Securing the New Normal:

An Examination of Cybersecurity Issues Related to Remote Work and the Transition to a Digital Supervisory Relationship

January 11, 2021

ANCIAL SERVICES

Republicans

Hon. Patrick McHenry | Ranking Member
Committee on Financial Services

Hon. Andy Barr | Ranking Member
Subcommittee on Oversight and Investigations

Table of Contents

Executive Summary

On March 13, 2020, the President declared a national emergency in response to the spread and severity of COVID-19. Two weeks later, on March 27, Congress sent the Coronavirus Aid, Relief, and Economic Security (CARES) Act to the President's desk. For hospitals, small businesses, workers, schools, and state and local governments across the country, the CARES Act represented $2 trillion in much-needed aid. For cybercriminals, it represented an opportunity.

On April 8, 2020, American and British cybersecurity agencies jointly concluded, "it is likely that [criminals] will use new government aid packages responding to COVID-19" to target people and businesses.[1] The agencies issued a dire warning: cybercriminals were scanning for "vulnerabilities in software and remote working tools" to target people working from home due to the pandemic, and that the "frequency and severity of COVID-19 related cyberattacks" were likely to "increase" over the coming weeks.[2]

They were right. The coronavirus pandemic and related relief programs created an environment ripe for cybercriminal activity in the United States and around the world.

The coronavirus pandemic and related relief programs created an environment ripe for cybercriminal activity in the United States and around the world.

The federal effort to stabilize the economy via the CARES Act depended to some extent on the government's capacity to disburse COVID-19 relief funds rapidly, and an expansion of the availability of options for virtual banking relationships. Under those circumstances, financial institutions were put in a position to balance the government's interest in disbursing money quickly against their long-standing interest in implementing a robust system to prevent cyberattacks and scams. The federal financial regulatory agencies—which were similarly dealing with a new threat environment as their employees shifted to remote work status—were tasked with strengthening cybersecurity throughout the financial industry and with respect to their own functions.

The Proliferation of Malicious Cyberactivity since March 2020

Cybercriminals and hackers sought access to sensitive systems at government agencies and financial institutions alike. Malicious actors adapted their tactics to leverage the uncertainty caused by the COVID-19 pandemic to attack individuals. They invoked official corporate and government insignia to create the appearance of authenticity to lure consumers into providing personal or financial information.[3] Hackers sent emails featuring World Health Organization markings and phony information about the pandemic to hack into recipients' computers.[4] Cybercriminals used the pandemic to target corporate and government networks and preyed on "individuals . . . with a range of ransomware and malware" by "using financial themes in their phishing campaigns."[5] They used phishing schemes and other tactics to target government employees working from home on less secure networks.[6]

Cybercrime, however, was not strictly limited to non-state actors motivated by financial interests. In the spring of 2020, as the federal government mobilized its response to the dual health and economic crisis caused by the COVID-19 pandemic, a Russian-backed group launched what would become "one of the most sophisticated, and perhaps among the largest, attacks on federal systems in the past five years."[7] On December 13, 2020, the

1 Joint Press Release, U.S. Dep't of Homeland Security and U.K. Nat'l Cyber Security Centre, "UK AND US SECURITY AGENCIES ISSUE COVID-19 CYBER THREAT UPDATE" (Apr. 8, 2020), https://www.cisa.gov/news/2020/04/08/uk-and-us-security-agencies-issue-covid-19-cyber-threat-update.
2 *Id.*
3 *Id.*
4 *Id.*
5 *Id.*
6 Paul Shinkman, *Hackers Exploit Coronavirus to 'Surge' Attacks on the Pentagon,* U.S. NEWS & WORLD REPORT, Apr. 13, 2020.
7 David Sanger, *Russian Hackers Broke Into Federal Agencies, U.S. Officials Suspect*, N.Y. TIMES, Dec. 13, 2020, https://www.nytimes.com/2020/12/13/us/politics/rus-

Administration confirmed cybercriminals "broke into a range of key government networks, including in the Treasury and Commerce departments, and had free access to their email systems."[8] The breach affected government, consulting, technology, telecom, and oil and gas companies in North America, Europe, Asia and the Middle East.[9]

The Ranking Member requested information about the breach and on December 21, 2020, the Treasury Department provided a non-classified briefing. According to Treasury Department staff, the breach most severely affected systems belonging to the Departmental Offices division, including files and email accounts that belong to high-ranking Department officials, among others.[10] The network systems at several other Treasury bureaus were also breached.[11] The Department, like other federal agencies and companies, is assessing the scope of the breach and determining whether there are ongoing attempts to exfiltrate data.[12] On January 5, 2021, the U.S. intelligence and cybersecurity communities stated jointly that the attack was "likely of Russian origin" and estimated aproximatel 18,000 public and private sector entities were compromised.

The evidence makes clear the Committee should focus on further strengthening the nation's financial cybersecurity systems.

The extraordinary proliferation of attacks on systems with a nexus to the financial industry raised questions about how those targets were responding, and those questions remain important in light of the scope and breadth of the 2020 cyberattack on sensitive public and private sector networks. Understanding these threats, in January 2019, House Committee on Financial Services Ranking Member Patrick McHenry wrote to Chairwoman Maxine Waters to request the Committee focus on cybersecurity issues during the 116th Congress. Next, on April 22, 2020, House Committee on Financial Services Ranking Member Patrick McHenry requested information from financial regulators and the country's largest financial institutions regarding their efforts to detect and prevent COVID-19 related cyberattacks and similar tactics. This staff report is based on documents and information provided in response to the Ranking Member's request. This report also includes documents and information obtained from federal regulators related to their ongoing efforts to digitize their operations, and the community of jurisdictional inspectors general related to their most urgent unimplemented recommendations, many of which relate to IT and cybersecurity. The evidence makes clear the Committee must focus on further strengthening the nation's financial cybersecurity systems.

* * *

An Expedited Shift to Remote Work in the Private Sector

COVID-19 forced many private sector entities to rapidly adapt to a digital workplace. According to an April 2020 study by McKinsey, even before the virus hit, 92 percent of companies believed their business models to be outdated and in need of digitization.[13] This concept was reinforced by the pandemic, as millions of employees tested the remote work ecosystem. By one estimate, 31 percent of workers who were employed in early March had switched to working at home by the first week of April.[14] McKinsey found most companies—including many in the financial services industry—will continue remote work even after the current health crisis subsides.[15]

sian-hackers-us-government-treasury-commerce.html?auth=login-email&login=email
8 *Id.*
9 Ellen Nakashima and Craig Timberg, *Russian government hackers are behind a broad espionage campaign that has compromised U.S. agencies, including Treasury and Commerce*, WASH. POST, Dec. 14, 2020, https://www.washingtonpost.com/national-security/russian-government-spies-are-behind-a-broad-hacking-campaign-that-has-breached-us-agencies-and-a-top-cyber-firm/2020/12/13/d5a53b88-3d7d-11eb-9453-fc36ba051781_story.html.
10 Briefing from Dep't of Treasury Staff for H. Comm. on Fin. Services Staff (Dec. 21, 2020).
11 *Id.*
12 *Id.*
13 Matt Fitzpatrick, *et al., The Digital-Led Recovery from COVID-19,* McKinsey & Co., Apr. 2020, https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/the-digital-led-recovery-from-covid-19-five-questions-for-ceos#.
14 Erik Brynjolfsson, John J. Horton, Adam Ozimek, Daniel Rock, Garima Sharma, and Hong Yi Tu Ye, "COVID-19 and remote work: an early look at US data," Working Paper 27344 (Cambridge, MA: Nat'l Bur. of Economic Research, Apr. 2020), https://www.nber.org/papers/w27344.
15 *Id.*

Federal Agencies Follow Suit

As the financial services industry transitioned away from in person contacts toward a model that allowed for remote work and virtual interactions, federal regulators needed to do the same. In many cases, federal financial regulators needed a new and modernized digital infrastructure for efficient and secure digital operations.[16] For example, many agencies were conducting certain aspects of their regulatory work remotely for the first time, including hosting meetings using web-based platforms; employing e-delivery systems; and otherwise adapting new end-to-end processes.

Congress must consider reforms to address the need for federal regulators to modernize their operations to accommodate what may be a permanent transition toward digital interactions.

With regulated entities encouraging employees to continue work remotely, Congress should consider reforms to address the need for federal regulators to modernize their operations to accommodate what may be a permanent transition toward digital interactions.

