United States Government Accountability Office

Report to Congressional Addressees

September 2020

CRITICAL INFRASTRUCTURE PROTECTION

Treasury Needs to Improve Tracking of Financial Sector Cybersecurity Risk Mitigation Efforts

Accessible Version

GAO-20-631

September 2020

GAO Highlights

Highlights of GAO-20-631, a report to Congressional Addressees

CRITICAL INFRASTRUCTURE PROTECTION

Treasury Needs to Improve Tracking of Financial Sector Cybersecurity Risk Mitigation Efforts

Why GAO Did This Study

For decades, the federal government has taken steps to protect the nation's critical infrastructures. The financial services sector's reliance on information technology makes it a leading target for cyber-based attacks. Recent high-profile breaches at commercial entities have heightened concerns that data are not being adequately protected.

Under the Comptroller General's authority, GAO initiated this review to (1) describe the key cyber-related risks facing the financial sector; (2) describe steps the financial services industry is taking to share information on and address risks to its sector; and (3) assess steps federal agencies are taking to enhance the security and resilience of the sector. GAO analyzed relevant reports and information to determine risks and mitigation efforts and compared agency efforts against federal policies and guidance. GAO also interviewed officials at 16 private sector entities, two self-regulatory organizations, and eight federal agencies, including the Department of the Treasury.

What GAO Recommends

GAO is making recommendations to Treasury to track and prioritize the sector's cyber risk mitigation efforts, and to update the sector's plan with metrics for measuring progress and information on how sector efforts will meet sector goals and requirements, including those contained within the *National Cyber Strategy Implementation Plan.* Treasury generally agreed with the recommendations.

View GAO-20-631. For more information, contact Nick Marinos at (202) 512-9342 or marinosn@gao.gov or Michael Clements at (202) 512-7763 or clementsm@gao.gov.

What GAO Found

The federal government has long identified the financial services sector as a critical component of the nation's infrastructure. The sector includes commercial banks, securities brokers and dealers, and providers of the key financial systems and services that support these functions. Altogether, the sector holds about $108 trillion in assets and faces a variety of cybersecurity-related risks. Key risks include (1) an increase in access to financial data through information technology service providers and supply chain partners; (2) a growth in sophistication of malware—software meant to do harm—and (3) an increase in interconnectivity via networks, the cloud, and mobile applications. Cyberattacks that exploit risks can occur against either public or private components of the sector. For example, in February 2016, hackers were able to install malware on the Bangladesh Central Bank's system through a service provider, which then directed the Federal Reserve Bank of New York to transfer money to accounts in other Asian countries. This attack resulted in the theft of approximately $81 million.

Several industry groups and firms are taking steps to enhance the security and resilience of the U.S. financial services sector through a broad range of cyber risk mitigation efforts. These efforts include coordinating within the sector through groups such as the Financial Services Sector Coordinating Council and the Financial Systemic Analysis and Resilience Center, conducting industrywide incident response exercises, sharing threat and vulnerability information, developing and providing guidance in conducting risk assessments, and offering cybersecurity-related training.

The Departments of Homeland Security and the Treasury and federal financial regulators are also taking multiple steps to support cybersecurity and resilience through risk mitigation efforts. Among other things, federal agencies provide cybersecurity expertise and conduct simulation exercises related to cyber incident response and recovery. Treasury, as the designated lead agency for the financial sector, plays a key role in supporting many of the efforts to enhance the sector's cybersecurity and resiliency. For example, Treasury's Assistant Secretary for Financial Institutions serves as the chair of the committee of government agencies with sector responsibilities, and Treasury coordinates federal agency efforts to improve the sector's cybersecurity and related communications.

However, Treasury does not track efforts or prioritize them according to goals established by the sector for enhancing cybersecurity and resiliency. Treasury also has not fully implemented GAO's previous recommendation to establish metrics related to the value and results of the sector's risk mitigation efforts. Further, the 2016 sector-specific plan, which is intended to direct sector activities, does not identify ways to measure sector progress and is out of date. Among other things, the sector-specific plan lacks information on sector-related requirements laid out in the 2019 *National Cyber Strategy Implementation Plan*. Unless more widespread and detailed tracking and prioritization of efforts occurs according to the goals laid out in the sector-specific plan, the sector could be insufficiently prepared to deal with cyber-related risks, such as those caused by increased access to data by third parties.

Contents

Tables

Abbreviations

ABA American Bankers Association

BPI	Bank Policy Institute
CFTC	Commodity Futures Trading Commission
CIP	critical infrastructure protection
DHS	Department of Homeland Security
FBIIC	Financial and Banking Information Infrastructure Committee
FDIC	Federal Deposit Insurance Corporation
FFIEC	Federal Financial Institutions Examination Council
FINRA	Financial Industry Regulatory Authority
FRB	Board of Governors of the Federal Reserve System
FSARC	Financial Systemic Analysis and Resilience Center
FS-ISAC	Financial Services Information Sharing and Analysis Center
FSSCC	Financial Services Sector Coordinating Council
GCC	government coordinating council
ICBA	Independent Community Bankers of America
NCUA	National Credit Union Administration
NFA	National Futures Association
NIPP	National Infrastructure Protection Plan
OCC	Office of the Comptroller of the Currency
PPD-21	Presidential Policy Directive 21
SCC	sector coordinating council
SEC	Securities and Exchange Commission
SIFMA	Securities Industry and Financial Markets Association
Treasury	Department of the Treasury

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

September 17, 2020

Congressional Addressees

The federal government has identified the financial services sector as part of its critical infrastructure protection (CIP) efforts.[1] The financial services sector includes commercial banks, mutual funds, securities brokers and dealers, insurance companies, credit and financing organizations, and the providers of the critical financial systems and services that support these functions.

U.S. financial institutions held over $108 trillion in assets as of the fourth quarter of 2019, making their security vital to public confidence and the nation's safety, prosperity, and well-being.[2] The potential for monetary gains and economic disruptions increases the financial services sector's attractiveness as a target for malicious actors. High-profile breaches at commercial entities, such as Equifax, have heightened concerns that data are not being adequately protected.[3]

In 2003, we expanded our existing federal information security high-risk area to include the protection of critical cyber infrastructure and it continues to be listed in our high-risk series report.[4] In the latest report of

[1]The term "critical infrastructure" as defined in the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001* (USA PATRIOT Act) refers to systems and assets so vital to the United States that their incapacity or destruction would have a debilitating impact on security, national economic security, national public health or safety, or any combination of these. 42 U.S.C. §5195c(e). Federal policy identifies 16 critical infrastructures: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; health care and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems.

[2]Board of Governors of the Federal Reserve System, *Financial Accounts of the United States: Flow of Funds, Balance Sheets, and Integrated Macroeconomic Accounts* (Washington, D.C.: Mar. 12, 2020).

[3]See GAO, *Data Protection: Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach,* GAO-18-559 (Washington, D.C.: August 30, 2018) for more details on this breach.

[4]GAO, *High-Risk Series:* Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas, GAO-19-157SP (Washington, D.C.: Mar. 6, 2019).

the high-risk series, we identified actions that the federal government and other entities needed to take to address cybersecurity challenges facing the nation.

We performed our current work under the authority of the Comptroller General, to further assist Congress with its oversight of efforts to enhance the cybersecurity of the financial services sector. The specific objectives of this review were to (1) describe the key cyber-related risks facing the financial services sector, (2) describe steps the financial services industry is taking to share information on and address risks to its sector, and (3) assess steps that federal agencies are taking to enhance the security and resilience of the financial services sector.

To address all three objectives, we selected a subset of federal agencies, self-regulatory organizations, private sector organizations, and private sector firms with relevance to the financial services sector.[5]

- We analyzed federal policy and prior GAO work to identify federal agencies with regulatory or critical infrastructure protection roles related to the financial services sector. We identified and selected eight agencies with these roles: the Departments of Homeland Security (DHS) and the Treasury (Treasury), the Commodity Futures Trading Commission (CFTC), the Federal Deposit Insurance Corporation (FDIC), the Board of Governors of the Federal Reserve System (FRB), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Securities and Exchange Commission (SEC).
- We analyzed federal guidance and prior GAO work, and held interviews with federal regulatory officials to identify relevant self-regulatory organizations. We identified and selected two self-regulatory organizations, based on their oversight of respective regulated entities within the financial services sector: the Financial Industry Regulatory Authority (FINRA) and the National Futures Association (NFA).
- We analyzed federal and sector guidance and past GAO reports to identify sectorwide groups that were established to meet the cybersecurity related goals of the financial services sector. Based

[5]Self-regulatory organizations are non-governmental organizations that have the responsibility to regulate their own members through the adoption and enforcement of rules of conduct for fair, ethical, and efficient practices in their industries.

on our analysis and the corroboration of responsible federal agency officials about the most active groups, we identified and selected six groups. Two of the six groups, the Financial Sector Information Sharing and Analysis Center (FS-ISAC) and the Financial Services Sector Coordinating Council (FSSCC), are focused on the critical infrastructure of the sector. Four of the six groups represent the interest of their members in the financial services industry: the American Bankers Association (ABA), Bank Policy Institute (BPI), Independent Community Bankers of America (ICBA), and the Securities Industry and Financial Markets Association (SIFMA).

- We analyzed sector firms based on the risk level of their critical infrastructure, firm size, role within the sector, and willingness to voluntarily participate in our review. Based on our analysis and feedback from private sector groups, we selected 10 private sector financial firms, including banks, an exchange, and technology providers, to gain insight into their efforts to mitigate cybersecurity risks. We included large and small banks, as measured by total assets, because their operations were very different. The 10 firms were the Bank of America, Capital City Bank, Chicago Board Options Exchange, the Depository Trust & Clearing Corporation, First United Bank and Trust, Goldman Sachs, Morgan Stanley, Neocova, Paypal, and SoFi.

To accomplish the first objective, we performed a literature search to identify reports that focused on one or more specific risks to the financial sector. From this search, we identified six private-sector reports that were completed by firms with cybersecurity expertise within the last decade. We analyzed each report to determine the risks that were referenced in each and the types of individuals or groups that posed threats to exploit them. We corroborated the list of risks through interviews with officials from each of the agencies, sectorwide groups, and private sector firms with responsibility for mitigating cybersecurity risks within their respective firm or within the financial services sector.

To accomplish the second objective, we collected and analyzed documentation to understand the cyber risk mitigation efforts performed by each of the sectorwide groups that we selected. We also interviewed senior officials with responsibilities related to cybersecurity efforts, such as vice presidents or those in charge of financial operations, at each organization using a standard set of questions pertaining to cyber risk mitigation roles, coordination partners, and efforts. We analyzed the information provided and interview responses and, based on the analysis,

developed a list of cyber risk mitigation efforts that we categorized by common themes, such as information sharing. Also, based on the interviews, we developed a list of the most common challenge areas for which firms believed greater assistance was needed from the government.

To accomplish the third objective, we collected and analyzed documentation from each selected agency and self-regulatory organization regarding their cyber risk mitigation efforts. Similar to the steps we took with private-sector organizations, we also interviewed officials with responsibilities related to the cybersecurity of the sector, to learn about each entity's cyber risk mitigation roles, requirements, coordination partners, and efforts. Based on our analysis of information provided to us about their cyber risk mitigation efforts, we categorized the efforts being performed by the agencies and self-regulatory organizations by common themes, such as conducting incident response and recovery exercises.

We then compared the list of categorized efforts to a set of requirements derived from federal policy documents pertaining to the critical infrastructure of the financial services sector to determine if the efforts performed by each agency or self-regulatory organization met the applicable requirements. We determined which requirements from federal policy documents were applicable using an "independent coder" method, in which multiple staff independently assigned a priority level to each potential requirement, and then met to discuss and agree on overall priorities. Only the highest priority requirements were used in the comparison

In addition, we analyzed agency efforts to set up mechanisms for collaboration with private-sector entities by comparing information in sector plans and actions taken by Treasury and DHS against leading practices for collaboration identified by GAO. Appendix I provides a more complete description of our objectives, scope, and methodology.

