FINANCIAL SERVICES Information Sharing and Analysis Center

Testimony of Bill Nelson, President and CEO of the Financial Services Information Sharing and Analysis Center (FS-ISAC)

Committee on Banking, Housing and Urban Affairs
US Senate
May 24, 2018

Chairman Crapo, Ranking Member Brown and other members of the committee: Thank you for inviting me to testify at this hearing on "Cybersecurity: Risks to Financial Services Industry and Its Preparedness." My name is Bill Nelson and I am President and CEO of the Financial Services Information Sharing and Analysis Center (FS-ISAC), as well as Chairman of the Global Resilience Federation (GRF) for cross-sector threat-intelligence sharing.

At your request, I will cover the following topics:

- Current cyber-risks and threats that the financial-services industry faces;
- Efforts by the financial-services industry that are already underway in order to increase cyber-readiness, combat cyber-attacks and strengthen the industry from cyberthreats; and
- Proposed additional measures by public and private sectors to better protect companies' and consumer's information.

Before I describe these, I want to provide background about the role the FS-ISAC plays in the financial sector. Three key takeaways I would like to leave you with today:

- Despite a dynamic and ever-changing cyberthreat environment, the financial sector has invested heavily to protect the sector's assets and consumers' information from adversaries and cybercrime;
- The financial sector has collaborated effectively to enhance cyber-resilience; and
- The financial sector continues to benefit from strong public-private partnerships that enable cyberthreat intelligence to flow through the sector and improve sector detection, prevention and response to cyberthreats and other risks.

FS-ISAC: Information Sharing to Fight Cybercrime

FS-ISAC's mission is to help assure the resilience and continuity of the global financial-services infrastructure and individual firms against acts that could significantly impact the sector's ability to provide services critical to the orderly function of the economy. As such, FS-ISAC stands front and center in the face of continued cyber-attacks against our sector. FS-ISAC shares real-time threat and vulnerability information, conducts coordinated contingency planning exercises, manages rapid-response communications for cyber- and physical events, conducts education and training programs, and fosters collaboration with and among other key sectors and government agencies. Think of FS-ISAC as a "virtual neighborhood watch," where financial institutions help keep an eye out for each other.

FS-ISAC was formed in 1999 in response to Presidential Decision Directive 63 (PDD 63) of 1998, which called for the public and private sectors to work together to address cyberthreats to the nation's critical infrastructures. After the 9/11/2001 attacks, and in response to Homeland Security Presidential Directive 7 (and its 2013 successor, Presidential Policy Directive 21) and the Homeland Security Act, FS-ISAC expanded its role to encompass physical threats to the sector. FS-ISAC is a 501(c)(6) nonprofit organization and is funded by its member firms, sponsors and partners.

Rapid Growth Both Nationally and Globally

FS-ISAC has grown rapidly in recent years. Today, we have about 7,000 member organizations of all sizes, including commercial banks, credit unions, exchanges, brokerages and investment companies, insurance companies, payment processors and professionals, and trade associations. We also maintain close ties with other financial-industry trade associations as well as select, trusted Community Emergency Response Teams (CERTs) and Computer Security Incident Response Team (CSIRTs), law enforcement agencies, and other information-sharing initiatives around the world.

FS-ISAC is based in Reston, Va. Because today's cybercriminal activities transcend country borders, the FS-ISAC has expanded globally and has active members in 44 countries. FS-ISAC has more than 100 employees and consultants in eight countries across five continents.

Financial Firms Respond to a Dynamic Threat Environment

In many respects, the current threat environment feels like an "arms race," and the financial sector has done a lot to enhance its individual and collective capabilities. Each day, cyber-risk evolves as attacks increase in number, pace and complexity.

The financial sector has invested significantly to detect, prevent and respond to cyberthreats and other risks. Our member firms constantly adapt to this changing threat environment. At the same time, malicious cyber-actors, with increasing sophistication and persistence, continue to target the financial-services sector. These actors vary considerably, in terms of motivations and capabilities, from nation-states conducting corporate espionage or launching disruptive and even destructive attacks, to advanced cybercriminals seeking to steal money and hacktivists intent on making political statements.

The financial sector (in addition to other critical-infrastructure sectors) is increasingly concerned about the possibility of attacks that could potentially undermine the integrity of critical data, or lead to the manipulation or destruction of data. This growing threat affects all institutions in our sector, regardless of size or type of financial institution (e.g., bank, credit union, insurer, payment processer or brokerage/investment firm).