The Ranking Member's Requests for Information

On April 17, 2020, Ranking Member McHenry issued requests to federal financial regulators and large financial institutions for documents and information pertaining to: attacks on third-party service providers; attacks on remote workers; malware attacks; denial of service activities; efforts to infiltrate, disrupt, or exfiltrate information and communications technology systems or networks; and other efforts to undermine cybersecurity.[17] The Ranking Member requested information to determine whether there was in fact an increase in cyberattacks since March 2020 and what federal resources were applied in response. Specifically, these documents were to include data related to the daily amount of cyberattacks detected; the agencies deployment of resources and technologies; the appointment and inclusion of qualified staff, cybersecurity training, staff accountability measures, and senior appointed leadership to strengthen accountability of cybersecurity measures; and any new efforts to prevent data loss.

Ranking Member McHenry also sought information on steps regulators took to modernize internal and external processes, specifically with the transition to a new at-home work environment brought on by the pandemic. On June 23, 2020, the Ranking Member sent letters to financial regulators requesting a description of their efforts to digitize operations, including how they would allow for digital interactions with regulated entities, and whether such policies will be permanent.[18]

The data also show cybercriminals are indeed attempting to leverage the pandemic, and COVID-related phishing and hacking schemes are ongoing.

The documents and information obtained by the Ranking Member show regulators and financial institutions moved quickly to implement new digitization and cybersecurity protocols. The data also show cybercriminals are indeed attempting to leverage the pandemic, and COVID-related phishing and hacking schemes are ongoing.

16 Till Contzen, *Increased Resilience Through Digitization*, Deloitte, Apr. 2020, *available at* https://www2.deloitte.com/global/en/pages/legal/covid-19/accelerate-digitization-increase-resilience.html.
17 Letter from Patrick McHenry, Ranking Member, H. Comm on Financial Services, to Jerome Powell, Chairman, Board of Governors of the Federal Reserve System, et al., Apr. 17, 2020 (on file with the committee).
18 Letter from Patrick McHenry, Ranking Member, H. Comm on Financial Services, to Jerome Powell, Chairman, Board of Governors of the Federal Reserve System, et al., June 23, 2020 (on file with the committee).

Conclusion

Congress must prioritize cybersecurity oversight as remote work and virtual interactions will continue permanently in some form. On September 24, 2019, Ranking Member McHenry introduced H.R. 4458, the Cybersecurity and Financial Systems Resilience Act. H.R. 4458 will ensure regulators are prioritizing cybersecurity efforts to combat the growing threat of cyberattacks to our financial system, represents an important step in that direction. On January 13, 2020, the House passed H.R. 4458 by voice vote. It was included in the Consolidated Appropriations Act for 2021, which Congress passed on December 21, 2020. The President signed the measure into law on Dec. 27, 2020.

H.R. 4458 will require U.S. banking regulators to provide Congress with detailed analysis of their efforts to protect against cyberattacks.

H.R. 4458 will require U.S. banking regulators to provide Congress with detailed analysis of their efforts to protect against cyberattacks. This will allow Congress to better understand what federal financial regulators are doing internally and in collaboration with financial institutions to prevent weak links in the financial system from causing widespread problems. The reports the Committee receives pursuant to H.R. 4458 in the summer of 2021 should form the basis for hearings and oversight initiatives throughout the 117th Congress. The Committee should also seek testimony and information from other key stakeholders, including the community of relevant inspectors general and the private sector. Congress can use this information to strengthen the cybersecurity platforms of financial regulators and institutions in order to better protect the consumers they serve.

The reports the Committee receives pursuant to H.R. 4458 in the summer of 2021 should form the basis for hearings and oversight initiatives throughout the 117th Congress.

Summary of Key Findings

1. Public and private sector stakeholders have long-standing concerns about the state of federal IT and the adequacy of cybersecurity measures throughout the financial services industry.

2. Information obtained by the Ranking Member in 2019 showed nearly one quarter (24.2 percent) of all open and unimplemented recommendations from inspectors general in the financial services jurisdiction related to information security. Some of those recommendations date back to 2011.

3. In March 2020, amidst the sharp increase in remote work and digital interactions between consumers, financial institutions, and federal agencies, cybercriminals and malicious actors apparently perceived an opportunity to exploit outdated IT and cybersecurity infrastructure at federal agencies.

4. Documents obtained by the Ranking Member in 2020 show an increase in COVID-related malicious cyberactivity since the federal workforce shifted to maximum remote work status.

5. Cybersecurity agencies identified a growing use of COVID-19 related themes in attacks by advanced persistent threat groups.

6. Financial regulators such as the Federal Deposit Insurance Corporation (FDIC) reported a rise in the risk of cybercrimes like phishing, email fraud, and cyberattacks on third party service providers and consumers that use mobile and online banking.

7. Financial institutions and their customers face threats from phishing, malware, ransomware, and denial of service attacks. Those tactics pre-date the pandemic and have remained largely unchanged. What has changed, however, are the themes and language used by malicious actors, which invoke pandemic themes at an increased rate.

8. Twenty-five percent of firms surveyed reported increased attacks targeting employees working from home.

9. Regulatory agencies moved quickly to adapt to conditions caused by COVID-19 and successfully transitioned to remote working and a virtual supervisory relationship. Several regulators credited IT and cybersecurity initiatives that started before 2020 for the successful transition to remote examinations and other supervisory functions.

10. The documents show financial institutions were able to serve new and existing customers using a mix of legacy and novel tools for digital interactions. Similarly, federal financial regulators were able to perform their supervisory and examination functions at levels roughly equivalent to those in 2019.

Background

Various public and private sector stakeholders have long-standing concerns about the state of federal IT and the adequacy of cybersecurity measures throughout the financial services industry. The COVID-19 pandemic shined a light on the issues that gave rise to those concerns and created an opportunity-rich environment for cybercriminals to exploit them.

Concerns Related to Federal Cybersecurity and IT Pre-Date the Pandemic

In early January 2019, Ranking Member Patrick McHenry wrote to the inspectors general at nine agencies under the Committee's jurisdiction requesting information regarding their work and as a follow up to their most recent semiannual report to Congress.[1] The Ranking Member requested that each office of inspector general (OIG) identify its most urgent open and unimplemented recommendations, the status of each identified recommendation, and the office's audit and investigative priorities.[2] The Ranking Member received responses from all nine jurisdictional OIGs.

The responses showed a total of 550 open and unimplemented OIG recommendations across all agencies as of March 31, 2019. Of those, nearly one quarter (24.2 percent) related to information security. Outstanding recommendations within the information security category focus on modernizing IT platforms and ensuring compliance with the Federal Information Security Modernization Act.[3] In fact, the vast majority of the open recommendations that were identified as "urgent" related to information security.[4] Those recommendations dated back to 2011 in some cases.

On January 23, 2019, at the outset of the 116th Congress, the Ranking Member called for a hearing on cybersecurity and information security in the financial sector to examine the readiness of financial firms and the U.S. government to protect digital consumer accounts and personal information against fraud, misuse, and unauthorized access. The Committee did not hold such a hearing until the summer of 2020.

The conditions that give rise to widespread concerns about the state of IT and cybersecurity at key government agencies and throughout the financial services industry persisted throughout 2019. The rapid spread of COVID-19 in early 2020, however, forced the public and private sector to address those concerns on an expedited basis.

An Evolving Threat Environment in 2020

In the spring of 2020 and throughout the year, various government agencies and public commissions identified cybersecurity threats and provided guidance for the private sector and consumers. The evolving nature of the threat environment created challenges for the financial

[1] Letters from Hon. Patrick McHenry, Ranking Member, Comm. on Fin. Serv. (Jan. 7, 2019).
[2] *Id.*
[3] Federal Information Security Modernization Act, 44 U.S.C.A §§ 3551-3558 (2014).
[4] Seven of nine IGs cited information security recommendations relating to compliance with the Federal Information Security Modernization Act in their responses to the Ranking Member's inquiry letter.

services industry, which was forced to adapt its model for interacting with consumers and regulators on an expedited basis. Collectively, the various threat assessments and alerts tended to focus on two issues: a proliferation of traditional digital scams that invoked COVID-19 themes; and vulnerabilities associated with systems that were not designed for remote work on a widespread scale.

Proliferation of Pandemic-Themed Cyberattacks

On April 8, 2020 the U.S. Cybersecurity and Infrastructure Security Agency (CISA) and the U.K.'s National Cyber Security Center (NCSC) issued an alert based on increased attempts to exploit the pandemic through ransomware and malware attacks.[5] The security agencies identified a growing use of COVID-19 related themes in attacks by advanced persistent threat groups.