We conducted this performance audit from June 2019 to September 2020 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

The financial services sector includes depository institutions, providers of investment products, insurance companies, other credit and financing organizations, equities and derivatives markets, and the providers of the critical financial market utilities and services that support these functions. Financial institutions vary widely in size and presence, ranging from some of the world's largest global companies with thousands of employees and many billions of dollars in assets, to community banks and credit unions with a small number of employees serving individual communities.

According to statistics from the FRB, U.S. financial institutions held over $108 trillion in assets as of the fourth quarter of 2019.[6] Some of the largest categories of financial institutions, in terms of assets held, are U.S.-chartered depository institutions ($16.33 trillion), insurance companies ($11.28 trillion), mutual funds ($17.66 trillion), government sponsored enterprises ($7.11 trillion), and pension funds ($24.36 trillion). The remaining assets are distributed among finance and mortgage companies, securities brokers and dealers, and other financial institutions.

Financial Institutions Provide a Variety of Products

Financial institutions are organized and regulated based on the services they provide and how they are chartered. These services include several types of financial product categories, such as: (1) deposit, consumer credit, and payment systems products; (2) credit and liquidity products; (3) investment products; and (4) risk transfer products.[7]

- **Deposit, consumer credit, and payment systems products.** Depository institutions are the primary providers of wholesale and retail payments services, such as wire transfers, checking accounts, and credit and debit cards. Depository institutions and their technology service providers facilitate the conduct of transactions across the payments

[6]Board of Governors of the Federal Reserve System, *Financial Accounts of the United States: Flow of Funds, Balance Sheets, and Integrated Macroeconomic Accounts* (Washington, D.C.: Mar. 12, 2020).

[7]Departments of Homeland Security and Treasury, *Financial Services Sector-Specific Plan 2015* (Washington, D.C.: Mar. 4, 2016)

infrastructure, including automated clearinghouses (ACH), large value payment systems, and automated teller machines (ATMs).[8]

At the federal level, primary regulatory responsibility for depository institutions is carried out by FRB, FDIC, NCUA, and OCC.

- **Credit and liquidity products.** Depository institutions, finance and lending firms, securities firms, and government-sponsored enterprises meet customers' long- and short-term credit needs through a variety of financial products. Some of these entities provide credit directly to the end customer, while others do so indirectly by offering liquidity to retail based financial services firms.
- **Investment products.** Investment products include debt securities, such as bonds; equities, such as stocks; mutual funds and exchange-traded funds that invest in, among other things, bonds and stocks; and derivatives, such as options and futures. At the federal level, SEC and CFTC provide financial regulation for certain investment products. The self-regulatory organizations—FINRA and NFA—have responsibilities, along with SEC and CFTC, in this regulation.
- **Risk transfer products.** Financial institutions also provide risk transfer products, including transfer of financial loss due to theft, destruction of property, cyber incidents, or loss of income, to ensure the sustainability of businesses and economic vitality when an adverse event occurs. The U.S. market for financial risk transfer products is among the largest in the world, measuring in the trillions of dollars.

The Financial Services Sector Uses Third-Party Vendors and Financial Technologies to Provide Services

The composition of the financial services sector extends beyond the categories of financial services to include a network of essential specialized service organizations and service providers that support the sector in its efforts to provide a trusted services environment. For

[8]The automated clearinghouse (ACH) network is the primary payment system that entities use for electronic funds transfer. ACH networks have traditionally been used to facilitate automatic bill paying to utilities or other merchants or funds transfers between banks. See https://www.nacha.org/content/history-nacha-and-ach-network for more details.

example, the financial services sector has become more dependent on outsourcing certain activities—such as systems and applications, hardware and software, and technically skilled personnel—to third-party providers that are now an indispensable part of the sector's infrastructure.[9] Currently, most of the sector's key services are provided through the use of information and communications technology, increasing further the importance of cybersecurity to the sector.[10]

In addition, consumer applications, known as "fintech," enable increased use of financial systems and data beyond the traditional boundaries of the sector. For example, digital wealth management platforms use algorithms based on consumers' data and risk preferences to provide digital services, including investment and financial advice, directly to consumers.

Further, mobile payment applications allow consumers to use their smartphones or other mobile devices to make purchases and transfer money instead of relying on the physical use of cash, checks, or credit and debit cards. Due in part to the introduction of these new technologies, the financial services sector has even stronger need for information technology capabilities and support from supply chain partners and third-party service providers.

Overview of Financial Regulators

While the missions of individual regulators differ, federal financial regulators are generally responsible for monitoring the safety and soundness of institutions, ensuring adequate consumer and investor protections and the integrity and fairness of markets, and acting to ensure the stability of the overall financial system. Several regulatory agencies oversee various aspects of the financial services industry. Table 1 identifies the primary regulators for the financial services industry.

[9]GAO, *Critical Infrastructure Protection: Efforts of the Financial Services Sector to Address Cyber Threats*, GAO-03-173 (Washington, D.C.: Jan. 30, 2003).

[10]The term ''information and communications technology'' means any hardware, software, or other product or service primarily intended to fulfill or enable the function of information processing and communication by electronic means, including transmission and display, including via the Internet.

Table 1: Primary Federal Regulators for the Financial Services Industry

Regulatory agency	Selected financial service entities for which the agency has primary supervisory or oversight responsibility
Commodity Futures Trading Commission (CFTC)—an independent federal agency	Derivatives markets Central counterparties and swap data repositories Sale of commodity and financial futures, swaps, and options Intermediaries, such as futures commission merchants (FCMs) Self-regulatory organizations
Federal Deposit Insurance Corporation (FDIC)—an independent agency	State-chartered banks that are not members of the Federal Reserve System Federally insured state savings banks Certain technology service providers that are considered bank service companies under the Bank Service Company Act
Board of Governors of the Federal Reserve System (FRB)—an independent agency	State-chartered banks that are members of the Federal Reserve System and member banks' foreign branches and subsidiaries Bank holding companies and their nonbank subsidiaries Savings and loan holding companies U.S. operations of foreign banking organizations Payment systems Reserve Bank services to depository institutions and to the U.S. Treasury Certain financial market utilities that are designated as systemically important under Title VIII of the Dodd-Frank Act, or that are considered bank service companies under the Bank Service Company Act
National Credit Union Administration (NCUA)—an independent agency	Federally chartered credit unions Federally insured, state-chartered credit unions Corporate credit unions
Office of the Comptroller of the Currency (OCC)—a bureau within Treasury	Nationally chartered banks, federal savings associations, and federal branches and agencies of foreign banks ***Certain technology service companies that are considered bank service companies under the Bank Service Company Act***
Securities and Exchange Commission (SEC)—an independent federal agency	Broker-dealers Financial Industry Regulatory Authority Investment advisers Investment companies Municipal Securities Rulemaking Board Securities exchanges Securities clearing agencies Self-regulatory organizations

Source: GAO analysis based on GAO-03-173 and data from the above financial services regulators. | GAO-20-631

Two of the federal regulators above are aided by self-regulatory organizations. Self-regulatory organizations are non-government

organizations that have responsibilities that include assisting regulators in conducting examinations. Specifically,

- The Financial Industry Regulatory Authority (FINRA) works under the supervision of the SEC. Among other things, it writes rules to govern securities broker-dealers and their representatives, and examines and enforces broker-dealer compliance with FINRA rules and federal securities laws. FINRA also currently provides regulatory services to other self-regulatory organizations—specifically, U.S. equities and options exchanges.
- The National Futures Association (NFA) is the self-regulatory organization for the U.S. derivatives industry. It is responsible for regulating member firms that conduct derivative business as a futures commission merchant, introducing broker, commodity pool operator, commodity trading advisor, retail foreign exchange dealer, swap dealer, or major swap participant. CFTC relies on NFA to establish and enforce rules governing the behavior of its members.

Each federal financial regulator is generally required to conduct a full-scope, on-site examination of federally insured depository institutions under its jurisdiction at least once during each 12- to 18-month period.[11]

Federal Policies Established Requirements for Critical Infrastructure Entities

Safeguarding systems that support critical infrastructures has been a long-standing concern for industry and government. In 2003, we expanded our federal information security high-risk area to include the protection of critical cyber infrastructure. At that time, we highlighted the need to manage critical infrastructure protection activities that enhance the security of the cyber public and private infrastructures essential to national security, national economic security, and/or national public health and safety. Our most recent high-risk report identified specific actions needed to address cybersecurity challenges facing the nation—including ensuring the security of emerging technologies, enhancing the federal

[11]NCUA requires examinations at least once every 12 months for most credit unions, and performs examinations on low risk credit unions every 14 to 20 months. While the examination cycle for federally insured, state-chartered credit unions by NCUA is longer, state regulators also conduct examinations that are monitored by NCUA.

response to cyber incidents, and improving implementation of governmentwide cybersecurity initiatives.[12]

Over the years, a variety of federal policies have focused attention on addressing issues related to enhancing the security of critical infrastructure sectors, including financial services. These policies also encouraged information sharing—in particular, the creation of mechanisms for gathering, analyzing, and appropriately sanitizing and disseminating information to and from infrastructure sectors and the federal government. Several of the policies issued since 2013 underpin federal and industry efforts to secure the sector.

Executive Order 13636 Called for Federal-Private Partnerships

In February 2013, the White House issued *Improving Critical Infrastructure Cybersecurity*, Executive Order 13636 (EO 13636).[13] This order stated that the cyber threat to critical infrastructure continues to grow and represents one of the United States' most serious national security challenges.

The order called for a partnership with the owners and operators of critical infrastructure to improve cybersecurity-related information sharing. To do so, it promoted engagement between a number of federal and private organizations, including government coordinating councils that include federal agencies with responsibilities related to critical infrastructure protection; sector coordinating councils that include private sector entities with roles in protecting a critical infrastructure sector, such as the Financial Services Sector Coordinating Council (FSSCC); critical infrastructure owners and operators; federal sector-specific agencies, such as Treasury for the financial services sector; and other relevant agencies, such as regulatory agencies.

The executive order also required the periodic evaluation of the critical infrastructure systems at greatest risk. Specifically, the executive order directed DHS, with help from the sector-specific agencies, to annually identify and update a list of critical infrastructure for which a cybersecurity incident could reasonably result in catastrophic effects on public health or safety, economic security, or national security.

[12]GAO-18-622.

[13]Exec. Order No. 13636, 78 Fed. Reg. 11,739 (Feb. 19, 2013).

Presidential Policy Directive 21 Established Agency Responsibilities

Also in February 2013, the White House issued *Critical Infrastructure Security and Resilience*, Presidential Policy Directive 21 (PPD-21), to further specify critical infrastructure responsibilities.[14] PPD-21 established three strategic imperatives to strengthen critical infrastructure security and resilience: to (1) refine and clarify functional relationships across the federal government; (2) enable effective information exchange by identifying baseline data and systems requirements; and (3) implement an integration and analysis function to inform planning and operations decisions regarding critical infrastructure.

In addition, PPD-21 identified lead federal agencies, referred to as sector-specific agencies (SSAs), for each identified critical infrastructure sector. Among other things, SSAs are required to (1) coordinate with DHS and collaborate with critical infrastructure owners and operators, regulatory agencies, and others; (2) serve as a day-to-day federal interface for the prioritization and coordination of sector-specific activities; and (3) provide or facilitate technical assistance for each sector to identify vulnerabilities and help mitigate incidents. PPD-21 designated Treasury as the sector-specific agency for the financial services sector.

