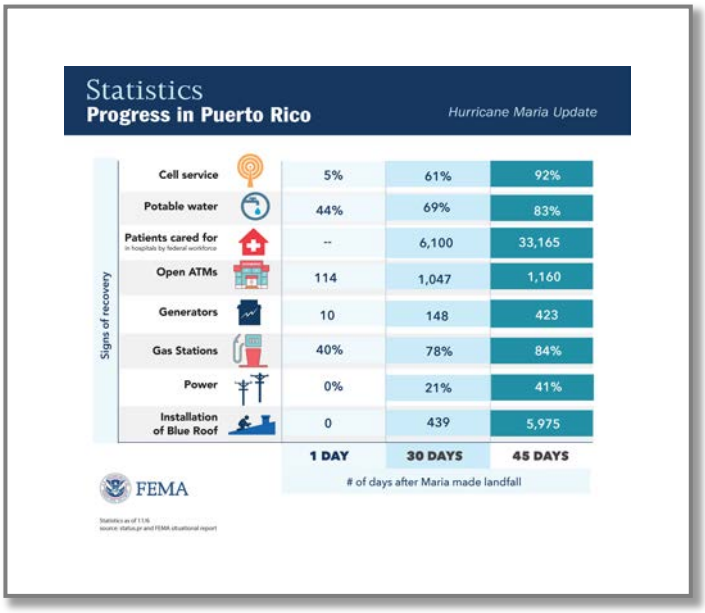
[41] Since the end of 2009, the DIF has grown every quarter and became positive in the second quarter of 2011. The DIF balance as of December 31, 2017 was $92.7 billion.

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

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

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

Figure 2: FEMA Hurricane Maria Statistics



Readiness for Failures of Financial Institutions

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

---

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

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

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

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

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

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

Readiness for Disaster Aid

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

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

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

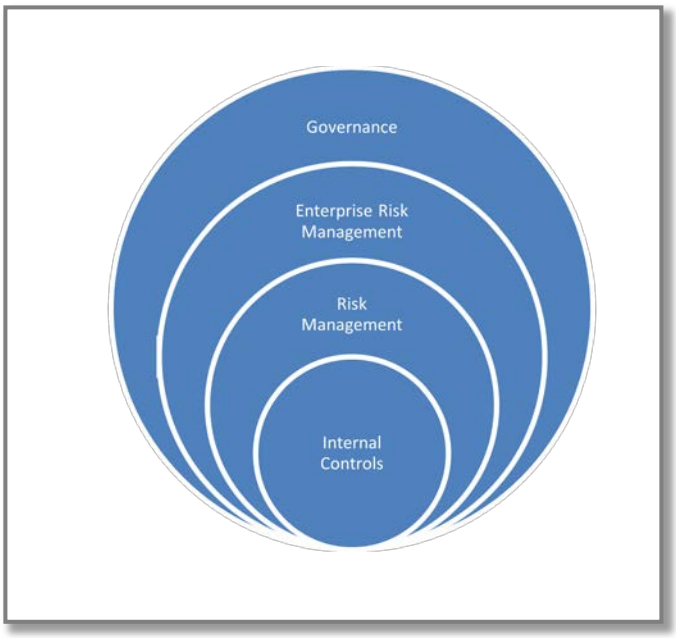
[49] Created by Congress in 1970, NCUA administers the Share Insurance Fund and insures individual credit union member accounts against losses up to $250,000 and a member's interest in all joint accounts combined up to $250,000. https://www.ncua.gov/services/Pages/share-insurance.aspx

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

CHALLENGE 5 STRENGTHENING AGENCY GOVERNANCE

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

Figure 3: OMB Governance Model



Source: Office of Management and Budget

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

Enhance Enterprise Risk Management

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

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

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

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

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

Improve Internal Controls

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

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

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

CHALLENGE 6 MANAGING HUMAN CAPITAL

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

Succession Planning

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

Effective Human Capital Management

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

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

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

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

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

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

CONCLUSION

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

APPENDIX 1 ABBREVIATIONS AND ACRONYMS

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

APPENDIX 2 METHODOLOGY

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

Department of the Treasury

Federal Deposit Insurance Corporation

Commodity Futures Trading Commission

Bureau of Consumer Financial Protection

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

Board of Governors of the Federal Reserve System

Federal Housing Finance Agency

National Credit Union Administration (begins on page 81)

Securities and Exchange Commission

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

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