For example, cybercriminals embedded malware in emails that claimed to originate from the Director General of the World Health Organization, and emails offering thermometers and face masks. In the U.K., a series of SMS messages used a government-themed lure to harvest email, address, name, and banking information.[6] These SMS messages—purporting to be from "COVID" and "UKGOV"—included a link directly to a phishing site.[7]

The alert also noted that cybercriminals were exploiting remote work tools. Specifically, the agencies identified "a growing use of COVID-19-related themes by malicious cyber actors" and found "the surge in teleworking has increased the use of potentially vulnerable services, such as virtual private networks (VPNs), amplifying the threat to individuals and organizations."[8]

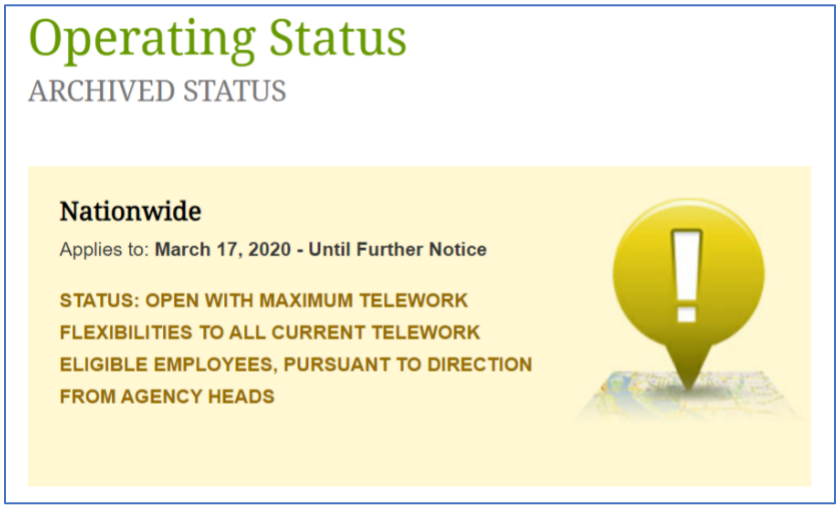
[5] Joint Press Release, U.S. Dep't of Homeland Security and U.K. Nat'l Cyber Security Centre, "UK AND US SECURITY AGENCIES ISSUE COVID-19 CYBER THREAT UPDATE" (Apr. 8, 2020), https://www.cisa.gov/news/2020/04/08/uk-and-us-security-agencies-issue-covid-19-cyber-threat-update.
[6] U.S. Dep't of Homeland Security and U.K. Nat'l Cyber Security Centre, Alert AA20-099A (Apr. 8, 2020), https://us-cert.cisa.gov/ncas/alerts/aa20-099a.
[7] *Id.*
[8] *Id.*

The agencies expected the frequency and severity of COVID-19 related cyberattacks to increase as the pandemic persisted. To prepare for these threats, the NCSC Director of Operations encouraged the public and organizations to remain vigilant and follow cybersecurity guidance to limit risk. To assist organizations within the United States, CISA provided guidance for individuals and businesses on defending and securing their networks and software against COVID-19 scams.

Indeed, as the federal government disbursed financial aid to small businesses and individuals affected by the pandemic, cybercriminals increased their activity too. The Treasury Inspector General for Tax Administration correctly predicted a surge in attempts to steal Economic Impact Payments from taxpayers by attacking the IRS systems.[9] Other financial agencies such as the Federal Deposit Insurance Corporation (FDIC) reported a rise in the risk of cybercrimes like phishing, email fraud, and cyberattacks on third party service providers and consumers that use mobile and online banking.[10]

Vulnerabilities Related to Remote Work

The Office of Personnel Management (OPM) shifted the federal workforce to maximum telework operating status on March 17, 2020, which forced the aging federal IT infrastructure to absorb an extreme increase in the number of employees using virtual private networks and other telework tools.[11] The shift toward telework at agencies throughout the federal government strained agency networks and shifted IT resources.[12]



On June 17, 2020, The Pandemic Response Accountability Committee (PRAC) released a report entitled "Top Challenges Facing Federal Agencies: COVID-19 Emergency Relief and Response Efforts." The report identified challenges faced by thirty-seven federal agencies that

[9] *Id.*
[10] *Id.*
[11] *Id.*
[12] *Id.*

received pandemic related funding.[13] Among its findings, the PRAC found pre-existing concerns related to cybersecurity were aggravated by the conditions caused by COVID-19. As the pandemic progressed throughout 2020, new opportunities for cyberattacks arose created by remote access and widespread telework operations.[14] The PRAC found cyberattacks posed a risk for both the financial services sector and security systems of regulators.[15]

Agencies are required to ensure that government systems are secure and protected because information that agencies obtain have the "potential to put personal information at risk and compromise national security."[16] The PRAC found the government's maximum telework status creates vulnerabilities in systems and strains the abilities of IT systems to support operations.

In particular, the PRAC found OPM's quick shift to a virtual workforce highlighted the agency's lack of secure teleconferencing software, among other shortcomings in its remote systems.[17]

According to the Environmental Protection Agency OIG, the large levels of remote access raises the risk of security breaches of remotely stored and transmitted data.[18] The National Reconnaissance Office (NRO) OIG reports similar risks of inadvertent disclosure of classified information by employees working from home and using poorly secured wi-fi, cell phones, and other non-secure means of communications.[19]

On September 14, 2020, the President's National Security Telecommunications Advisory Committee (NSTAC) released recommendations regarding the impacts of the new work-from-home environment caused by COVID-19 and provided guidance to the Administration on how to strengthen the resiliency of the nation's information and communications infrastructure.[20] The NSTAC identified critical steps to ensure the "resiliency of the U.S. national security and emergency preparedness communications."[21] While the NSTAC concluded that the "overall IT ecosystem response to the pandemic was strong," NSTAC identified areas for improvement that would enhance the nation's resiliency moving forward.[22]

According to NSTAC, USTelecom members reported a usage increase of over twenty-five percent nationwide during the first five months of the pandemic.[23] Even with this massive

---

[13] Offices of Inspector Generals, "Top Challenges Facing Federal Agencies: COVID-19 Emergency Relief and Response Efforts", June 2020 https://www.oversight.gov/sites/default/files/oig-reports/Top%20Challenges%20Facing%20Federal%20Agencies%20-%20COVID-19%20Emergency%20Relief%20and%20Response%20Efforts_1.pdf .
[14] *Id.*
[15] *Id.*
[16] *Id.*
[17] *Id.*
[18] *Id.*
[19] *Id.*
[20] Letter from John Donovan, Chair, The President's National Security Telecommunications Advisory Committee, to President Donald J. Trump, Sept. 14, 2020.
[21] *Id.*
[22] *Id.*
[23] *Id.*

uptick in usage, the U.S. network infrastructure was able to "serve the needs of the Nation well" due to capital investments and coordinated efforts across the industry.[24] Although IT infrastructure was capable of supporting peak capacity demands, even with the change to geographic distribution with employees working from home, NSTAC found that the massive usage increase revealed "unexpected gaps in preparedness and capabilities that should be addressed."[25]

NSTAC also identified that phishing attacks have increased greatly since the start of the pandemic due to the use of at-home networks. Cybercriminals shifted to "leveraging COVID-19 themes and targeting popular technology," such as collaboration platforms, in order to prey upon this new work environment.[26] With companies quickly moving to remote meetings, by using collaborative applications like Zoom, experts reported an increase in the amount and effectiveness of cyberattacks.[27] The NSTAC report identified that only incremental security measures were added to certain platforms in order to mitigate vulnerabilities, but that these platforms are working to update their cybersecurity infrastructure as they continue to play a major role in supporting remote work.[28]

NSTAC found employees working remotely shifted more than just their collaborative work duties to personal devices and at-home networks, which are outside the traditional purview of corporate IT offices. NSTAC identified that employee remote work set-ups left the door open to a range of new targets and "provided opportunities for malicious activities across threat vectors and at a scale not seen before."[29] As companies moved to avoid any productivity delays by shifting to a work-from-home environment, NSTAC reported that this change may have "left both the remote workforce and the core business systems vulnerable," and must be addressed going forward.[30]

Findings: Public and Private Sector Cybersecurity Measures

The increase in malicious cyberactivity and challenges related to widespread remote work, as described above, raised questions about how the public and private sector were responding. To address those questions, and to identify best practices to mitigate those challenges, Ranking Member McHenry sent letters to a sampling of financial institutions and their regulators on April 22, 2020.[31] The request covered information about COVID-19 related cyberattacks and their efforts to detect and prevent malicious cyberactivity.[32]

The Ranking Member requested documents pertaining to apparent COVID-19 related cyberattack, including, but not limited to, attacks on third-party service providers; attacks on

[24] *Id.*
[25] *Id.*
[26] *Id.*
[27] *Id.*
[28] *Id.*
[29] *Id.*
[30] *Id.*
[31] Letter from Patrick McHenry, Ranking Member, H. Comm on Financial Services, to Jerome Powell, Chairman, Board of Governors of the Federal Reserve System, et al., Apr. 22, 2020 (on file with the committee).
[32] *Id.*

remote workers; malware attacks; denial of service activities; efforts to infiltrate, disrupt, or exfiltrate information and communications technology systems or networks; and other efforts to undermine cybersecurity.[33]

Additionally, the Ranking Member requested information that would show cyberattack trends starting at the beginning of 2020, and what agency resources were used to respond to increased malicious cyberactivity. Specifically, these documents were to include data related to the daily amount of cyberattacks detected; deployment of resources, technologies, and qualified staff; cybersecurity training, staff accountability measures, and involvement of senior appointed leadership; and any new efforts to prevent data loss.