PPD-21 also created roles and responsibilities for DHS, the overall lead federal agency for national critical infrastructure policy, and for sector-specific agencies. PPD-21 required DHS and the SSAs to develop a description of functional relationships across the federal government related to critical infrastructure security and resilience; conduct an analysis and recommend options for improving public-private partnership effectiveness; and provide an implementation plan, including the identification of a risk management framework to strengthen the security and resilience of critical infrastructure.

National Policies Define Federal Agency Responsibilities for Supporting Cyber Infrastructure

In response to the PPD-21 requirement to create a critical infrastructure implementation plan, DHS, with the help of private industry and federal

[14]The White House, *Critical Infrastructure Security and Resilience*, Presidential Policy Directive 21 (Washington, D.C.: Feb. 12, 2013).

agencies within designated sectors, created a new version of the *National Infrastructure Protection Plan* (NIPP) later in 2013.[15] The NIPP, intended as a national guide for the management of risks to critical infrastructure, breaks down the policy requirements in EO 13636 and PPD-21 into risk management-related goals and objectives. The NIPP highlights three broad activity areas to guide collaborative efforts of the critical infrastructure community: building upon partnership efforts; innovating in managing risk; and focusing on outcomes.

The NIPP also reaffirms sector council structures from earlier policies—in particular, sector coordinating councils (SCCs) and government coordinating councils (GCCs). SCCs are self-run private sector councils, which serve as principal collaboration points between the government and private sector owners and operators for critical infrastructure security and resilience policy coordination and planning. GCCs enable inter-agency, intergovernmental, and cross-jurisdictional coordination within and across sectors, and partner with SCCs on public-private efforts. Together, SCCs and GCCs are intended to be mechanisms that enhance information sharing in critical infrastructure sectors.

According to the NIPP, the critical infrastructure community should work jointly to set specific national priorities. In turn, the national priorities should be supplemented by various sector activities. In addition, the national priorities are to be supported by objectives and priorities developed at the sector level. The NIPP states that sector objectives and priorities may be articulated in sector-specific plans, which are to serve as targets for collaborative planning between SSAs and their sector partners.

The *National Cyber Strategy*, issued in September 2018, describes actions that federal agencies are to take to protect the United States from cyber threats.[16] Among other things, the *National Cyber Strategy* includes a series of priority actions to secure the nation's critical infrastructure and manage its cybersecurity risk. In June 2019, the National Security Council (NSC) developed an accompanying implementation plan to further detail the activities and associated responsibilities of federal entities that are directed to accomplish the goals established in the *National Cyber*

[15]Department of Homeland Security, *National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience* (Washington, D.C.: December 2013).

[16]The White House, *National Cyber Strategy of the United States of America* (Washington, D.C.: Sept. 2018).

Strategy.[17] The implementation plan is not a publicly available document, but is available to the federal agencies with responsibilities under the plan.

Federal Agencies' Cyber Risk Mitigation Responsibilities within the Financial Services Sector Vary Based on Role

PPD-21 designated Treasury to be the SSA for the financial services sector. In this role, Treasury is to coordinate the partnership between private sector firms and the federal government. In addition, Treasury is to coordinate with DHS, federal financial regulators, and other regulators to improve the reliability and security of U.S. financial systems; serve as a day-to-day interface for prioritization and coordination of sector activities; carry out incident management responsibilities; and provide technical assistance and consultations to identify vulnerabilities and help mitigate incidents.

Federal policies call for federal regulators to support Treasury in enhancing the security of the financial services sector. This support includes, among other things, facilitating information exchange with the private sector, promoting interactions through public-private partnerships, participating in councils and resilience initiatives, and contributing to policymaking and oversight of the sector.

DHS is responsible for conducting overall federal efforts to promote the security and resilience of the nation's critical infrastructure sectors, including the financial services sector. In its role as the nationwide critical infrastructure protection coordinator, DHS is to support Treasury and federal regulators by providing analysis, expertise, and technical assistance to critical infrastructure owners and operators, and conducting vulnerability assessments, among other things.

Financial Industry Groups Assist Sector Members in Collaborating to Mitigate Cyber Risks

The financial services sector includes several groups aimed at helping entities within the sector to collaborate in mitigating their cyber risks.

[17]National Security Council, *National Cyber Strategy Implementation Plan* (Washington, D.C.: June 2019).

Among these are two sectorwide groups created specifically to assist members of the sector:

- The Financial Services Sector Coordinating Council (FSSCC) is the designated coordinating council for the financial sector. As the sector coordinating council, FSSCC is to fulfill specific functions established in the NIPP. Specifically, it is to operate as a principal collaboration point between the government and private sector owners/operators on policy coordination and planning, and participate in efforts to establish voluntary practices in order to gain sector perspectives.

  According to an FSSCC official, the mission of the FSSCC is to strengthen the resilience of the financial services sector against attacks and other threats to the nation's critical infrastructure by proactively identifying threats and promoting protection, driving preparedness, collaborating with the federal government, and coordinating crisis response. FSSCC and its member organizations promote the resilience of the sector through information sharing and incident response and recovery efforts, and by promoting best practices and the development of effective policies, among other activities. It also has assisted in creating several versions of the financial services sector's sector-specific plan. The latest version of the sector-specific plan was created in partnership with Treasury and DHS.[18]

  As of June 2020, over 70 sector associations and financial institutions that represent major subsectors of the industry made up the FSSCC. Members include trade groups such as the American Bankers Association (ABA), the Bank Policy Institute (BPI), the Securities Industry and Financial Markets Association (SIFMA), and the Independent Community Bankers of America (ICBA), which are discussed later in this report. Another trade group with membership in FSSCC is the Credit Union National Association, which, according to a CUNA official, advocates on behalf of approximately 115 million consumer members and is the largest national trade association representing credit unions.

- The Financial Services Information Sharing and Analysis Center (FS-ISAC) serves as the operational arm of the FSSCC. The mission of FS-ISAC is to assist in ensuring the resilience and continuity of firms and financial services against intentional acts,

[18]Departments of Homeland Security and Treasury, *Financial Services Sector-Specific Plan 2015.*

including cyberattacks, which could significantly impact the sector's ability to provide critical services.

FS-ISAC is made up of close to 7,000 member financial institutions and more than 15,000 users in more than 70 countries. According to FS-ISAC officials, the organization considers financial institutions to be those that have a fiduciary or regulatory obligation to protect the public's transactions, assets, or personally identifiable information in the financial space. Its members include banks, brokerages, credit unions, trade associations, insurance companies, investment firms, service providers, and payment processors. Together, the member financial institutions maintain a majority of assets under control by the financial services industry.

Among other things, FS-ISAC focuses on improving information sharing, coordination between members, and crisis response. FS-ISAC also distributes recommendations for protective measures and practices to thousands of institutions, and advocates a common standard for data sharing across the sector.

In addition, the Financial Systemic Analysis and Resilience Center (FSARC) was formed within the FS-ISAC in 2016 by eight private firms with major critical infrastructure responsibilities. Shortly after founding, FSARC added another eight members. FSARC's mission is to improve the resiliency of the critical functions that underpin the U.S. financial sector and to develop intelligence to protect and defend them. Compared to FS-ISAC, FSARC members share more detailed risk information in an attempt to mitigate systemic risks to the entire financial sector.

In addition, industry organizations that represent the interests of their member firms contribute to efforts to improve the cybersecurity and resilience of the sector. Federal agencies identified the American Bankers' Association (ABA), the Bank Policy Institute (BPI), the Independent Community Bankers of America (ICBA), and Securities Industry and Financial Markets Association (SIFMA) as central to the sector's efforts to mitigate cyber risks.

- ABA is a trade association that represents small, regional, and large banks. According to an ABA official, the organizations it represents employ more than 2 million people and safeguard nearly $14 trillion in deposits. ABA works to promote leading industry practices in security and risk management through bank employee training, consumer education, and policy advocacy.

ABA administers discussion groups that address best practices on emerging issues, and plays a role in financial sector cybersecurity initiatives such as use of the Financial Sector Cybersecurity Profile, a scalable cybersecurity assessment used sectorwide, as well as other sectorwide initiatives for data protection and identity verification.

- BPI is an association of about 40 member firms including national and regional banks and major foreign banks doing business in the United States, including investment banks, holding companies, and those offering financial services such as credit cards.[19] Its four main focus areas are: producing technology standards, creating policy and strategy positions regarding cybersecurity and new financial-based technologies; conducting outreach to industry CEOs brainstorming government responses to key issues, such as moving legacy systems to the cloud; and working to ensure better communication between agencies on fraud mitigation efforts.

According to its Managing Director, in 2020, the Cyber Risk Institute was created as a subsidiary of BPI to maintain and update the Financial Sector Cybersecurity Profile. The Cyber Risk Institute is a not-for-profit coalition of institutions and trade associations. It has over 30 members throughout the financial industry, which have specific cybersecurity responsibilities for the sector.

- ICBA is a national trade association dedicated to serving the interests of community banks. According to an ICBA official, it advocates for the development of national standards in cybersecurity and data privacy, and works to ensure community banks have the information they need to mitigate cybersecurity threats and fraud, including through guidance and best practices, informational events, and classroom and online training. The official also stated that ICBA works with its governmental and regulatory partners, along with its member banks, to share information, strategies, and operational risk intelligence.
- SIFMA is a trade association for broker-dealers, investment banks, and asset managers operating in both the U.S. and global capital markets. It serves as an industry coordinating body to promote fair and orderly markets, informed regulatory compliance, and efficient market operations and resiliency. Its cybersecurity-

[19]BPI was formed by the merger of the Financial Services Roundtable and the Clearing House Association to specialize in cybersecurity concerns.

related roles include coordinating crisis management for the financial sector, providing subject matter expertise across worldwide financial markets, leading simulated cyberattack-related tests of the sector at regular intervals, and developing controls and consensus to protect against insider threats. In addition, SIFMA has led a number of efforts related to promulgating cybersecurity best practices and guidance for its members.

Previous GAO Reports Recommended Actions to Improve Collaboration and Develop Metrics in the Financial Services Sector

We have previously reported on steps taken by critical infrastructure sectors in general, and the financial sector in particular, to address cybersecurity risks.[20]

- In December 2011, we reported on the guidance available to the seven critical infrastructure sectors, including the financial services sector, and the extent to which implementation of this guidance was enforced and promoted.[21] We noted that there was a large volume and wide variety of guidance for each sector, but that sector-specific agencies had not identified the key cybersecurity guidance applicable to, or widely used in each sector, and could have taken additional steps to promote such guidance. Most sector-specific critical infrastructure protection plans did not identify the key guidance and standards for cybersecurity because doing so was not outlined in DHS guidance.

  We recommended that DHS, in collaboration with both private and public sector partners, determine whether it is appropriate to have cybersecurity guidance listed in individual sector plans. DHS agreed with this recommendation and took steps to implement it. In particular, DHS issued guidance for critical infrastructure sectors to update their sector-specific plans to explain how sector efforts align with the

[20]In addition to the other reports referenced in this section, see GAO, *Critical Infrastructure Protection: Efforts of the Financial Services Sector to Address Cyber Threats*, GAO-03-173 (Washington, D.C.: Jan. 30, 2003).

[21]GAO, *Critical Infrastructure Protection: Cybersecurity Guidance Is Available, but More Can Be Done to Promote Its Use*, GAO-12-92 (Washington, D.C.: Dec. 9, 2011).

National Institute of Standards and Technology's *Framework for Improving Critical Infrastructure Cybersecurity*.[22]

- In November 2015, we reported on how federal agencies that were designated as sector-specific agencies measured cybersecurity progress.[23] Specifically, we examined the extent to which SSAs identified the significance of cyber risks to their respective sectors' networks and industrial control systems, took actions to mitigate cyber risks, collaborated across sectors to improve cybersecurity, and established performance metrics to monitor improvements in their respective sectors.