Tactics Used by Adversaries and Criminals to Target Financial Firms

There are numerous tactics that malicious cyber-actors use to target institutions, including the following:

- ***Targeted spear-phishing campaigns, which are*** fraudulent emails that appear to be legitimate. These emails trick users into supplying sensitive information such as passwords that can result in the theft of online credentials and fraudulent transactions.
- ***Destructive malware attacks*** that impact the confidentiality, integrity and availability of data.
- ***Ransomware attacks***, which involve malware that is downloaded and used to restrict access to an infected computer (often via encryption) until a ransom is paid (often in Bitcoin).
- ***Distributed-denial-of-service (DDoS) attacks,*** which can impede access to services for extended periods of time.
- ***Pretexting***, which is built on a false narrative and establishment of trust to ultimately initiate unauthorized activity such as wire transfers. One form of this type of scheme is known as a "business email compromise" attack.
- ***Data breaches*** which steal sensitive information including payment and account information.
- ***Supply chain threats***.
- ***Insider threats***.

Beyond Sharing: FS-ISAC and Financial Sector Resilience

Driven by the direction of our membership, FS-ISAC performs a number of key critical functions. We share threat and vulnerability information; conduct coordinated exercises; manage rapid-response communications for cyber- and physical events; produce education and training programs; and foster collaboration with other key sectors and government agencies. We have greatly expanded our products and services to members. In particular, we have devoted a large number of resources to expand our services and tailor them to smaller financial institutions and their service providers.

1. Information Sharing

FS-ISAC enables its members to voluntarily and efficiently share real-time threat and vulnerability information for cyber- and physical incidents. We delivery timely, relevant and actionable cyber- and physical threat information through email, web portal, telephone, and automated feed alerts from various trusted sources and our members. FS-ISAC maintains policies, procedures and controls to ensure that all threat information shared by members is properly gathered, stored, labeled and used in a manner that abides by related sharing agreements, privacy protections, circles of trust, member operating rules, regional requirements and governing laws.

FS-ISAC cooperates with members and partner organizations, including several public-private partnerships. These include facilitating information sharing from government partners to the FS-ISAC community and assisting members in engaging government and law enforcement members when required. For example, an FS-ISAC employee participates in the watch floor of the U.S. Department of Homeland Security's (DHS) National Cybersecurity and Communications Integration Center (NCCIC), playing an important role in our public-private sector information and analysis sharing.

The Basis for the Community: Circles of Trust

We support numerous "circles of trust" based on roles (e.g., chief information security officers, business continuity

executives, payments professionals, compliance experts) and institutions (e.g., asset managers, broker dealers, clearing houses, community banks, credit unions, payment processors). We host regular threat-information sharing conference calls for members and invite subject matter experts to discuss the latest threats, vulnerabilities and incidents affecting critical infrastructure. We organize and coordinate numerous regional member meetings, roundtables, workshops and other forums that allow face-to-face exchange between members.

Our largest trust circle – the Community Institution and Association Council -- includes thousands of community banks and credit unions that actively share information about threats, incidents and best practices. Since 2014, over 4,500 community institutions have joined FS-ISAC. Within this Council, member discussions and participation increased 24 percent in 2017. In the last 12 months, the FS-ISAC's industry-focused webinars on numerous topics, including protections against fraud, threat-intelligence methods and cybersecurity tools, were attended by nearly 20,000 attendees.

In addition, FS-ISAC works with numerous national and state-based financial and payments organizations, including the American Bankers Association (ABA), Financial Services Roundtable (FSR), Credit Union National Association (CUNA), Independent Community Bankers of America (ICBA), National Automated Clearing House Association (NACHA) and Securities Industry & Financial Markets Association (SIFMA), as well as card payment associations, payment processors and state banking associations.

2. Creating and Invoking Playbooks for Incident Response

FS-ISAC maintains the financial-services sector's "All Hazards Crisis Response Playbook," which outlines the processes and considerations for identifying and responding to significant threats or events. As an example of sector-wide collaboration, this playbook was developed in conjunction with many of our members and other industry associations. We also lead sector-level crisis-response coordination and manage the Critical Infrastructure Notification System (CINS) for emergency threat or incident notifications to members.