Finally, the Ranking Member sought documents relating to the adequacy of cybersecurity among third-party service providers; investigation requirements of regulated entities for COVID-19 related fraud; coordination efforts with financial institutions for detection and prevention of COVID-19 related fraud; processes for examining and verifying websites purporting to provide information and resources related to COVID-19; and any guidance or recommendations provided to regulated entities relating to COVID-19 and cybersecurity.[34]

The community of relevant financial institutions and each of the agencies surveyed by the Ranking Member on April 22, 2020 provided responses. The following sections summarize those responses.

Federal Deposit Insurance Corporation

The Federal Deposit Insurance Corporation (FDIC) responded to the Ranking Member on May 19, 2020. The FDIC reported an increase in cyber threats associated with COVID-19.[35] According to the FDIC's response, the Chair is accountable for addressing those threats. In addition to actively monitoring threats independently identified by the agency, the FDIC also relies on threat identifications from other government agencies including the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA).[36]

The FDIC stated that the agency strengthened internal controls in response to the current threat environment.[37] For example, the FDIC advised staff via internal communications about fraudulent activity related to COVID-19 and reemphasized security-related processes.[38]

The FDIC further stated the agency committed resources to advise regulated entities about new potential threats.[39] The FDIC collaborated with other government banking agencies to inform financial institutions of cybersecurity threats associated with COVID-19.[40] As of May

[33] *Id.*
[34] *Id.*
[35] Jelena McWilliams, Chair, Federal Deposit Insurance Corporation, *FDIC response to House Committee on Financial Services Ranking Member's Request*, May 19, 2020, on file with the Committee.
[36] *Id.*
[37] *Id.*
[38] *Id.*
[39] *Id.*
[40] *Id.*

2020, the FDIC issued three cybersecurity-related, non-public communications to financial institutions and service providers that are critical to the banking industry. FDIC examinations ensure that institutions are adequately monitoring, sharing, and responding to cyber threats and vulnerable information infrastructure.[41] The FDIC jointly authored guidelines for cybersecurity through the Federal Financial Institutions Examination Council (FFIEC).[42] The plan, entitled *Cybersecurity Resource Guide for Financial Institutions,* provides financial institutions with information and resources related to COVID-19.[43] The FDIC emphasized the importance of communication with institutions, and the FDIC also released a joint statements promoting risk management practicing for cloud computing services to protect consumer information.[44]

The FDIC has also taken action to inform and protect consumers from cybercriminal activity related to COVID-19. It published information on its public website to help consumers avoid COVID-19 related scams and identify possible cyberthreats.[45] The FDIC cites a March 18, 2020 press release that reminded consumers that the FDIC does not send unsolicited correspondence asking for money or sensitive information.[46] FDIC has worked to combat deceptive advertising targeting vulnerable consumers, including by issuing demands to at least two outlets to stop and correct false advertising stating that FDIC-insured deposits were at risk of forfeiture.[47]

National Credit Union Administration

The National Credit Union Administration (NCUA) responded to the Ranking Member on May 8, 2020. The NCUA has continued to communicate to credit unions of their legal duty to report to the NCUA catastrophic events that significantly impact their members.[48] The NCUA also continues to coordinate with other federal banking agencies on significant service provider reviews when there is a credit union or bank interest.[49] While the NCUA has not experienced any increase in cybersecurity probing internally, it has observed an increase in COVID-19 themed cyberattacks, and is committed to strengthening efforts to combat these attacks.[50]

---

[41] Federal Financial Institutions Examination Council, *Cybersecurity Threat and Vulnerability Monitoring and Sharing Statement,* November 3, 2014, *https://www.ffiec.gov/press/pdf/FFIEC_Cybersecurity_Statement.pdf*.
[42] Jelena McWilliams, Chair, Federal Deposit Insurance Corporation, *FDIC response to House Committee on Financial Services Ranking Member's Request*, May 19, 2020, on file with the Committee.
[43] Federal Financial Institutions Examination Council, *Cybersecurity Resource Guide for Financial Institutions*, October 2018, https://www.ffiec.gov/press/pdf/FFIEC%20Cybersecurity%20Resource%20Guide%20for%20Financial%20Institutions.pdf.
[44] Federal Financial Institutions Examination Council, *Joint Statement: Security in a Cloud Computing Environment*, April 30, 2020, https://www.ffiec.gov/press/pdf/FFIEC_Cloud_Computing_Statement.pdf.
[45] Federal Deposit Insurance Corporation, *Coronavirus (COVID-19) Information for Bankers and Consumers*, https://www.fdic.gov/coronavirus/.
[46] Federal Deposit Insurance Corporation, *FDIC: Insured Deposits are Safe; Beware of Potential Scams Using the Agency's Name*, March 18, 2020, https://www.fdic.gov/news/press-releases/2020/pr20032.html.
[47] Federal Deposit Insurance Corporation, *FDIC Demands Monetary Gold Cease False Advertising Campaign*, (March 19, 2020), https://www.fdic.gov/news/press-releases/2020/pr20037.html.
[48] Rodney Hood, Chairman, National Credit Union Administration, *NCUA response to House Committee on Financial Services Ranking Member's Request*, May 7, 2020, on file with the Committee.
[49] *Id.*
[50] *Id.*

The NCUA informed the Committee that its external cybersecurity capabilities, which focuses on information systems used by regulated credit unions, is led by the Special Advisor for Cybersecurity and the Director of Critical Infrastructure.[51] Its internal systems focus on information systems that the NCUA relies on to conduct its work, the systems are managed by the agency's Chief Information Officer and Senior Agency Information Security and Risk Officer.[52] NCUA stated its cybersecurity policies and practices for monitoring the industry adhere to all criteria established by the National Initiative for Cybersecurity Education.[53]

The NCUA has dedicated resources to work with credit unions on cyber related issues, especially during the pandemic. Credit unions are required to report directly to the NCUA Chairman and its Responsible Risk Executive for accountability and oversight under the Gramm-Leach-Bliley Act and the Federal Information Security Management Act of 2002.[54] This requirement, according to NCUA, has held entities accountable during the pandemic.[55] The NCUA insists that its system of layered security architecture and its utilization of public and private services have been effective in identifying, responding, and recovering from cybersecurity associated threats and attacks.[56]

The NCUA continues to coordinate with the Financial Crimes Enforcement Network, the Department of Homeland Security, and other law enforcement entities, including the Federal Bureau of Investigation and Secret Service to monitor and investigate instances of COVID-19 related financial fraud.[57] Staff at the NCUA participates in daily calls led by the Department of the Treasury and the Financial Services Information Sharing and Analysis Center, which includes the DHS Cybersecurity and Infrastructure Security Agency in addition to industry regulators, trade associations, and institutions.[58]

Additionally, the NCUA noted the importance of outreach to their regulated entities.[59] The NCUA has made several internal and external communications related to cybersecurity issues since March 2020, and dedicated resources specifically to monitoring the adequacy of industry's cybersecurity policies and procedures.[60]

---

[51] *Id.*
[52] *Id.*
[53] *Id.*
[54] *Id.*
[55] *Id.*
[56] *Id.*
[57] *Id.*
[58] *Id.*
[59] *Id.*
[60] Rodney Hood, Chairman, National Credit Union Administration, *NCUA response to House Committee on Financial Services Ranking Member's Request*, May 7, 2020, on file with the Committee.