  With respect to the financial services sector, we pointed out that Treasury had determined that cyber risk was significant and had taken actions to mitigate cyber risks in alignment with the NIPP. However, Treasury had not developed metrics to measure and report on the effectiveness of all of its cyber risk mitigation activities or the financial sectors' cybersecurity posture. This was because, among other reasons, Treasury relied on private sector partners to voluntarily share information needed to measure efforts.

  We recommended that Treasury develop performance metrics and determine how to overcome challenges to monitoring the financial services sector's cybersecurity progress. Treasury did not agree or disagree with this recommendation. Treasury stated that it continued to take steps designed to enhance the cybersecurity of the financial sector. As of February 2020, Treasury had not implemented this recommendation and we continue to monitor its efforts.

- In February 2018, we reported on the extent to which each of the 16 federal critical infrastructure sectors had adopted the NIST cybersecurity framework. We noted that, while most sectors had developed guidance for implementing the framework, none of the sectors had reported having qualitative or quantitative measures of framework adoption. In particular, Treasury officials stated that they had not captured data on framework adoption rates for the financial services sector.

[22]National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* (Gaithersburg, MD: Apr. 16, 2018).

[23]GAO, *Critical Infrastructure Protection: Sector-Specific Agencies Need to Better Measure Cybersecurity Progress*, GAO-16-79 (Washington, D.C.: Nov. 19, 2015).

We recommended that Treasury take steps to consult with respective sector partners to develop methods for determining the level and type of framework adoption by entities across their respective sector. Treasury did not agree or disagree with this recommendation, stating that it did not have the authority to compel entities to share cybersecurity framework adoption data. The department stated that it would continue to engage and consult with sector partners to develop methods for determining the level of framework adoption.[24]

The Financial Services Sector Faces a Variety of Cybersecurity-related Risks

The financial services sector faces significant risks due to its reliance on sophisticated technologies and information systems, as well as the potential monetary gain and economic disruption that can occur by attacking the sector. A successful widespread cyberattack could erode public confidence in financial institutions, deny businesses and individuals access to their funds, result in the loss of funds, or affect the integrity of financial information. Table 2 shows what the private-sector firms and federal agencies included in our review consider to be the primary cyber-related risks to the sector.

Table 2: Primary Cyber Risks Identified by Financial Sector Firms and Federal Agencies

Risks	Details
Social Engineering[a]	The financial services sector is at risk due to social engineering attacks, which include a broad range of malicious activities accomplished through human interaction that enable attackers to gain access to sensitive data by convincing a legitimate, authorized user to give them their credentials and/or other personal information. For example, a common social engineering exploit method is phishing, which occurs frequently through email. In phishing, an attacker is disguised as a trusted individual and tricks the target into revealing sensitive data or clicking a link that exploits a vulnerability or introduces malware into the network.

[24]GAO, *Critical Infrastructure Protection: Additional Actions are Essential for Assessing Cybersecurity Framework Adoption,* GAO-18-211 (Washington, D.C.: Feb. 15, 2018).

Risks	Details
Malware[b]	The risk of malware exploits impacting the sector has increased as malware exploits have grown in sophistication. Often, the goal of malware is to infiltrate a network at a vulnerable point and then gain access to key assets through lateral network movement.[c] Common exploits seen in malware attacks on the financial sector include • Trojan horse attack, where software misrepresents itself to be useful; • Watering hole attack, in which a particular organization is targeted through websites regularly visited by employees. • Distributed denial of service (DDoS) attacks, in which a network of compromised computer systems attack a target, such as a server, website, or other network resource, and cause a denial of service for users of the targeted resource. • Ransomware, which blocks access to the victim's data and threatens to publish or delete it unless a sum of money is paid.
Third-Party Access	Increased connectivity with third-party providers and the potential for increased cyber risk is a concern in the financial industry as core systems and critical data are moved offsite to third parties. Cyber risks affecting a depository institution can arise from weaknesses in practices of technology service providers, and attacks on third-party connections can lead to a data breach. For example, consumer services and mobile applications that offer personal financial management are likely to be a target for credential theft, especially if they have lower defenses compared to major retail banks. Also, because many third-party service providers service numerous banks and credit unions, a failure of one provider can pose systemic risk issues.
Insider Threats	Risks due to insider threats involve careless, poorly trained, or disgruntled employees or contractors hired by an organization who may intentionally or inadvertently introduce vulnerabilities or malware into information systems. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a target system often allows them to gain unrestricted access to cause damage to the system or to steal system data. Results of insider threats can include data destruction and account compromise.
Interconnectivity	Interconnectivity involves interdependencies throughout the financial services sector and the sharing of data and information via networks, the cloud, and mobile applications. Organizations in the financial services sector utilize data aggregation hubs and cloud service providers, and new financial technologies such as algorithms based on consumers' data and risk preferences to provide digital services for investment and financial advice.

Source: GAO analysis of data from federal agencies, and private sector firms and organizations. | GAO-20-631

[a]Social engineering is the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes. Social engineering is the art of manipulating people into performing actions or divulging sensitive information.

[b]Malware is defined as software designed to carry out annoying or harmful actions.

[c]Lateral movement is the movement attackers make to harvest credentials from compromised machines through accessing domain controllers and card processing segments after establishing a foothold in the victim.

According to officials from several government and private sector entities, several cyber-related risk categories common to the financial sector, such as the use of social engineering and types of malware, are similar to those faced by other critical infrastructure sectors and throughout the federal government. A 2019 white paper issued by staff at the Federal Reserve Bank of Richmond also stated that a number of factors contribute to cyber risk at financial institutions, including: (1) the use and

early adoption of quickly evolving technology and (2) the intrinsic nature of financial institutions' businesses and services.[25]

Various financial sector-focused reports also highlighted primary threat actors. Specifically, according to two private sector reports that we analyzed, there have been significant attacks conducted by advanced persistent threat groups on the financial services sector. These resource-rich groups take direction from a nation state to steal information, disrupt operations, or destroy infrastructure.

Advanced persistent threat attackers pursue their objectives over months or years by adapting to cyber defenses and frequently targeting the same victim.[26] According to one private sector report, advanced persistent threat groups are also more likely to attack financial targets by exploiting the increased level of trust and reliance on new technology in banking infrastructure.

Cyberattacks that exploit risks can occur against either public or private components of the financial services sector. Examples of recent incidents demonstrate the impact of such attacks:

- In January 2019, the SEC announced charges against nine individuals for participating in a scheme to hack into the SEC's Electronic Data Gathering, Analysis and Retrieval (EDGAR) system and extract nonpublic information to use for illegal trading. The SEC alleged that the hacking started in at least May 2016 and continued through at least October 2016, and that efforts to compromise EDGAR continued into early 2017. The Department of Justice announced related criminal charges against two hackers.[27]

[25]Filippo Curti, Jeffrey Gerlach, Sophia Kazinnik, Michael Lee and Atanas Mihov, *Cyber Risk Definition and Classification for Financial Risk Management,* (Washington, D.C.: August 26, 2019).

The views expressed in this white paper are solely those of the authors. They do not necessarily reflect the views of the Federal Reserve Bank of Richmond, the Federal Reserve Bank of New York, or the Federal Reserve System.

[26]According to NIST, an advanced persistent threat can be an adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors, such as cyber, physical, and deception.

[27]GAO, *Cybersecurity: Agencies Need to Fully Establish Risk Management Programs and Address Challenges,* GAO-19-384 (Washington, D.C.: July 25, 2019).

- From May to July 2017, the breach of an Equifax online dispute portal resulted in the compromise of personal information of more than 145 million U.S. consumers, including the credit card number for approximately 209,000 customers.[28]
- In February 2016, a series of cyberattacks[29] on the Bank of Bangladesh resulted in the theft of approximately $81 million. Hackers accessed the Bangladesh Central Bank's systems that interfaced with the Society for Worldwide Interbank Financial Telecommunication (SWIFT) with malware through use of spear phishing[30] e-mails, which directed the Federal Reserve Bank of New York to transfer money to accounts in other Asian countries.[31]
- U.S. depository institutions and their customers have experienced losses through attacks known as account takeovers.[32] For example, in February 2015, FBI and the Department of State announced a $3 million reward for information leading to the arrest of a Russian accused of executing account takeovers that stole more than $100 million from American bank accounts.[33]
- A major U.S. depository institution suffered a data breach during the summer of 2014. According to public statements made by the

[28]See GAO, *Data Protection: Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach,* GAO-18-559 (Washington, D.C.: August 30, 2018) for more details on this breach. Companies that assemble consumer credit information and sell this information are referred to as "consumer reporting agencies". See 15 U.S.C. §1681a(f). These companies can also be referred to as a "credit bureau," "credit reporting company," or a "credit reporting agency." Equifax is one of the nation's largest consumer reporting agencies.

[29]Cyberattacks refer to techniques performed by cyber threat actors that adversely affect computers, software, a network, an industry, or the Internet itself.

[30]Spear phishing is a phishing exploit that is targeted to a specific individual or group.

[31]Department of Justice, *North Korean Regime-Backed Programmer Charged with Conspiracy to Conduct Multiple Cyberattacks and Intrusions* (Washington, D.C.: September 6, 2018) and Congressional Research Service, *North Korean Cyber Capabilities: In Brief* (Washington, D.C.: August 3, 2017).

[32]In account takeovers, criminals target victims, causing them to unknowingly install malicious software on their computers. When the victim next logs on to their banking website, the new software transmits data back to the criminals, who then use the victim's credentials to transfer funds from the victim's account. See GAO-15-509.

[33]GAO, *Cybersecurity: Bank and Other Depository Regulators Need Better Data Analytics and Depository Institutions Want More Usable Threat Information,* GAO-15-509 (Washington, D.C.: July 2, 2015).

institution, the breach compromised some account information for 83 million households and small businesses.[34]

The Financial Services Industry Is Taking Multiple Steps to Enhance Sector Security and Resilience

Firms and sectorwide groups within the financial services sector are taking steps to enhance the cybersecurity and resilience of the entire sector through a broad range of risk mitigation efforts. These efforts largely fall into the following five categories:

- **Coordination between organizations.** Many entities, including seven private sector firms, identified their involvement with industry groups such as FSSCC and FSARC as providing important sources of information on best practices, and facilitating sectorwide coordination. For example, one firm described using FSSCC and FSARC as conduits for interactions with Treasury, and as sources to enable sharing and receiving of information on key sector issues.
- **Sectorwide incident response exercises.** For example, FS-ISAC has been a co-leader with federal entities, including Treasury, and other private entities on 30 cyberattack simulation exercises that have been conducted over the past 5 years to help financial entities discover gaps in capabilities and policies, or to identify weaknesses. An ABA official stated that it has offered similar exercises, such as a one-day, hands-on-keyboard exercise in which participants observe and respond to different types of attacks. ABA also has encouraged participation in sectorwide exercises sponsored by Treasury and DHS. According to an ICBA official, it participates in several exercises each year, and disseminates after-action reports and lessons learned to community banks to aid in their preparation against cyberattacks.
- **Guidance to sector industry.** Guidance provided by sectorwide groups includes the Financial Sector Cybersecurity Profile, which an FSSCC working group developed based on the NIST cybersecurity

[34]Securities and Exchange Commission, *Current Report (Form 8-K) JPMorgan Chase & Co.* (Washington, D.C.: Oct. 2, 2014).

framework.[35] The profile is a scalable assessment that firms can use as both a risk management assessment, and as an indicator for compliance with regulatory frameworks. According to an official at the Cyber Risk Institute, which maintains and updates the profile, its creation was a collaborative effort between more than 300 financial firms, regulatory agencies, and experts to create a harmonized approach to cybersecurity assessments. The official also stated that the profile will continue to evolve based on regulations and cybersecurity standards.