Reducing Fear, Uncertainty, Doubt Through Media Response

FS-ISAC seeks to reduce fear, uncertainty and doubt through sector-level responses on significant cyber- and physical events. The FS-ISAC Media Response Team was established in 2014, following highly visible cyberattacks that impacted the financial-services sector and other sectors like retail that were broadly reported in the press. The Team's mission is to accurately assess the actual current and potential risk of cybersecurity events (as opposed to the potential media "hype" commonly seen) and leverage the FS-ISAC brand to properly respond to media activity using a fact-based approach. The team also strives to educate reporters and the public about cybersecurity and financial-sector practices, concepts and terminology.

3. Always Ready: Cyber-Exercises and Incident Response

Exercises are a proactive step to practice plans, find and close gaps, and better protect systems and communities. FS-ISAC began conducting exercises in 2010 with the Cyber-Attack Against Payments Systems (CAPS) exercises. FS-ISAC has since added exercises, such as drills, to test the All-Hazards Crisis Response Playbook as well as regional exercises. In 2014, we launched the "Hamilton Series" of exercises in collaboration with the U.S. Treasury Department and the Financial Services Sector Coordinating Council (FSSCC). These exercises simulate a variety of plausible cybersecurity incidents or attacks to better prepare the financial sector and the public sector for cyberattacks. They also aim to improve public- and private-sector policies, procedures and response capabilities. The "Hamilton Series" has included leaders from the U.S. Treasury Department, financial regulatory bodies, the Department of Homeland Security and law enforcement agencies. Starting in 2018, FS-ISAC added range-based cyber-exercises for more technical, hands-on-keyboard experiences to raise capability maturity levels and resiliency across the sector. Collectively, these efforts build on the strong risk-management culture within the financial-services sector, in conjunction with extensive regulatory requirements.

FS-ISAC has improved its ability to respond to major cyber- and physical events, including emergency member calls regarding new vulnerabilities and threats. The last call we had had over 3,000 participants.

4. Support for the FSSCC, Sheltered Harbor, FSARC, Regional Coalitions and Other Sectors

FS-ISAC supports several programs, either through direct funding or through subsidiary arrangements. These are outlined below.

Addressing Policy Issues: The Financial Services Sector Coordinating Council (FSSCC)

The FSSCC was established in 2002 to coordinate the development of critical-infrastructure strategies and initiatives with its financial-services members, trade associations and other industry sectors. The FSSCC works with the public sector on policy issues concerning the resilience of the sector. Members include 70 financial trade associations, financial utilities and critical-infrastructure financial firms.

FS-ISAC serves as the operational arm of FSSCC, providing operational support of FSSCC-initiatives. The FS-ISAC and FSSCC have built and maintained relationships with the U.S. Treasury and Homeland Security Departments, all the federal financial regulatory agencies (e.g., Federal Deposit Insurance Corp., Federal Reserve Board of Governors, Federal Reserve Banks, Office of the Comptroller of the Currency, Securities and Exchange Commission), and law enforcement agencies (e.g., Federal Bureau of Investigation, U.S. Secret Service). Many of these public-sector agencies are part of the FSSCC's public-sector counterpart, the Financial and Banking Information Infrastructure Committee (FBIIC), which is chaired by the U.S. Treasury Department.

An Extra Layer of Security for Consumer Accounts: Sheltered Harbor

Sheltered Harbor was established in 2016 as an LLC, operating under FS-ISAC's umbrella, to enhance the financial-services industry's resiliency capabilities in the event of a major disaster or event. The concept for Sheltered Harbor arose in 2015 during a series of successful cybersecurity simulation exercises between public and private sectors known as the "Hamilton Series."

Sheltered Harbor is based on industry-established standards and the concept of mutual assistance. Should a financial institution be unable to recover from a cyber-attack in a timely fashion, firms that adhere to the Sheltered Harbor standards will enable customers to access their accounts and balances from another service provider or financial institution. Sheltered Harbor members access specifications for common data formats, secure storage ("data vaults") and operating processes to store and restore data and receive a Sheltered Harbor acknowledgement of adherence to the specification. As of April 2018, Sheltered Harbor membership covers more than 69 percent of U.S. retail bank deposit accounts and 56 percent of U.S. retail brokerage client assets.

Systemic Risk Reduction: Financial Systemic Analysis and Resilience Center (FSARC)

The CEOs of eight U.S. Government designated critical infrastructure firms – Bank of America, BNY Mellon, Citigroup, Goldman Sachs, JPMorgan Chase, Morgan Stanley, State Street and Wells Fargo – came together to proactively identify ways to enhance the resilience of critical infrastructure underpinning the U.S. financial system. The result was the creation of the FSARC as a subsidiary of the FS-ISAC. Shortly after the FSARC was founded, an additional eight financial institutions, including the key financial market utilities identified by the U.S. Department of Homeland Security as operators of essential critical infrastructure, joined the FSARC as member firms.