Federal Reserve Board

The Federal Reserve Board (the Fed) responded to the Ranking Member on June 11, 2020. The response stated that the Fed prioritizes cybersecurity and is proactively limiting cybercriminal activity targeting COVID-19 relief programs.[61] The Fed highlighted its emphasis on cybersecurity resilience through supervision and regulation of financial institutions.[62] Through policy and examination procedures, the Fed addresses cybersecurity threats by emphasizing the importance of safeguarding financial systems and infrastructure, which took on heightened importance as the number of cyberattacks increased during the course of the pandemic.[63] Its supervisory function also enables the Fed to provide more informed recommendations for oversight and incident management, as it uses cyber situational awareness analytics to monitor and collect information from across the financial sector.[64]

The Fed described an ongoing effort to monitor, identify, and mitigate cybersecurity threats through coordination with federal agencies and public and private groups.[65] The Federal Reserve uses the Federal Financial Institutions Examination Council (FFIEC) on Information Security and Business Continuity Management IT booklets to assess cybersecurity infrastructure, incident management capabilities, and operational resilience of supervised institutions.[66] The Federal Reserve also acted through interagency coordination by issuing financial institution guidance statements for areas of risk associated with the pandemic.[67] The Fed highlighted the importance of coordination when combating cybersecurity challenges associated with COVID-19.[68]

The Fed's consumer compliance supervision program ensures supervised institutions continue to safeguard the personal financial information of customers by assessing institutions' compliance with financial privacy laws and regulations, such as Regulation P and the "red flags" rule under the Fair Credit Reporting Act.[69] Compliance supervision has taken on heightened importance in the midst of increased cybercriminal activity.

The Fed prioritizes information sharing with regulated banks and continues to issue alerts and educational statements that inform both consumers and institutions of cybercriminal activity related to COVID-19.[70] The Fed has also focused outreach on reinforcing security measures and

---

[61] Jerome Powell, Chairman, Federal Reserve Board, *Federal Reserve Board response to House Committee on Financial Services Ranking Member's Request*, June 11, 2020, on file with the Committee.
[62] *Id.*
[63] *Id.*
[64] *Id.*
[65] *Id.*
[66] Federal Financial Institutions Examination Council, *Information Security*, https://ithandbook.ffiec.gov/it-booklets/information-security.aspx.
[67] Board of Governors of the Federal Reserve System, *SR 20-3 / CA 20-2: Interagency Statement on Pandemic Planning*, March 10, 2020, https://www.federalreserve.gov/supervisionreg/srletters/SR2003.htm.
[68] Jerome Powell, Chairman, Federal Reserve Board, *Federal Reserve Board response to House Committee on Financial Services Ranking Member's Request*, June 11, 2020, on file with the Committee.
[69] 15 U.S.CA § 1681.
[70] Jerome Powell, Chairman, Federal Reserve Board, *Federal Reserve Board response to House Committee on Financial Services Ranking Member's Request*, June 11, 2020, on file with the Committee.

providing updates related to the Department of the Treasury's Treasury Check Verification Application.[71]

Office of the Comptroller of the Currency

On May 11, 2020, the Office of the Comptroller of the Currency (OCC) responded to the Ranking Member's request and identified cybersecurity as a top concern for the financial sector.[72] The OCC acknowledged major concerns relating to COVID-19 emergency relief programs.[73] As a banking supervisor, the OCC assesses the ability of banks to manage risk by monitoring cybersecurity trends.[74] The OCC coordinates with several associated public and private agencies to maintain awareness of cybersecurity threat trends.[75] The OCC constantly coordinates with other regulators, and cited a FFIEC statement for strengthening coordination and collaboration among financial institutions for sharing and receiving cyber threat information, specifically referencing the Financial Services Information Sharing and Analysis Center (FS-ISAC).[76]

The Comptroller stated that the agency prioritizes cybersecurity in the course of supervising the financial institutions in its jurisdiction.[77] The OCC requires these institutions to have programs for collecting, analyzing, and mitigating cyber vulnerabilities. OCC examiners assess whether financial institutions have adequate processes for identifying cybersecurity threats by leveraging the FFIEC Cybersecurity Assessment Tool (CAT).[78]

OCC examinations have continued throughout the pandemic. The OCC stated it took appropriate steps to address cybersecurity trends by adjusting examination focus, sharing threat information with financial institutions, and publishing areas of concern for financial institutions.[79]

The Comptroller acknowledged the new risks and challenges created by the pandemic.[80] The OCC has acted in coordination with other banking agencies to combat cybersecurity threats associated with COVID-19 and to supervise financial institutions during the pandemic.[81] The

[71] Board of Governors of the Federal Reserve System, *Coronavirus Disease 2019 (COVID-19)*, https://www.federalreserve.gov/covid-19.htm.
[72] Joseph Otting, Comptroller, Office of the Comptroller of the Currency, *OCC response to House Committee on Financial Services Ranking Member's Request*, May 11, 2020, on file with the Committee.
[73] *Id.*
[74] *Id.*
[75] *Id.*
[76] Federal Financial Institutions Examination Council, *Cybersecurity Threat and Vulnerability Monitoring and Sharing Statement*, https://www.ffiec.gov/press/PDF/FFIEC_Cybersecurity_Statement.pdf.
[77] Joseph Otting, Comptroller, Office of the Comptroller of the Currency, *OCC response to House Committee on Financial Services Ranking Member's Request*, May 11, 2020, on file with the Committee.
[78] Federal Financial Institutions Examination Council, *Cybersecurity Assessment Tool*, https://www.ffiec.gov/cyberassessmenttool.htm.
[79] Joseph Otting, Comptroller, Office of the Comptroller of the Currency, *OCC response to House Committee on Financial Services Ranking Member's Request*, May 11, 2020, on file with the Committee.
[80] *Id.*
[81] *Id.*

agency has prioritized maintaining an informational COVID-19 webpage on the OCC website and communicating with financial institutions.[82]

The OCC acknowledges concerns regarding a heightened cybersecurity risk to third-party service providers, and has issued third-party risk guidelines and examines risk management programs related to third-parties vendors.[83] The OCC coordinates with other banking agencies under the Bank Service Company Act in conducting cybersecurity examinations of service providers determined to be critical to the banking industry.[84]

Consumer Financial Protection Bureau

The Consumer Financial Protection Bureau (CFPB) responded to the Ranking Member's request on May 7, 2020. The CFPB recognized the legitimacy of concerns related to cybersecurity and COVID-19 relief programs.[85] The CFPB coordinates with federal and state regulatory agencies and financial institutions to respond to emerging cybersecurity threats.[86]

The CFPB stated its commitment to strengthening cybersecurity protections for consumers.[87] Its role on the Financial and Banking Information Infrastructure Committee (FBIIC) positions CFPB to participate in the inter-agency development of cybersecurity policy and to identify and improve cybersecurity infrastructure, further the adoption of effective cybersecurity practices, and enhance financial institutions' ability to respond and recover from cyberattacks, especially during the pandemic.[88]

The CFPB is also a member of the Federal Financial Institutions Examination Council's (FFIEC's) Cybersecurity and Critical Infrastructure Working Group (CCIWG), which coordinates with federal agencies to develop cybersecurity related standardized examinations for financial institutions. The FFIEC recently released a joint statement addressing the use of cloud computing services and cybersecurity risk management practices for financial institutions.[89]

---

[82] Office of the Comptroller of the Currency, *COVID-19 (Coronavirus)*, https://www.occ.treas.gov/topics/supervision-and-examination/bank-operations/covid-19-information/convid-19-info-index.html ;

[83] Office of the Comptroller of the Currency, *Third-Party Relationships: Risk Management Guidance*, (October 30, 2013), https://www.occ.treas.gov/news-issuances/bulletins/2013/bulletin-2013-29.html.

[84] Joseph Otting, Comptroller, Office of the Comptroller of the Currency, *OCC response to House Committee on Financial Services Ranking Member's Request*, May 11, 2020, on file with the Committee.

[85] Kathleen Kraninger, Director, Consumer Financial Protection Bureau, *CFPB response to House Committee on Financial Services Ranking Member's* Request, May 7, 2020, on file with the Committee.

[86] *Id.*

[87] *Id.*

[88] *Id.*

[89] Federal Financial Institutions Examination Council, *Joint Statement: Security in a Cloud Computing Environment*, (April 30, 2020), https://www.ffiec.gov/press/pdf/FFIEC_Cloud_Computing_Statement.pdf.