Several sector members have mentioned the profile as a key risk mitigation effort and, according to an official affiliated with FSSCC, at least 100 members have begun to use it. In support of the profile, ABA manages two groups to facilitate its adoption and implementation. One group is made up of community and midsize banks, and the other includes larger banks and securities firms. Firms we spoke with noted the importance of the profile and several stated that they had incorporated it in their internal cybersecurity framework.

- **Sharing of risk and threat information.** Five private-sector firms noted information they obtained from sectorwide organizations such as the FS-ISAC was important to their understanding of the threat environment. For example, FS-ISAC instituted a traffic light protocol with color coding so that potential sharers can more easily indicate appropriate boundaries for sharing the information. ICBA also collects information from several sectorwide sources and provides it to community banks using a single login location for greater ease of access.
- **Training for sector members.** For example, ABA and ICBA have installed cyber risk training programs for their members. ABA provides its training through sources such as webinars, workbooks, presentations, and white papers, as well as a cyber-compliance program for conference attendees. An ABA official stated that it also maintains several cyber and operational security working groups which that meet regularly to share information about threat trends and resources. ICBA's education division also provides several weeklong

[35]National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* (Gaithersburg, MD: Feb. 12, 2014). The NIST framework is a voluntary, consensus-based framework that comprises industry standards and best practices to help organizations manage cybersecurity risks. It provides private sector organizations with principles and best practices of risk management to improve the security and resilience of their critical infrastructures. Version 1.1 of the framework was issued April 16, 2018.

training sessions and webinars, on topics such as the mitigation of cyber risk and protection against emerging threats.

In addition to the five primary categories of efforts mentioned, some individual firms discussed specific efforts that they were taking, such as monitoring existing systems for vulnerabilities and reviewing and monitoring their relationships with third-party vendors. For example, officials at eight firms stated that they performed ongoing vulnerability management efforts such as monitoring their systems and conducting penetration testing, where evaluators mimic real-world attacks in an attempt to identify ways to circumvent the security features of the system. Officials at five firms stated that they performed risk assessments and continuous monitoring of their third-party vendors.[36] According to officials at sectorwide groups, their organizations plan to take continuing action to further address cyber threats.

While sectorwide groups and firms have many cyber risk mitigation efforts underway, officials at private-sector firms identified areas for which they remain in need of assistance or guidance from sector groups, such as regulators, sectorwide organizations, or policymakers, regarding current cybersecurity challenges. The firms included in our review most commonly identified the following four areas in which they needed assistance:

- improving information sharing among firms during a cybersecurity incident, including clarifying what information can be shared after a breach;
- establishing more guidance and providing clarity on the regulation of vendors and third parties;
- increasing cybersecurity training across each firm; and
- further improving harmonization among regulatory requirements. For example, four firms mentioned the difficulty of following differing state breach notification requirements, as compared to following one national requirement.

Officials from both small banks also pointed to the lack of clarity of regulations related to third-party vendors as a challenge area. They stated that additional guidance is needed, both to improve the bank's

[36]Continuous monitoring includes ongoing observation, assessment, analysis, and diagnosis of an organization's cybersecurity posture, hygiene, and operational readiness.

management of third-party vendors and to educate the vendors on the sectors' cybersecurity requirements.

Federal Agencies Take Multiple Steps to Support the Financial Services Sector's Cybersecurity and Resilience, but Progress Is Unclear

To assist the financial services sector in enhancing its cybersecurity and resilience, federal agencies with responsibility for the financial services sector perform a number of cyber risk mitigation activities. Among other things, federal agencies provide cybersecurity expertise, conduct and use the results of regulatory examinations to inform subsequent corrective efforts, and conduct simulation exercises related to cyber incident response and recovery.

According to PPD21 and the NIPP, sector-specific agencies should assist in the prioritization of sector activities, and measure the effectiveness of federal agencies' risk mitigation activities to monitor progress against national goals and priorities. While the performance of the federal agencies' activities generally fulfills responsibilities laid out in policy and Treasury plays a key role in supporting the sector's cyber risk mitigation efforts, Treasury does not prioritize, track, or measure the progress of the sector's efforts against sector goals for enhancing security and resilience. Further, based on the same criteria, we previously recommended establishing metrics to measure the progress of the risk mitigation efforts the sector is performing. However, the current financial sector-specific plan does not include such metrics.[37]

Federal Agencies Assist the Financial Services Sector in Cyber Risk Mitigation

Agencies with responsibility for the financial services sector, including designated sector leaders, Treasury and DHS, and federal financial regulators, conduct efforts aimed at improving the security and resiliency of the sector. Agencies with cybersecurity-related responsibilities coordinate their efforts primarily through two organizations—the Financial

[37]See GAO-16-79.

and Banking Information Infrastructure Committee (FBIIC) and the Federal Financial Institutions Examination Council (FFIEC).

- FBIIC was established to improve coordination and communication among financial regulators, enhance the resiliency of the financial sector, and promote public-private partnership. FBIIC is chaired by Treasury's Assistant Secretary for Financial Institutions and includes representatives from each of the primary federal financial regulatory agencies and liaisons from state regulatory agencies.[38]
- FFIEC is an interagency forum created by Congress to promote consistency in the examination and supervision of depository institutions.[39] Its efforts include enhancing the capabilities of examiners to perform information technology and cybersecurity-related reviews and raising awareness of cybersecurity-related risks to institutions and third-party service providers.

Federal agencies' cybersecurity and resiliency efforts related to the financial services sector fulfill responsibilities laid out in policy and guidance, such as PPD-21 and the NIPP.[40] The agencies' efforts largely fall into seven categories, many of which provide support to the private sector in conducting their cyber risk mitigation efforts.

- **Collaborating to encourage regular communication.** Federal and other financial regulators collaborate on risk mitigation efforts facilitated through the FBIIC and FFIEC. In this regard, FRB, FDIC, SEC, and CFTC all regularly work with several industry-based sector organizations, including the FS-ISAC, FS-SSC, and FSARC. For example, federal regulators provided input to the FSARC's risk committee, which develops and prioritizes a list of systemic risks.

  According to a Treasury official, it is also leading a range of initiatives through the President's Working Group on Financial Markets and in

[38]FBIIC consists of 18 member organizations from across the financial regulatory community, both federal and state. See Financial and Banking Information Infrastructure Committee, *FBIIC Members*, https://www.fbiic.gov/fbiic-members.html. In addition to national financial regulatory agencies, FBIIC includes a representative from a group of state bank supervisors.

[39]The FFIEC is comprised of leaders from the Board of Governors of the Federal Reserve System, Bureau of Consumer Financial Protection, FDIC, NCUA, OCC, and State Liaison Committee.

[40]The White House, *Critical Infrastructure Security and Resilience*, Presidential Policy Directive 21; and DHS, *National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience*.

cooperation with critical infrastructure entities and government partners to study primary cybersecurity vulnerabilities in the financial sector. Through these efforts, Treasury has identified vulnerabilities that could have a broad impact on the sector. In addition, several financial regulatory agencies have created a communication protocol for the regulators to coordinate during a cybersecurity related crisis. Federal regulators also conduct international collaboration efforts, which have informed domestic supervision activities and programs.

- **Providing cybersecurity expertise.** Within this area of effort, for example, the DHS Cybersecurity and Infrastructure Security Agency (CISA) provides free cyber assessment services to inform users of specific vulnerabilities. This includes cyber hygiene scans and penetration testing to enable customers to secure their network perimeter by assessing systems for known vulnerabilities and configuration errors. CISA also coordinates the remediation and disclosure of newly identified cyber vulnerabilities and provides an intrusion prevention capability to protect public and private networks against unauthorized access and exploitation.
- **Conducting and using the results of regulatory examinations to inform corrective efforts.** Federal and other financial regulators assess remediation plans and pursue follow-up enforcement of the issues uncovered in their examinations. For example, if in the course of an examination, regulators, such as SEC or FRB, determine that an entity has failed to comply, or potentially failed to comply, with federal securities laws or rules, or identifies a significant weakness in controls, regulators provide entities with a deficiency letter discussing their findings. The letter generally requests entities to respond within 30 days detailing planned or ongoing corrective actions. In some cases, depending on the severity, the regulators may follow up on these issues and any efforts at remediation during a subsequent examination. Similarly, CFTC follows up during continuous monitoring and later examinations to assess the effectiveness of the changes made to correct the deficiency. NFA also conducts compliance reviews of member firms and provides firms with a report identifying deficiencies. NFA requires firms to provide evidence of corrective actions.
- **Conducting incident response and recovery exercises.** Treasury leads a series of cybersecurity-related exercises, referred to as the Hamilton exercises, which are performed on both a sectorwide and local scale and include participation from members of the FBIIC, FSSCC, and FS-ISAC. The subject and scenario of these exercises varies based on observed need. For instance, a recent exercise was

conducted on insider threats. In addition, the President's Working Group on Financial Markets, made up of Treasury, CFTC, FRB, and SEC, can meet up to four times per year with OCC and FDIC to perform tabletop exercises regarding threats to the sector. According to officials, information gleaned from these exercises has enabled other efforts.

- **Sharing threat information.** In collaboration with other federal agencies, for example, Treasury conducts periodic briefings on cybersecurity threat intelligence to financial firms, and facilitates the availability of classified threat information to cleared members of financial firms. Treasury and the DHS Cybersecurity Infrastructure and Security Agency (CISA) also have mechanisms to provide classified information to firms outside of regularly scheduled meetings when needed. In addition, officials stated that they worked on making the sharing process easier and faster; for example, FS-ISAC and FSARC have spaces on the CISA watch floor to facilitate ongoing exchanges of information with the government. The DHS CISA Automated Indicator Sharing (AIS) and Cyber Information Sharing and Collaboration Program (CISCP) capability are further conduits for the exchange of unclassified cyber threat indicators between the federal government and the private sector.
- **Dissemination of cyber-related guidance and best practices.** Within this area of effort, for example, the FFIEC developed the Cybersecurity Assessment Tool, on behalf of its members, to help institutions identify their risks.[41] The assessment provides a repeatable and measurable process for institutions to measure their cybersecurity preparedness. This voluntary self-assessment tool incorporates cybersecurity-related principles from the FFIEC Information Technology Examination Handbook and regulatory guidance, and concepts from other industry guidance, including guidance related to the use of the NIST cybersecurity framework.[42] FRB also has worked with other central banks to develop international guidance for cybersecurity and resilience.
- **Training for sector members.** Federal entities offer cybersecurity-related training to enhance the sector's capabilities, including to examiners and to employees of regulated entities. For example, NFA

[41]Federal Financial Institutions Examination Council, *Cybersecurity Assessment Tool* (Arlington, VA: May 2017).

[42]The Federal Financial Institutions Examination Council Information Technology (IT) Examination Handbook is a set of guidance documents that can be accessed at https://ithandbook.ffiec.gov/.

regularly provides education workshops for its regulated entities, covering such topics as changes to compliance requirements and common deficiencies identified in examinations, and how to correct them. NFA also provides training to its employees on common types of attacks, such as phishing and malware.

Financial Services Sector Plan Does Not Address Tracking or Prioritization to Ensure Progress in Enhancing Security and Resilience

According to PPD-21, sector-specific agencies should continuously prioritize the day-to-day activities of the sector. In addition, the NIPP risk management framework, used as a basis for the development of sector-specific plans, recommends measuring the effectiveness of the SSAs' risk mitigation activities as a method of monitoring sector progress. GAO leading practices for collaboration similarly state that agencies should develop mechanisms to monitor and evaluate results and reinforce accountability through plans and reports.[43] The NIPP also suggests that all sectors update their sector-specific plans every 4 years based on guidance developed by DHS in collaboration with SSAs and cross-sector councils.