The FSARC's mission is to proactively identify, analyze, assess and coordinate activities to mitigate systemic risk to the U.S. financial system from current and emerging cybersecurity threats. This is accomplished through focused operations and enhanced collaboration between participating firms, industry and government partners. Key FSARC functions include:

1) Identifying operational risks associated with systemically relevant business processes, functions and technologies underpinning the financial sector (collectively "Identified Systemic Assets");
2) Developing resiliency plans to address those risks;
3) Working with critical-infrastructure operators and the U.S. Department of Homeland Security, intelligence and defense communities to deliver strategic early warnings of attack on Identified Systemic Assets;

4) Working with law enforcement agencies to disrupt sophisticated malicious actors that may pose a systemic risk to the sector over time or may be targeting Identified Systemic Assets.

Thinking Nationally, Acting Locally: Regional Coalitions.

Financial institutions in more than a dozen areas participate in the "FIRST" (Fostering Industry Resilience and Security through Teamwork) movement through the formation of public-private partnerships focused on Homeland security and emergency management issues with the public sector. Each coalition provides the opportunity for members to collaborate with one another and with government at all levels about issues of resilience and security.

FS-ISAC has established regional coalitions in the Northeast (Connecticut, Maine, Massachusetts, New Hampshire, New Jersey, New York, Rhode Island and Vermont), Mid-Atlantic (District of Columbia, Delaware, Maryland and Northern Virginia) and California (San Francisco, Fresno and Los Angeles). Through regional coalitions, FS-ISAC learns the ground truth about the local effects of crises, while the coalitions obtain national-level crisis and threat information from FS-ISAC. FS-ISAC also supports RPCfirst, an umbrella organization for all of the regional coalitions across the nation.

Cross-Sector Collaboration and Sharing

The FS-ISAC collaborates with other sectors, including the National Council of ISACs (NCI). Formed in 2003, the NCI today comprises 24 organizations designated as their sectors' information sharing and operational arms.

Last year, the FS-ISAC spun off its Sector Services division into a new standalone, not-for-profit called the Global Resilience Federation. I serve as the chairman of GRF, which is an information-sharing hub and intelligence provider. GRF develops and distributes cyber-, physical and geo-political security information among not-for-profit ISACs, ISAOs, CERTs and other information sharing communities across vital sectors around the world. The company assists in the creation and operation of ISACs and ISAOs, or, if requested, support for the expansion of existing communities. This "community of communities" was founded by charter members -- FS-ISAC, Legal Services Information Sharing and Analysis Organization (LS-ISAO) and Energy Analytic Security Exchange (EASE) -- and has since been joined by National Health ISAC, Oil and Natural Gas ISAC, Multi-State ISAC, Retail Cyber Intelligence Sharing Center and National Retail Federation. As a cross-sector hub that also works with government and industry partners, GRF facilitates and supports cross-sector intelligence sharing as well as collaboration.

Regulatory Requirements and Risk Management Culture

The financial sector has historically led the way in making substantial investments in not only security infrastructure and highly qualified experts to maintain the systems, but also in driving collaboration across industries and with the government. Financial institutions recognize that customers trust them to protect their investments, their records and their information. Individual financial institutions invest in personnel, infrastructure, services and top-of-the-line security solutions and protocols to protect their customers and themselves, and to respond to cyber-attacks. These investments protect the individual institutions and their customers, but on its own, an individual institution generally only has the ability to protect what is within its control. Financial institutions, however, are interconnected to each other, with other sectors and with the government. This reliance on others gives the financial-services sector a unique and critical role in the cyber-landscape and requires coordinated action for the most effective response. Recognizing the cyberthreat environment continues to expand in complexity and frequency, and that individual institution efforts alone will not be enough, executives from the financial-services sector have stepped up efforts to work together.