The CFPB stated it has taken steps to monitor its own cyber information systems, as it coordinates closely with law enforcement and national security agencies.[90] According to the CFPB, this coordination has become even more crucial as the pandemic progresses.[91]

The CFPB highlighted its automated detection capabilities that would notify the CFPB's Cybersecurity Incident Response Team (CSIRT), which develops a coordinated response with the U.S. Computer Emergency Readiness Team and the Department of Homeland Security in the event that the CFPB's "first layer of defense" was breached.[92] The CFPB noted that while there has been an increase in the amount of cyberattacks on its internal systems since the beginning of the year, none have been successful.[93]

The CFPB is committed to strengthening its cybersecurity system infrastructure and procedures for mitigating risk and protecting sensitive information.[94] The CFPB has issued internal guidelines to its staff for using third-party teleconference platforms, increased malware protection associated with CFPB network gateways, and issues cybersecurity-related advisories to staff of new cyber activity and developments.[95] The CFPB included its most recent Office of Inspector General (OIG) yearly audit of its information security program. The audit concluded that its information security continuous monitoring process and incident response process are effective.[96]

Financial Institutions

The Bank Policy Institute's (BPI) Technology Policy Division collected responses from the financial institutions surveyed by the Ranking Member. The documents and information produced by BPI shed light on the unique cybersecurity challenges created by the pandemic and how the banks have responded to these cyberthreats.[97]

The documents and information show the industry is dealing with cybersecurity threats, as usual, but adapting to the fact that cybercriminals are attempting to exploit the pandemic using new tactics.[98] The financial institutions stated that the quantity of cybersecurity threats increased from pre-pandemic levels and remained steady since the beginning of the pandemic.[99] Throughout the United States, financial institutions (FIs) constantly face threats from phishing, malware, ransomware, and denial of service attacks—those tactics pre-date the pandemic and have remained largely unchanged. What has changed, however, are the themes and language used by malicious actors:

---

[90] Kathleen Kraninger, Director, Consumer Financial Protection Bureau, *CFPB response to House Committee on Financial Services Ranking Member's* Request, May 7, 2020, on file with the Committee.
[91] *Id.*
[92] *Id.*
[93] *Id.*
[94] *Id.*
[95] Consumer Financial Protection Bureau, *Teleconference Participation Directive (TPD)*, April 20, 2020.
[96] Bureau of Consumer Financial Protection, Office of Inspector General, *2019 Audit of the Bureau's Information Security Program*, October 31, 2019.
[97] Christopher Feeney, Executive Vice President, Bank Policy Institute, *BITS response to House Committee on Financial Services Ranking Member's* Request, May 13, 2020, on file with the Committee.
[98] *Id.*
[99] *Id.*

- Eighty-two percent of the firms found various scams shifted to COVID-19 related themes.[100]

- Eighteen percent reported an increase in specific attacks such as phishing, credential stuffing, and anomalous web traffic targeting websites.[101]

- Since the start of the pandemic, over 1,500 financial-themed cybercriminal webpage domains were created.[102] These online portals are designed to steal information, usernames, and passwords.[103]

The FIs also reported an increase in cyberattacks internally.[104] Twenty-five percent of firms reported increased attacks targeting employees working from home, such as fraudsters pretending to be executives using personal email addresses.[105] Other firms reported seeing many COVID-19 related subject lines from compromised business emails. [106] This represents an ongoing cybersecurity challenge for financial institutions and firms of all kinds, which has grown more acute with the increase of remote working.

The financial services industry works closely with third party service providers that must also maintain strong cybersecurity practices.[107] These standards are enforced through contracts, and financial institutions have committed to ensuring their vendors apply best practices.[108] Forty-eight percent of firms reported an increase of attacks against third party providers.[109] Firms report that the increase of attacks on third parties is similar to trends during natural disasters.[110] Despite the increase in attacks, eighty-six percent of financial firms continued to receive information from third parties and forums such as FS-ISAC, FSARC, and CISA as a means of information sharing and transparency.[111]

According to BPI, firms have implemented new protocols and standards to prevent pandemic-era cyberattacks.[112] Although firms had to increase the network capacity to allow more employees to work from home, they restricted access to information in the home and increased training for phishing and fraud.[113] About sixty-two percent of firms created "war rooms" typically used in times of crisis to test response plans and procedures to build and prepare for resiliency and business continuity.[114] Furthermore, sixty-seven percent of firms

---

[100] *Id.*
[101] *Id.*
[102] *Id.*
[103] *Id.*
[104] *Id.*
[105] *Id.*
[106] *Id.*
[107] *Id.*
[108] *Id.*
[109] *Id.*
[110] *Id.*
[111] *Id.*
[112] *Id.*
[113] *Id.*
[114] *Id.*

enhanced reporting and communications functions to address technology and cyber-related governance. Those firms also enhanced the security of their remote network infrastructures.[115] Many firms reported being in ongoing communications with their regulators on the status of the firm's efforts to respond and adjust to the nuances of the pandemic.[116]

BPI stated that financial firms throughout the country improved their overall security by enhancing training tools and increasing communication of reporting to management and regulators.[117] Financial institutions stated that they continue to adapt and maintain cybersecurity and resiliency practices despite the impact of the ongoing and constantly-evolving health crisis through cooperation within the industry and with government.[118]

Findings: Digitization of Federal Supervisory Functions

On June 23, 2020, Ranking Member McHenry sent letters to banking regulators requesting documents and information related to progress toward digitizing operations in response to the environment caused by the pandemic.[119] The request covered new protocols for digital interactions with regulated entities and whether these digitization policies will be permanent.[120] The Ranking Member emphasized modernizing digital infrastructure to ensure efficient and secure operations, as many regulated entities are currently working remotely, and intend to continue to do so after the pandemic.

Federal Deposit Insurance Corporation

The Federal Deposit Insurance Corporation (FDIC) responded to the Ranking Member's letter on July 10, 2020. The Chair wrote that the FDIC has acted quickly to modernize and digitalize its operations to allow for remote working due to the COVID-19 pandemic.[121] Chair Jelena McWilliams emphasized the measures the agency has undertaken to modernize its own IT infrastructure and encourage the adoption of advanced technology used more widely in the private financial services sector.[122] The FDIC established the Subcommittee on Supervision Modernization for the Advisory Committee on Community Banking (CBAC) to find solutions related to leveraging technology and improving procedures to make examinations more efficient, while recognizing the needs of a remote workforce.[123] The Chair of the Subcommittee indicated that the agency has incorporated ideas from subcommittee meetings for advancing long-distance/virtual learning and new supervisory technologies for improving efficacy.[124]

---

[115] *Id*.
[116] *Id*.
[117] *Id.*
[118] *Id.*
[119] Letter from Patrick McHenry, Ranking Member, H. Comm on Financial Services, to Jerome Powell, Chairman, Board of Governors of the Federal Reserve System, et al., June 23, 2020 (on file with the committee).
[120] *Id.*
[121] Jelena McWilliams, Chair, Federal Deposit Insurance Corporation, FDIC *response to House Committee on Financial Services Ranking Member's Request*, July 10, 2020, on file with the Committee.
[122] *Id.*
[123] Federal Deposit Insurance Corporation, *FDIC's Subcommittee on Supervision Modernization for the Advisory Committee on Community Banking Holds its Inaugural Meeting*, March 6, 2019.
[124] Jelena McWilliams, Chair, Federal Deposit Insurance Corporation, FDIC *response to House Committee on Financial Services Ranking Member's Request*, July 10, 2020, on file with the Committee.