Treasury, along with sector partners DHS, FSSCC, and FBIIC, created the most recent financial service sector-specific plan and released it in March 2016.[44] The sector-specific plan is intended to serve as the primary strategic framework for the sector, and includes a mission, vision, goals, and priorities for implementing the goals. Its goals include discussing policy and regulatory initiatives to advance security and resilience priorities.

Treasury, as the sector-specific agency, plays a key role in efforts to enhance the cyber-related security and resiliency of the sector. For example, in addition to chairing the FBIIC, Treasury performs regular outreach to sector entities, including monthly and quarterly meetings through the FBIIC, as well as other daily and weekly outreach; conducting

[43]GAO, *Managing for Results: Key Considerations for Implementing Interagency Collaborative Mechanisms,* GAO-12-1022 (Washington, D.C.: Sept. 27, 2012) and *Results-Oriented Government: Practices That Can Help Enhance and Sustain Collaboration among Federal Agencies,* GAO-06-15 (Washington, D.C.: Oct. 21, 2005).

[44]Departments of Homeland Security and Treasury, *Financial Services Sector-Specific Plan 2015.*

sectorwide incident response exercises on specific cybersecurity topics; and the sharing of cyber best practices sectorwide. Treasury is also leading an effort in collaboration with government and critical infrastructure owners in the financial sector to identify key cyber vulnerabilities to the sector.

In addition, Treasury acts as a liaison for sector firms when a cyber issue occurs by working to respond to firms' immediate issues and interacting with federal regulators on several sectorwide efforts. In doing so, it works with financial sector companies, industry groups, and government partners to share information about cybersecurity and physical threats and vulnerabilities and to respond to and recover from significant incidents. Treasury officials also stated that it is working on a process to effectively document the cyber challenges the agency receives in an efficient way.

However, Treasury does not act as a primary interface for the tracking of financial services sector efforts. Specifically, it does not track the content or progress of ongoing sectorwide cyber risk mitigation efforts to minimize duplication or ensure results. In addition, Treasury does not assist in prioritizing sector efforts by linking them to sector goals and priorities laid out in the sector-specific plan.

Further, the sector-specific plan does not identify ways to measure sector progress against its goals and priorities. In particular, the sector-specific plan does not include explicit metrics for how to measure the progress of risk mitigation efforts in enhancing the sector's security and resilience. According to the NIPP, development of metrics is a key element to effective tracking of results. In November 2015, we recommended that Treasury, working with its partners, develop such metrics.[45] While we continue to monitor Treasury's actions, as of February 2020, Treasury had not fully implemented this recommendation.[46] Without metrics in place, Treasury does not have a basis for measuring progress.

[45]GAO-16-79.

[46]Treasury officials have stated that, in lieu of sector-specific metrics, they planned to use the NIST cybersecurity framework as a guide for implementation of the sector's cybersecurity efforts. However, in February 2018, we noted that no critical infrastructure sectors reported having qualitative or quantitative measures of framework adoption, and that Treasury did not capture data on framework adoption rates for the financial services sector. See GAO-18-211.

The financial services sector-specific plan is also out of date, having not been updated since March 2016—just beyond the 4-year cycle suggested in the NIPP. The sector has not yet completed a draft version of a new sector-specific plan. Due to the length of time since the last plan iteration, it lacks information on the sector's plans to implement efforts required by the *National Cyber Strategy* and its follow-on *National Cyber Strategy Implementation Plan*, including

- developing a long-term strategy, for use in the financial sector, on a cyber incident detection information sharing program;
- finalizing a comprehensive playbook detailing Treasury's information requirements during an operational incident and outline Treasury's engagement with partners and stakeholders; and
- prioritizing sector risk management activities using a cybersecurity risk register.

While, according to a Treasury official, Treasury and DHS have begun initial planning on these efforts, strategies for their eventual implementation and details on planned implementation steps do not exist in the sector-specific plan.

Treasury officials responsible for the department's sector-related efforts stated that greater tracking or prioritization of efforts does not take place because Treasury, as an SSA, operates within a voluntary partnership with both the private sector members of the financial services sector and the federal financial regulators. Due to these voluntary relationships, the officials viewed Treasury's role as facilitating communication and providing information and the opportunity for interactions among members of the financial services sector. Additionally, they believed that Treasury does not need to track and prioritize individual efforts, or to centrally track the sector's cyber risks. The officials also stated that the communications infrastructure that Treasury has in place and its roles in FBIIC, FSSCC, and FS-ISAC allow it to keep up with broader issues relevant to the sector as well as the status of individual initiatives.

However, while these actions are useful in ensuring that Treasury is aware of the major sector risk mitigation efforts that are underway, without tracking to determine whether progress is being made toward enhancing sectorwide security and resilience, it is more difficult to ensure that the efforts being performed are meeting the goals and priorities of the sector or are addressing remaining challenge areas, such as those identified by sector firms. Unless Treasury, as the SSA, undertakes more

widespread and detailed tracking and prioritization of efforts, based on explicit metrics that measure progress against the sector's goals and requirements, the sector will remain unable to determine whether its efforts are effective at reducing cyber risk. This, in turn, could leave the sector insufficiently prepared to deal with primary sector risks, such as insider threats and unauthorized access to sector data by third parties.

Conclusions

Increased access to financial services sector systems, combined with the potential for monetary gains and economic disruptions, poses significant information security risks to the sector's systems and to the critical operations and infrastructures they support. The financial services sector faces several different types of cyber-related risks, including ensuring adequate security for service providers traditionally considered external to the sector, an increased interconnectivity between sector entities that could result in simpler attack vectors, and the potential introduction of malware such as ransomware through social engineering techniques, such as spear phishing, or insider access. The sector has also faced an increase in attacks from well-organized attackers with significant resources.

The financial services industry, including firms and sectorwide groups set up to assist firms in ensuring the cybersecurity and resilience of the sector, have undertaken a series of risk mitigation efforts, in areas such as coordination and information sharing between organizations, development of guidance and training for members, and sectorwide incident response exercises. However, industry firms also pointed to challenge areas for assistance from regulators and policymakers. The most common of these areas were improved information sharing of actionable data after a cyber incident; improved harmonization among regulators, such as minimizing differences in use of state versus national requirements; establishing clearer guidance regarding regulation of the sector's third-party service providers; and increasing cybersecurity training to firm employees.

Federal agencies are conducting risk mitigation efforts intended to support private industry in improving cybersecurity of the financial services sector. These efforts, including regular outreach by the designated financial sector-specific agency, Treasury, generally meet responsibilities laid out in policy. However, Treasury does not prioritize or track the progress of sectorwide risk mitigation efforts, and does not

explicitly link sector efforts to the goals in the sector specific plan, which is the primary sector planning document. Furthermore, the plan is out of date and does not include information on how the sector plans to implement recently required efforts. The plan also does not identify ways to measure sector progress, such as explicit metrics for determining the progress of risk mitigation efforts to enhance the cybersecurity and resilience of the sector. Unless Treasury undertakes tracking and prioritization of efforts based on metrics that reflect sector planning documents, the sector will remain unable to determine the effectiveness of its efforts, which could leave the sector insufficiently prepared to deal with primary sector risks.

Recommendations for Executive Action

We are making two recommendations to Treasury:

Regarding financial sector cyber risk mitigation efforts, we recommend that the Secretary of the Treasury, in coordination with the Department of Homeland Security and other federal and nonfederal sector partners, track the content and progress of sectorwide cyber risk mitigation efforts, and prioritize their completion according to sector goals and priorities in the sector-specific plan. (Recommendation 1)

Regarding the financial sector-specific plan, we recommend that the Secretary of the Treasury, in coordination with the Department of Homeland Security and other federal and nonfederal sector partners, update the financial services sector-specific plan to include specific metrics for measuring the progress of risk mitigation efforts and information on how the sector's ongoing and planned risk mitigation efforts will meet sector goals and requirements, such as requirements for the financial services sector in the *National Cyber Strategy Implementation Plan*. (Recommendation 2)

Agency Comments, Third-Party Views, and Our Evaluation

We provided a draft of this report to CFTC, DHS, FDIC, FINRA, FRB, NCUA, NFA, OCC, SEC, and Treasury. In response, two of the entities—Treasury and NCUA—provided written comments on the report. In written comments that are reprinted in appendix II, Treasury stated that it

generally agreed with our two recommendations. However, the department expressed caution about its level of authority to implement them.

Specifically, in response to both of our recommendations, Treasury stated that its ability is limited to track, monitor, and to both devise and measure progress toward metrics on sector risk mitigation efforts. In particular, Treasury stated that this was because it cannot require that financial regulators or sector firms provide it with data on efforts that are underway or information on how those efforts reduce risks. The department stated that some financial services sector entities would need legal assurance that the information they share with Treasury on cyber risks and mitigation efforts will not be released in response to *Freedom of Information Act* requests. It also stated that further information requests might be seen by firms as a further layer of regulatory compliance that would undermine trust in Treasury and that, due to requirements under the *Paperwork Reduction Act*, Treasury cannot issue an information collection request to 10 or more firms without going through an approval process.

However, Treasury already performs coordination steps on cyber risk mitigation efforts throughout the financial services sector that could facilitate its ability to measure progress. For example, it led a study of cybersecurity vulnerabilities in the financial services sector, for which Treasury collaborated with regulatory, government, and critical infrastructure partners on resilience initiatives related to identified vulnerabilities. Treasury is already a participant in many sectorwide efforts that deal with risks to firms. The department also collaborates extensively with organizations such as FS-ISAC and FSSCC, which represent the interests of firms sectorwide, and were partners with Treasury in development of the most recent sector-specific plan.

As leader of the FBIIC, Treasury is well-positioned to coordinate in a similar manner with sector regulators, sectorwide organizations, and firms to develop a list of mutually agreed-upon risk mitigation efforts tied to the sector goals and priorities listed in the sector-specific plan.

Treasury, in its role as sector-specific agency, is also ideally positioned to secure voluntary agreement from these groups to provide only a focused amount of information on that set of efforts that would enable them to be tracked and prioritized against sector goals. Just as Treasury and financial sector firms tailor the level of data currently shared to avoid unnecessary disclosures or administrative burden, they could also

determine an appropriate level of information sharing for how to measure the results of efforts needed to achieve sectorwide goals.

In response to our second recommendation, Treasury further stated that the next update to the sector-specific plan should occur after DHS CISA updates the NIPP. The NIPP establishes cross-sector critical infrastructure priorities and objectives, and provides guidance on the development of the next set of sector-specific plans. While we believe that use of an updated NIPP as a source for a new sector-specific plan would be optimal, should the implementation of the new NIPP be delayed, it would still be beneficial for the financial services sector to consider interim adjustments to the current sector-specific plan to describe how specific ongoing efforts meet the goals and priorities outlined in the plan.

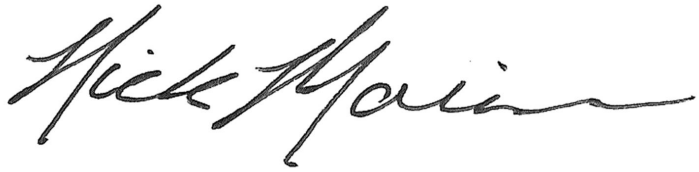
Further, NCUA provided written comments, which are reprinted in appendix III. In its comments, NCUA stated that cybersecurity is one of its top priorities and that it would continue to work closely with federal and state counterparts, as well as the Treasury, to keep the financial sector safe.

In addition to the aforementioned comments, we received technical comments from officials in DHS, FDIC, FINRA, FRB, NFA, and SEC. CFTC and OCC had no comments. We incorporated their technical comments in the report, where appropriate. We also provided report excerpts to the six sectorwide groups established to meet the cybersecurity related goals of the financial services sector. All six groups provided technical comments, which we incorporated as appropriate.

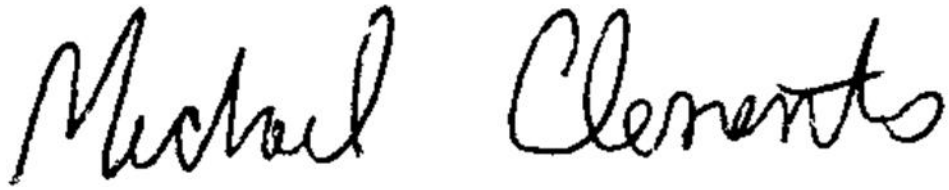
We are sending copies of this report to our Congressional addressees, the Secretaries of Homeland Security and the Treasury; the Chairmen of the Commodity Futures Trading Commission, the Federal Deposit Insurance Corporation, the Board of Governors of the Federal Reserve System, the National Credit Union Administration, and the Securities and Exchange Commission; as well as the private-sector participants in this study. In addition, the report will be available at no charge on the GAO website at http://www.gao.gov.

If you or your staff have any questions on the matters discussed in this report, please contact Nick Marinos at (202) 512-9342 or marinosn@gao.gov, or Michael Clements at (202) 512-7763 or clementsm@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report.

GAO staff who made major contributions to this report are listed in appendix II.



Nick Marinos
Director, Information Technology and Cybersecurity



Michael Clements
Director, Financial Markets and Community Investment

Congressional Addressees

The Honorable Ron Johnson
Chairman
The Honorable Gary C. Peters
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Maxine Waters
Chairwoman
Committee on Financial Services
United States House of Representatives
The Honorable Bennie G. Thompson
Chairman
Committee on Homeland Security
United States House of Representatives

The Honorable Carolyn B. Maloney
Chairwoman
Committee on Oversight and Reform
United States House of Representatives

The Honorable Cedric L. Richmond
Chairman
Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation
Committee on Homeland Security
United States House of Representatives

The Honorable Margaret Wood Hassan
United States Senate

The Honorable Jim Langevin
United States House of Representatives

Appendix I: Objectives, Scope, and Methodology

The specific objectives of our review were to (1) describe the key cyber-related risks facing the financial services sector, (2) describe steps the financial services industry is taking to share information on and address risks to its sector, and (3) assess steps that federal agencies are taking to enhance the security and resilience of the financial services sector.

To address all three objectives, we selected a subset of eight federal agencies, two self-regulatory organizations,[1] six private sector organizations, and 10 private sector firms with relevance to the financial services sector.

- Based on the agencies mentioned in federal policy documents, such as Presidential Policy Directive 21 (PPD-21),[2] pertaining to critical infrastructure protection efforts including for the financial services sector, federal regulators responsible for examining portions of the sector, and the scope and content of previous GAO reports related to the sector, we selected eight federal agencies. Two agencies were critical infrastructure protection leaders: the Departments of Homeland Security (DHS) and the Treasury (Treasury). In addition, we selected six regulators: the Commodity Futures Trading Commission (CFTC), the Federal Deposit Insurance Corporation (FDIC), the Board of Governors of the Federal Reserve System, the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Securities and Exchange Commission (SEC).
- We analyzed federal guidance, prior GAO work, and held interviews with federal regulatory officials to identify relevant self-regulatory organizations. Based on their oversight of respective regulated entities within the financial services sector, we selected two self-regulatory organizations: the Financial Industry Regulatory Authority (FINRA) and the National Futures Association (NFA).

[1]Self-regulatory organizations are independent from the government, but assist specific regulators in conducting examinations.

[2]The White House, *Critical Infrastructure Security and Resilience*, Presidential Policy Directive 21 (Washington, D.C.: Feb. 12, 2013).

- We analyzed federal and sector guidance and past GAO reports to identify sectorwide groups that were established to meet the cybersecurity related goals of the financial services sector. Based on our analysis and corroboration of responsible federal agency officials about the most active groups, we selected six groups. Two groups focus on the critical infrastructure of the sector: Financial Sector Information Sharing and Analysis Center (FS-ISAC) and the Financial Services Sector Coordinating Council (FSSCC). Four groups represent the interests of their members in the financial services industry, including efforts to mitigate cybersecurity risks: the American Bankers Association (ABA), Bank Policy Institute (BPI), Independent Community Bankers of America (ICBA), Securities Industry and Financial Markets Association (SIFMA).
- We analyzed sector firms based on the risk level of their critical infrastructure, firm size, role within the sector, and willingness to voluntarily participate in our review. When selecting financial firms, we included input provided from the sectorwide groups that we interviewed. Since private sector firms are not required to speak with GAO, we created a larger list of firms and contacted firms until we located 10 who agreed to speak with us.

  Based on our analysis and feedback from private sector groups, we selected private sector financial firms that would give us perspectives from across the sector, including banks, an exchange, and technology providers, to gain insight into their efforts to mitigate cybersecurity risks. We included large and small banks, as measured by total assets, because their operations were very different. The 10 firms were the Bank of America, Capital City Bank, Chicago Board Options Exchange, the Depository Trust & Clearing Corporation, First United Bank and Trust, Goldman Sachs, Morgan Stanley, Neocova, Paypal, and SoFi.

To accomplish the first objective, we performed a literature search to identify private-sector reports that focused on one or more specific risks to the financial sector. From this search, we identified six reports by firms with cybersecurity expertise that were completed within the last decade. We analyzed each report to determine and categorize the risks referenced in each, and the types of individuals or groups that posed threats to exploit them. For example, since phishing is a type of social engineering, we included it in the social engineering category. We ranked each risk category based on the number of times it was identified in reports we analyzed and the interviews we conducted. We placed threat actors into a separate category, to avoid double-counting in cases where

threat actors performed an action already addressed by a risk. We then corroborated and added to the list of risks through interviews with officials at each of the agencies, sectorwide groups, and private sector firms with responsibility for mitigating cybersecurity risks within their respective firm or across the financial services sector.

To accomplish the second objective, we collected documentation to understand the cyber-related risk mitigation efforts performed by the sectorwide groups that we selected. We also interviewed senior officials with responsibilities related to cybersecurity efforts, such as vice presidents, chief security officers, or those in charge of financial operations, at each of the private sector groups and firms. We used a standard set of discussion topics on cyber risk mitigation roles, coordination partners, and efforts, to get information on the cyber risk mitigation efforts they are performing.

For all private sector groups and firms, we analyzed the information provided and their interview responses regarding cyber risk mitigation efforts. Once we had a complete list of efforts from private sector organizations, we used an independent coder method to place identified efforts into a list of categories that best encapsulated the types of efforts. To perform this method, two analysts independently categorized each effort based on their professional judgement, and then the two analysts met to discuss and resolve any areas of disagreement. Based on our analysis, we then categorized the efforts by common themes, such as information sharing. For individual firms, we determined that each of their efforts fit into one of the primary categories we had created for efforts by private sector organizations. Therefore, we added the firms' efforts to the existing categories using the same independent two-coder method. Based on the interviews, we also developed a list of the most common challenge areas for which firms believed greater assistance was needed from the government.

To accomplish the third objective, we collected and analyzed documentation from each selected agency and self-regulatory organization regarding their cyber risk mitigation efforts. Similar to the steps we took with private-sector organizations, we also interviewed officials with responsibilities related to the cybersecurity of the sector, to learn about each entity's cyber risk mitigation roles, requirements, coordination partners, and efforts. Once we had developed a list of efforts from each agency, we used the same independent coder method as we had used to analyze private sector efforts, to group the efforts into a list of categories that best encapsulated the types of efforts. Each analyst

independently categorized each effort, and then the two analysts met to discuss and approve any areas of disagreement. Based on our analysis of information provided to us about their cyber risk mitigation efforts, we categorized the efforts being performed by the agencies and self-regulatory organizations by common themes, such as conducting incident response and recovery exercises.

We then compared the list of categorized efforts to a set of requirements derived from federal policy documents pertaining to the critical infrastructure of the financial services sector to determine if the efforts performed by each agency or self-regulatory organization met the applicable requirements. We determined which requirements from federal policy documents, including from Executive Order 13636 and PPD-21, were applicable to our analysis through a similar independent coder method.[3] Each coder assigned a priority level to each potential requirement, and met to discuss and agree on overall priorities. Only the highest priority requirements were used in the comparison. Once the coding was complete, two supervisors performed a detailed review on the results.

For the comparison, if any one of a particular agency's efforts met a criterion, the agency was seen overall as meeting that requirement. We gave agencies scores of either met, not met, or not applicable for requirements that clearly only pertained to a specific agency or agencies. For example, several requirements in PPD-21 pertained only to Treasury. We validated scores by using a similar coder method and reconciling any differences, as well as an in-depth supervisory review of the results.

In addition, we analyzed Treasury and DHS efforts to set up mechanisms for collaboration with private-sector entities, by comparing information in sector plans and actions taken by Treasury and DHS against leading practices for collaboration identified by GAO, to determine if the plan information and actions taken were in accordance with them. We used five of the eight leading practices based on applicability to our scope.[4]

[3]Exec. Order No. 13636, 78 Fed. Reg. 11,739 (Feb. 19, 2013) and The White House, *Critical Infrastructure Security and Resilience*, Presidential Policy Directive 21 (Washington, D.C.: Feb. 12, 2013).

[4]GAO, *Managing for Results: Key Considerations for Implementing Interagency Collaborative Mechanisms,* GAO-12-1022 (Washington, D.C.: Sept. 27, 2012) and *Results-Oriented Government: Practices That Can Help Enhance and Sustain Collaboration among Federal Agencies,* GAO-06-15 (Washington, D.C.: Oct. 21, 2005).

We conducted our work from June 2019 to September 2020 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Comments from the Department of the Treasury

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

August 31, 2020

Mr. Nick Marinos
Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G St NW
Washington, DC 20548

Dear Mr. Marinos,

Thank you for the opportunity to review the report regarding Financial Services Cybersecurity (the Report). This letter serves as the official response of the Department of the Treasury (Treasury).

We are pleased that the Report acknowledges that Treasury, as the sector-specific agency (SSA) for the financial services sector (sector), meets its responsibilities as laid out in federal policy. The Report further recognized that Treasury plays a key role in supporting the sector's cyber risk mitigation efforts. As SSA, Treasury engages in many efforts with the objective of improving and enhancing the security and resiliency of the sector including through the sharing of threat information and conducting incident response and recovery exercises. The Report also recommends that Treasury (1) track and prioritize the sector's cyber risk mitigation efforts; and (2) update the sector-specific plan to include specific metrics for measuring the progress and information on how the sector's efforts will meet sector goals and requirements.

Although Treasury generally agrees with GAO's recommendations, we caution that, in its SSA capacity, Treasury does not have authority to implement them. As we have noted in prior management responses to GAO reports on this topic, Treasury's authorities are limited. Treasury does not have authority to require regulators or private companies to provide Treasury with data. Treasury's authorities are limited to requesting that regulators and firms share information voluntarily that would allow Treasury to track and monitor sector risk mitigation efforts. Without data, Treasury is unable devise metrics and measure progress toward such metrics.

To implement these recommendations, Treasury would need access to data and information that would provide insight into the progress firms are making to mitigate cyber and operational risks within their organizations and to understand how those efforts further reduce risks across the sector. Such insight would help Treasury further prioritize our programs and initiatives with the financial regulators, through the Financial and Banking Information Infrastructure Committee (FBIIC), and with the private sector, through the Financial Services Sector Coordinating Council (FSSCC).

Currently, financial regulators are not required to share information relevant to tracking and monitoring sector risk mitigation efforts with Treasury. To implement the Report's

recommendations, Treasury needs financial regulators to share information regarding trends they are observing with respect to the cyber and operational risk management efforts within the firms and sub-sectors they supervise.