The Chair stated that throughout the pandemic, FDIC has been able to complete nearly all scheduled examination activities since it mandated that all employees telework in March.[125] The FDIC credits previously implemented digital advances for allowing it to effectively complete examinations remotely, as it had conducted more than forty percent of all Risk Management and sixty percent of Consumer Compliance/Community Reinvestment Act (CRA) examinations off-site prior to COVID-19.[126]

In 2018, the FDIC began developing and testing a standardized export of imaged loan documents from financial institutions' core services providers to streamline examinations and adopted WebEx to alternatively allow examiners to review imaged loan files by connecting to an institution's non-transactional terminal. In 2019, the FDIC piloted the Microsoft Teams platform, to improve collaboration and communication between examiners and institutions.[127] While the FDIC has used Microsoft Teams as its predominant collaborative examination tool since mandatory telework began, it also uses VMWare to allow examiners to review financial institution system activity and WebEx for other file review and collaboration activities.[128] The FDIC commits to continuing to find more tools to make remote working more effective.[129]

The FDIC also implemented new policies to better serve financial institutions during the pandemic. For instance, the agency responded to COVID-19 by establishing a new process related to closing activities.[130] This approach limits physical presence, as a remote team supports a smaller on-site team using collaborative technology for virtual meetings and electronic file sharing.[131] The FDIC stated this approach has been successfully applied and that it may enable the use of smaller on-site teams even after COVID-19 related remote working concludes.[132]

The FDIC stated that previously implemented IT infrastructure and operation modernization programs enabled it to effectively transition to teleworking.[133] The FDIC prioritized the health and safety of employees and quickly leveraged existing remote access infrastructure and collaborative tools, as set out below, to quickly implement additional remote operation enhancements.[134]

First, the FDIC doubled internet bandwidth at data centers, upgraded remote access infrastructure, and increased conference line capacity.[135] It also increased network accessibility by enabling FDIC-issued smartphones to use wireless hotspots.[136]

---

[125] *Id.*
[126] *Id.*
[127] *Id.*
[128] *Id.*
[129] *Id.*
[130] *Id.*
[131] *Id.*
[132] *Id.*
[133] *Id.*
[134] *Id.*
[135] *Id.*
[136] *Id.*

Second, the FDIC used FDICLearn and other online applications to quickly transition all training into virtual formats.[137]

Third, the FDIC conducted on-boarding procedures entirely virtually, and shipped laptops and other electronic devices directly to new employees.[138]

Finally, the FDIC issued industry guidance to encourage the use of electronic communications through the FDIC's Secure Email Portal or its secure file exchange system rather than using physical mail. The FDIC also uses the Secure Email portal to send outgoing supervisory communications.[139]

Due to COVID-19, the agency has taken a creative approach to develop a new financial reporting portal by launching the Rapid Prototyping Competition, which invited leading technology companies to create programs over a six-month period. The project is intended to provide examiners more accessible and targeted data on certain specified financial metrics.[140] The FDIC believes this competition will help create a technology-based financial reporting system that is less-burdensome to banks, provides more timely and comprehensive data for examiners, and encourages more effective supervision of banks.[141] While the FDIC will not require financial institutions to participate, it hopes that market incentives from reduced compliance costs, more efficient operations, and increased dynamic competition will encourage adoption. The FDIC Chair has committed to continuing to engage with technology companies to modernize financial reporting.[142]

Finally, the FDIC released a Request for Information (RFI) seeking input on whether a public/private standard setting organization and voluntary-certification program would improve the ability of financial institutions to integrate new technology and perform due diligence on third-party providers.[143] The FDIC believes that a certification system would encourage financial institutions to implement innovative technologies, as it could potentially standardize due diligence processes, reduce costs, and decrease operational and regulatory uncertainty.[144] While third-parties would not be required to participate, the FDIC attests that certification would allow third-parties to avoid timely and costly on-boarding processes.[145]

National Credit Union Administration

On June 23, 2020, National Credit Union Administration Chairman Rodney Hood responded to Ranking Member McHenry's request. Chairman Hood stated that NCUA took

[137] *Id.*
[138] *Id.*
[139] *Id.*
[140] *Id.*
[141] *Id.*
[142] *Id.*
[143] Federal Deposit Insurance Corporation, *FDIC Seeks Input on Voluntary Certification Program to Promote New Technologies*, (July 20, 2020), https://www.fdic.gov/news/press-releases/2020/pr20083.html.
[144] Jelena McWilliams, Chair, Federal Deposit Insurance Corporation, FDIC *response to House Committee on Financial Services Ranking Member's Request*, July 10, 2020, on file with the Committee.
[145] *Id.*

proactive measures prior to the COVID-19 pandemic to be able to meet the new demands of the remote workplace.[146] In 2019, the NCUA allocated funding for the Information Technology Infrastructure, Platform and Security Refresh program to allow credit union examiners to perform their work more effectively and efficiently.[147] The agency refreshed and/or replaced virtual servicers, wireless network access points, virtual private networks, and central office routers to ensure secure data and stable operations.[148] The NCUA also upgraded its bandwidth, which now supports the increased usage throughout the pandemic.[149] The Chair indicated that these efforts assisted the agency transition into the current work necessities of the pandemic.[150]

The NCUA implemented a Security Management Tool optimization effort in 2019. With respect to its supervisory work and its nexus to cybersecurity and governance, the NCUA focuses on: risk management and compliance; vulnerability and patch management; perimeter protection; security event and information management; endpoint protection; and incident response capabilities for Cybersecurity and IT Operations.[151] The NCUA intends its optimization effort to create a more proactive, centralized, data-driven management of enterprise services.[152] These system wide upgrades seek to enhance the agency's security stance during the pandemic and strengthen the agency's infrastructure in the long term.[153]

The NCUA has been operating remotely since the beginning of the pandemic.[154] The agency procured licenses for virtual meeting software packages to allow credit unions to collaborate remotely.[155] Meeting software and web conferencing accounts were provided to all NCUA employees to optimize productivity at home, assist teams, conduct interviews and training, and share information with officials.[156]

The agency has been conducting offsite examination work since March 2020 due to the pandemic.[157] As of June 2020, NCUA conducted off site work with over 100 credit unions, and received positive responses and cooperation.[158] The agency states that the Secure File Transfer Portal (SFTP) implemented in June 2018 has facilitated the transition during the pandemic.[159] The SFTP is an alternative method for digitally sharing and exchanging examination files within the agency and has allowed for remote working.[160]

---

[146] Rodney Hood, Chairman, National Credit Union Administration, *NCUA response to House Committee on Financial Services Ranking Member's Request*, June 23, 2020, on file with the Committee.
[147] *Id.*
[148] *Id.*
[149] *Id.*
[150] *Id.*
[151] *Id.*
[152] *Id.*
[153] *Id.*
[154] *Id.*
[155] *Id.*
[156] *Id.*
[157] *Id.*
[158] *Id.*
[159] *Id.*
[160] *Id.*

The Chair stated that the agency continues to implement new procedures.[161] Looking forward, the NCUA plans to schedule an End of Life Voice over Internet Protocol (VoIP) Phone System, which will help to implement a new business productivity suite and an enhanced unified communications and conferencing capability.[162] The VoIP project will enable users to have an integrated unified communications capability for both voice and video communication that may lend itself for remote and virtual examinations.[163]

The agency has ongoing initiatives to improve and modernize how the agency conducts examinations and supervision as well.[164] The goals of these initiatives are to replace outdated examination systems and adopt enhanced examination techniques.[165] One project approved by the NCUA Board is currently in the research and discovery phase.[166] The project is a virtual examination process to allocate resources to research methods for conducting off site exams.[167] The goal of the current work group is to identify ways to advance analytical capabilities and standardize interaction protocols.[168]

The NCUA also plans to implement an Enterprise Solutions Modernization program.[169] The program will streamline and align examination and data processes, technology and infrastructure across business functions.[170] The NCUA stated this program will allow the agency to introduce new examination software to reduce manual reviews of examination reports.[171]

The NCUA's modernization efforts are carried out with the purpose of: reducing the burden on credit unions; improving off-site supervision capabilities; providing more consistency and standardization for the examination and supervision process; exploring the industry's interest in adopting new technology; and improving communications between examiners, credit unions and state regulatory authorities.[172] With these purposes in mind, the agency regularly assesses its response to COVID-19 and evaluates aspects of the digital operations that should be made permanent following the pandemic.[173] The NCUA credits its effective response to the COVID-19 pandemic to the prior implementation of IT and cybersecurity initiatives.[174] The NCUA plans to continue improving its digital tools and technology to increase the agency's reliability, efficiency, and effectiveness.[175]

---

[161] *Id.*
[162] *Id.*
[163] *Id.*
[164] *Id.*
[165] *Id.*
[166] *Id.*
[167] *Id.*
[168] *Id.*
[169] *Id.*
[170] *Id.*
[171] *Id.*
[172] *Id.*
[173] *Id.*
[174] *Id.*
[175] *Id.*

Office of the Comptroller of the Currency

The Office of the Comptroller of Currency (OCC) responded to the Ranking Member on July 10, 2020, and described its modernize the agency.[176] Since the beginning of the pandemic, the OCC has transitioned to remote work status for ninety-five percent of all employees.[177] Throughout this time, the OCC has worked to implement new technology and tools that digitize its workforce and to further develop future digitization plans.[178]

Efforts to digitize at the OCC started prior to COVID-19. Since June 2018, all OCC employees began using Cisco AnyConnect VPN software on their computers. In conjunction with a Personal Identity Verification (PIV) card, OCC employees can use the VPN software to access OCC software and data from any location.[179] In addition to establishing secure and safe connections through VPN, the OCC has used a variety of tools to support transmission of information with financial institutions that the agency regulates.[180]

The OCC modified the policy for Accessing and Managing Confidential Supervisory Information in August 2018 to allow financial institutions to access information remotely.[181] This allowed financial institutions to access confidential supervisory information under certain conditions such as using a web-based portal or VPN.[182] The Comptroller indicated that these efforts have allowed for an easier transition to remote work.[183]

The OCC also uses BankNet, the agency's own secure website for sharing confidential data with national banks and federal savings associations.[184] BankNet provides applications to support service providers, multi-regional data processing service providers, external attorneys and consultants, bank regulatory agencies that supervise financial institutions and individuals that supply information for the OCC's use.[185] These applications provide access for OCC employees to transfer large files from OCC-regulated institutions and other regulators to the OCC.[186] BankNet supports access to the Money Laundering Risk System so employees can submit money laundering reports online.[187] It also allows Central Application Tracking to authorize bank employees to draft, submit, and track filings and allows OCC analysts to manage those filings remotely.[188] Additionally, BankNet provides Intralinks, an externally hosted, cloud-based service and FDICconnect, the Federal Deposit Insurance Corporation's (FDIC) large file

[176] Brian Brooks, Acting Comptroller, Office of the Comptroller of the Currency, *OCC response to House Committee on Financial Services Ranking Member's Request*, July 10, 2020, on file with the Committee.
[177] *Id.*
[178] *Id.*
[179] *Id.*
[180] *Id.*
[181] *Id.*
[182] *Id.*
[183] *Id.*
[184] *Id.*
[185] *Id.*
[186] *Id.*
[187] *Id.*
[188] *Id.*

transfer system. The OCC can easily exchange information when participating in FDIC interagency examinations by using this service.[189]

The OCC enabled Adobe E-Signature functionality in August 2011.[190] This service allows employees to use their PIV cards to sign Adobe PDF documents.[191] As a means of security, the OCC also uses encrypted mail service provided by Microsoft Outlook to protect documents containing sensitive or Personally Identifiable Information.[192] The OCC plans to implement a single supervisory platform and streamlined process in 2022 to continue to modernize its operations.[193] By 2021, the agency expects it will modernize its network infrastructure and supporting technology to continue to support the OCC's mission.[194]

Consumer Financial Protection Bureau

In its response dated July 10, 2020, the Consumer Financial Protection Bureau (CFPB) recognized the need to further modernize operative capabilities to accommodate remote working especially with the current conditions of the pandemic.[195] The Director credited prior CFPB systems and technological modernization initiatives for allowing it to quickly respond to remote working in March 2020.[196] These initiatives included increasing cloud-based services, implementing internal collaborative workforce tools, and strengthening infrastructure.[197]

In her response, the Director stated the CFPB has responded quickly to challenges caused by COVID-19 by making three significant investments in digital operations initiatives that support the transition to remote work.[198] First, the CFPB configured new dual hardware for its Always on Virtual Private Network (AOVPN) to handle increased network demand from remote working.[199] The AOVPN allows users to remotely perform office related tasks by connecting users to the CFPB network through continuous cybersecurity identification protection processes.[200] Second, the CFPB replaced its virtual conferencing system with Cisco WebEx, a FedRAMP authorized and secured cloud-based application that allows CFPB employees to host virtual conferences for internal and external participants.[201] According to CFPB, the WebEx application will allow it to support employee education and development through new virtual Training Center capabilities.[202] Third, the CFPB began implementing the Microsoft Teams

---

[189] *Id.*
[190] *Id.*
[191] *Id.*
[192] *Id.*
[193] *Id.*
[194] *Id.*
[195] Kathleen Kraninger, Director, Consumer Financial Protection Bureau, *CFPB response to House Committee on Financial Services Ranking Member's Request*, July 10, 2020, on file with the Committee.
[196] *Id.*
[197] *Id.*
[198] *Id.*
[199] *Id.*
[200] *Id.*
[201] The Federal Risk and Authorization Management Program, FedRAMP, *About Us*, https://www.fedramp.gov/about/.
[202] Kathleen Kraninger, Director, Consumer Financial Protection Bureau, *CFPB response to House Committee on Financial Services Ranking Member's Request*, July 10, 2020, on file with the Committee.

platform, which in conjunction with other Microsoft Office 365 services, improves internal collaboration through instant messaging, video/audio conferencing, and OneDrive file sharing.[203]

The CFPB intends to further implement full group collaboration features and the Microsoft Teams iPhone app to support staff outside its Washington, D.C. headquarters. The CFPB will continue to use Microsoft Teams to maintain productivity as it transitions to a reentry posture from remote working.[204]

The Director recognizes the challenges associated with exercising oversight of financial institutions while working remotely due to COVID-19.[205] CFPB examiners are conducting supervisory activities at home, using all available digital and technological teleworking tools for completing exams, as they receive and review documentation from financial institutions electronically.[206] The CFPB has developed a "Prioritized Assessment" consisting of high-level inquiries designed to obtain information from financial institutions for assessing and identifying potential risks associated with COVID-19 on consumer financial products.[207] These assessments will reduce the burden on financial institutions associated with examinations and allow examiners to continue to work remotely.[208]

Finally, the CFPB's Enforcement staff continue to work remotely and have developed new teleworking processes and systems, including new procedures for receiving productions from financial institutions and for conducting investigations through video and phone conferences.[209] CFPB Enforcement continues to coordinate with Federal and State regulators to monitor and identify violations, and the Director states that their role has not diminished due to the new challenges caused by the pandemic.[210]

Conclusion

It is clear cybercriminals are attempting to leverage the environment created by the pandemic. Unprecedented levels of remote work in the public and private sectors, increased digital interactions between consumers and financial institutions, and increased interactions between financial institutions and regulatory agencies have combined to create opportunities for malicious actors. The experiences of the nation's largest financial institutions and the federal regulators they interact with bear this out—they respectively confirmed to the Committee that cyberattacks and other malicious cyberactivity have increased since March 2020.

As the federal government prepares to disburse additional relief funds, financial institutions are well equipped to deal with these acute challenges. Pre-pandemic investments in IT upgrades and modernization initiatives are paying off now. The lessons learned in this environment position those entities to prepare for a permanent transition to increased remote

[203] *Id.*
[204] *Id.*
[205] *Id.*
[206] *Id.*
[207] *Id.*
[208] *Id.*
[209] *Id.*
[210] *Id.*

work and more frequent digital interactions. Indeed, the current environment represents an opportunity for public and private sector entities to plan and develop a stronger, more modern cybersecurity infrastructure—investments in cybersecurity, consumer protection, and remote work capabilities now are likely to pay dividends as the threat environment evolves.

The supervisory relationship may also benefit by making strategies that were developed to deal with the COVID-19 pandemic more permanent. For example, regulators adapted their IT systems to accommodate remote examination processes. Several agencies cited cross-agency coordination as key to the successful transition to remote supervision. Regulators should continue working together to strengthen cybersecurity and implement new digitization guidelines for the supervisory relationship. Regulated entities should continue to be able to submit materials digitally, interact with regulators virtually, and complete examinations online.

Finally, Congress should prioritize issues related to cybersecurity and digitization. H.R. 4458 will require U.S. banking regulators to provide Congress with detailed analysis of their efforts to protect against cyberattacks. The Committee will begin receiving that information in the summer of 2021—it should form the basis for hearings and oversight initiatives throughout the 117th Congress. This will allow Congress to better understand how federal financial regulators and financial institutions are working to prevent weak links in the financial system from causing widespread problems. The extraordinary data breach that came to light in December 2020 made the stakes clear to government agencies and large corporations alike.

Recommendations

1. Regulators have linked cross-agency coordination with the success of the transition to remote supervision of the sector. Regulatory agencies should apply that coordinated model to strengthen cybersecurity and implement new digitization guidelines for the industry.

2. Public and private sector entities had no choice but to rely on existing software and IT solutions during the rapid transition to a remote work environment in March 2020. Those financial institutions and federal agencies that had previously invested in modernizing their IT infrastructures were best positioned to adapt to a remote work environment. The entire financial services community should use the current conditions to identify weaknesses and develop plans for a permanent remote work and virtual interaction environment.

3. Regulators should digitize operations to fully accommodate what may be a permanent transition toward virtual interactions between federal regulators and the firms they regulate.

4. In the interest of health and safety during the pendency of the pandemic, regulated entities should continue to submit materials to regulators digitally, interact with regulators virtually, and complete examinations online. There is no reason, however, that this more efficient arrangement should end when the pandemic does. Regulators should seek ways to permanently digitize their supervisory functions.