In the absence of information from the financial regulators as described above, Treasury would have to gather this information voluntarily from firms by surveying the sector. Sector stakeholders need legal assurance that the information they share with Treasury regarding their cyber and operational risks and mitigation efforts will not be released in response to a Freedom of Information Act (FOIA) request. Disclosure under FOIA could result in this information being revealed to sector peers and competitors and would also provide a roadmap for malicious actors to execute a successful attack against financial firms. The impediment to collecting information could be mitigated if Treasury was provided with a specific FOIA exemption for certain financial sector cybersecurity related information. A proposal for such an exemption was included in the President's FY2021 budget.[1]

In addition, Treasury recognizes the importance of building and maintaining trust with the sector in order to ensure maximum effectiveness within the context of the voluntary public-private partnership in which Treasury operates. Treasury is cognizant that any efforts to track and monitor the sector's progress to mitigate risk not be viewed by the sector as another layer of regulatory compliance. Any voluntary information collection conducted by Treasury will be mindful of this concern.

Finally, we note that under the Paperwork Reduction Act, Treasury cannot issue an information collection request to ten or more firms without approval from the Office of Management and Budget. The approval process can take a considerable amount of time and may affect Treasury's ability to obtain timely information from the sector to track and monitor sector risk mitigation efforts.

Regarding the second recommendation specifically, Treasury agrees that the sector-specific plan should be updated and that the plan should include metrics to measure risk mitigation efforts within the sector. However, the update to the sector-specific plan should occur after the Cybersecurity and Infrastructure Security Agency (CISA) updates the *National Infrastructure Protection Plan* (NIPP), in coordination with the sector coordinating councils (SCCs) and government coordinating councils (GCCs). Treasury believes that the NIPP needs to be updated first, as it establishes cross-sector critical infrastructure priorities and objectives to which we and the sector align. We anticipate that the NIPP update will be completed in the second quarter of

[1] "Create a Freedom of Information Act exemption for certain financial sector cybersecurity related information to increase protection of the U.S. financial services sector. This proposal would provide Treasury with an appropriately scoped Freedom of Information Act (FOIA) exemption for cybersecurity-related information, in furtherance of the Department's responsibilities to enhance the security and resilience of the financial services sector's critical infrastructure. To identify risks to financial sector critical infrastructure, Treasury relies on private-sector financial organizations to provide a range of cyber threat and vulnerability information. Firms in the sector have not been sharing such information with Treasury due to concerns that their sensitive information will be subject to public disclosure under FOIA. A narrowly-tailored FOIA exemption would enable Treasury to leverage its relationship with the sector to improve information sharing. This proposal would strengthen Treasury's ability to identify risks to financial sector critical infrastructure and enable public and private-sector action to mitigate significant risks." *See* https://home.treasury.gov/system/files/266/03.-DOSE-FY-2021-CJ.pdf.

fiscal year 2021, and that CISA will provide guidance to the SSAs and SCCs/GCCs on revising the sector-specific plans. Once that occurs, we will work with our federal and nonfederal partners within the financial services sector to revise the sector-specific plan.

Thank you again for the opportunity to review the Report. We look forward to continuing to work with your office in the future.

Sincerely,

David B. Lacquement
Deputy Assistant Secretary
Cybersecurity and Critical Infrastructure Protection
U.S. Department of the Treasury

Appendix III: Comments from the National Credit Union Administration

National Credit Union Administration
Office of the Executive Director

August 31, 2020

Michael Clements
Director, Financial Markets and Community Investment
U.S. Government Accountability Office
441 G. Street, NW
Washington, D.C. 20548

Dear Mr. Clements:

We reviewed GAO's draft report entitled "*Critical Infrastructure Protection: Treasury Needs to Improve Tracking of Financial Sector Cybersecurity Risk Mitigation Efforts*".

The report describes key cyber-related risks facing the financial sector as well as steps the financial service industry is taking to share information and address risk to the sector. It also assesses actions federal agencies are taking to enhance the security and resilience of the sector. Additional opportunities are identified to improve tracking of risk mitigation efforts and to enhance the sector specific plan.

Cybersecurity is one of the NCUA's top priorities and we will continue to work closely with federal and state counterparts as well as the U.S. Treasury to keep the financial sector safe.

Thank you for the opportunity to comment on the draft report.

Sincerely,

LARRY FAZIO Digitally signed by LARRY FAZIO Date: 2020.08.28 13:59:25 -04'00'

Larry Fazio
Executive Director

1775 Duke Street – Alexandria, VA 22314-3428 703-518-6300

Appendix IV: GAO Contacts and Staff Acknowledgments

GAO Contacts

Nick Marinos (202) 512-9342 or marinosn@gao.gov

Michael Clements (202) 512-7763 or clementsm@gao.gov

Staff Acknowledgments

In addition to the contact above, Michael W. Gilmore (Assistant Director), Shaun Byrnes (Analyst-in-Charge), Alexander Bennett, Christina Bixby, Christopher Businsky, Robert Lowthian, Catherine Maloney, Richard Sayoc, Priscilla Smith, Andrew Stavisky, and Adam Vodraska made key contributions to this report.

Appendix V: Accessible Data

Agency Comment Letters

Accessible Text for Appendix II Comments from the Department of the Treasury

Page 1

August 31, 2020

Mr. Nick Marinos

Director, Information Technology and Cybersecurity

U.S. Government Accountability Office

441 G St NW

Washington, DC 20548

Dear Mr. Marinos,

Thank you for the opportunity to review the report regarding Financial Services Cybersecurity (the Report). This letter serves as the official response of the Department of the Treasury (Treasury).

We are pleased that the Report acknowledges that Treasury, as the sector-specific agency (SSA) for the financial services sector (sector), meets its responsibilities as laid out in federal policy. The Report further recognized that Treasury plays a key role in supporting the sector's cyber risk mitigation efforts. As SSA, Treasury engages in many efforts with the objective of improving and enhancing the security and resiliency of the sector including through the sharing of threat information and conducting incident response and recovery exercises. The Report also recommends that Treasury (1) track and prioritize the sector's cyber risk mitigation efforts; and (2) update the sector-specific plan to include specific metrics for measuring the progress and information on how the sector's efforts will meet sector goals and requirements.

Although Treasury generally agrees with GAO's recommendations, we caution that, in its SSA capacity, Treasury does not have authority to implement them. As we have noted in prior management responses to GAO reports on this topic, Treasury's authorities are limited. Treasury does not have authority to require regulators or private companies to provide Treasury with data. Treasury's authorities are limited to requesting that regulators and firms share information voluntarily that would allow Treasury to track and monitor sector risk mitigation efforts. Without data, Treasury is unable devise metrics and measure progress toward such metrics.

To implement these recommendations, Treasury would need access to data and information that would provide insight into the progress firms are making to mitigate cyber and operational risks within their organizations and to understand how those efforts further reduce risks across the sector. Such insight would help Treasury further prioritize our programs and initiatives with the financial regulators, through the Financial and Banking Information Infrastructure Committee (FBIIC), and with the private sector, through the Financial Services Sector Coordinating Council (FSSCC).

Currently, financial regulators are not required to share information relevant to tracking and monitoring sector risk mitigation efforts with Treasury. To implement the Report's

Page 2

recommendations, Treasury needs financial regulators to share information regarding trends they are observing with respect to the cyber and operational risk management efforts within the firms and sub-sectors they supervise.

In the absence of information from the financial regulators as described above, Treasury would have to gather this information voluntarily from firms by surveying the sector. Sector stakeholders need legal assurance that the information they share with Treasury regarding their cyber and operational risks and mitigation efforts will not be released in response to a Freedom of Information Act (FOIA) request. Disclosure under FOIA could result in this information being revealed to sector peers and competitors and would also provide a roadmap for malicious actors to execute a successful attack against financial firms. The impediment to collecting information could be mitigated if Treasury was provided with a specific FOIA exemption for certain financial sector cybersecurity related

information. A proposal for such an exemption was included in the President's FY2021 budget.1

In addition, Treasury recognizes the importance of building and maintaining trust with the sector in order to ensure maximum effectiveness within the context of the voluntary public-private partnership in which Treasury operates. Treasury is cognizant that any efforts to track and monitor the sector's progress to mitigate risk not be viewed by the sector as another layer of regulatory compliance. Any voluntary information collection conducted by Treasury will be mindful of this concern.

Finally, we note that under the Paperwork Reduction Act, Treasury cannot issue an information collection request to ten or more firms without approval from the Office of Management and Budget. The approval process can take a considerable amount of time and may affect Treasury's ability to obtain timely information from the sector to track and monitor sector risk mitigation efforts.

Regarding the second recommendation specifically, Treasury agrees that the sector-specific plan should be updated and that the plan should include metrics to measure risk mitigation efforts within the sector. However, the update to the sector-specific plan should occur after the Cybersecurity and Infrastructure Security Agency (CISA) updates the National Infrastructure Protection Plan (NIPP), in coordination with the sector coordinating councils (SCCs) and government coordinating councils (GCCs). Treasury believes that the NIPP needs to be updated first, as it establishes cross-sector critical infrastructure priorities and objectives to which we and the sector align. We anticipate that the NIPP update will be completed in the second quarter of

[1] "Create a Freedom of Information Act exemption for certain financial sector cybersecurity related information to increase protection of the U.S. financial services sector. This proposal would provide Treasury with an appropriately scoped Freedom of Information Act (FOIA) exemption for cybersecurity-related information, in furtherance of the Department's responsibilities to enhance the security and resilience of the financial services sector's critical infrastructure. To identify risks to financial sector critical infrastructure, Treasury relies on private-sector financial organizations to provide a range of cyber threat and vulnerability information. Firms in the sector have not been sharing such information with Treasury due to concerns that their sensitive information will be subject to public disclosure under FOIA. A narrowly-tailored FOIA exemption would enable Treasury to leverage its relationship with the sector to improve information sharing. This proposal would strengthen Treasury's ability to identify risks to financial sector critical infrastructure and enable public and private-sector action to mitigate significant risks."

See https://home.treasury.gov/system/files/266/03.-DOSE-FY-2021-CJ.pdf.

Page 3

fiscal year 2021, and that CISA will provide guidance to the SSAs and SCCs/GCCs on revising the sector-specific plans. Once that occurs, we will work with our federal and nonfederal partners within the financial services sector to revise the sector-specific plan.

Thank you again for the opportunity to review the Report. We look forward to continuing to work with your office in the future.

Sincerely,

David B. Lacquement

Deputy Assistant Secretary

Cybersecurity and Critical Infrastructure Protection

U.S. Department of the Treasury

Accessible Text for Appendix III Comments from the National Credit Union Administration

August 31, 2020

Michael Clements

Director, Financial Markets and Community Investment

U.S. Government Accountability Office

441 G. Street, NW

Washington, D.C. 20548

Dear Mr. Clements:

We reviewed GAO's draft report entitled "Critical Infrastructure Protection: Treasury Needs to Improve Tracking of Financial Sector Cybersecurity Risk Mitigation Efforts".

The report describes key cyber-related risks facing the financial sector as well as steps the financial service industry is taking to share information and address risk to the sector. It also assesses actions federal agencies are taking to enhance the security and resilience of the sector. Additional opportunities are identified to improve tracking of risk mitigation efforts and to enhance the sector specific plan.

Cybersecurity is one of the NCUA's top priorities and we will continue to work closely with federal and state counterparts as well as the U.S. Treasury to keep the financial sector safe.

Thank you for the opportunity to comment on the draft report.

Sincerely,

Larry Fazio

Executive Director

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/fraudnet/fraudnet.htm

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@gao.gov, (202) 512-4400,
U.S. Government Accountability Office, 441 G Street NW, Room 7125,
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548