Cybersecurity Practices Often Burdened by Regulation and Supervisory Oversight

Financial institutions are subject to comprehensive regulations and supervisory requirements with respect to cybersecurity and the protection of sensitive customer information as well as business resiliency. For example, Title V of the Gramm-Leach-Bliley Act of 1999 (GLBA) directed regulators to establish standards for financial institutions to protect customer information. Pursuant to GLBA, regulators have imposed broad information security requirements for regulated financial institutions with strong enforcement authority. In addition to issuing regulations almost two decades ago, the federal financial

regulators have issued extensive "supervisory guidance" through the Federal Financial Institutions Examination Council (FFIEC) that outlines the expectations and requirements for all aspects of information-security and technology-risk issues, including authentication, business continuity planning, payments and vendor management." Among the obligations to secure systems and protect data under GLBA and supervisory guidance, financial institutions must:

- Develop and maintain an effective information-security program tailored to the complexity of their operations;
- Conduct thorough assessments of the security risks to customer information systems.
- Oversee service providers with access to customer information, including requiring service providers to protect the security and confidentiality of information;
- Train staff to prepare and implement information-security programs;
- Test key controls, systems and procedures, and adjust key controls and security programs to reflect ongoing risk assessments;
- Safeguard the proper disposal of customer information; and
- Update systems and procedures by taking business changes into account.

Many Regulations and Standards with Which to Comply

Financial institutions must comply with cybersecurity requirements and guidance from numerous regulatory bodies depending on their charter and activities. What's more, depending on the type of financial institution, organizations may have additional compliance and non-regulatory standards; for example, institutions that handle payment information also are required to comply with non-regulatory standards, such as the Payment Card Industry Data Security Standard (PCI-DSS). This adds to the compliance burden of financial institutions. as well as that of merchants and other organizations that handle payment information.

Most recently, the FFIEC issued the Cybersecurity Assessment Tool (CAT) – an assessment tool designed to help smaller institutions, in particular, identify their risks and determine their cybersecurity preparedness. The CAT provides a repeatable and measurable process for financial institutions to measure their cybersecurity preparedness over time and aligns with the NIST's Cybersecurity Framework. In 2016, the FS-ISAC and FSSCC leveraged the FFIEC's CAT to produce a "crowd-sourced" version that incorporated automation to assist financial institutions in utilizing the FFIEC document.

Recommendations to Further Protect Financial Institutions and Customers

Finally, you asked me to describe what more needs to be done by the private sector and the government to help protect companies' and consumers' information. For many years the financial sector has been working diligently and collaboratively to make significant improvements in five major areas:

- Enhance Information Sharing
- Improve Strategic and Tactical Analytics
- Improve Crisis Management Response and Coordination
- Improve Core Components of the Cyber-Ecosystem through R&D
- Improve Executive Communication and Advocacy

The financial-services sector has made significant progress in all of these. In so doing, the financial sector has developed strong collaborative relationships with numerous government agencies (including law enforcement, DHS, Treasury and U.S. regulatory agencies). These efforts have enhanced the resiliency of the financial-services sector. We also have worked closely with other "critical infrastructure" sectors (e.g., telecommunications, energy) to enhance their capabilities and to address interdependencies.

While we are making good progress, much more work needs to be done. The following are four major recommendations. Some of these recommendations were developed in collaboration with the Financial Services Sector Coordinating Council (FSSCC) and publicly released in early 2017.

Encourage Regulators to Harmonize Cyber-Regulatory Requirements.

Given that financial institutions are subject to numerous regulatory and supervisory requirements with respect to cybersecurity, protection of sensitive customer information, business resiliency, penetration testing, vendor management, etc., there is little need for additional regulation in this space. Instead, there is a need to reduce the burden of implementing regulations for financial firms. What the sector most needs now is a focused and coordinated effort among state, federal and global regulators to harmonize regulatory requirements. In so doing, this is a good opportunity to leverage the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

While regulatory requirements are a powerful and effective way to ensure that financial institutions have adequate controls in place, a growing challenge facing large and global financial institutions today is the need for greater coordination and harmonization among the regulatory agencies, within the U.S. and globally. This will help financial firms keep pace with new threats, new financial business process models, and the necessary skillsets to evaluate the intersection of those two for security and resiliency purposes. A common refrain we hear from senior executives and practitioners in large and global firms is the need for regulators to harmonize regulatory requirements at both the policy and examination levels to reduce unnecessary regulatory compliance burdens and to better focus limited resources to mitigate cyber-risks. In addition, it would help if the U.S. Congress and Administration enacted a consistent and strong data protection and breach notification law across state and national platforms.

Related to this recommendation to harmonize regulatory requirements, we also encourage Congress and regulatory rulemaking bodies to integrate cyber-risk assessment into the legislation and rule-making processes. Hence, Congress and regulatory rulemaking bodies should weigh the implications of concentrating sensitive data that will create new cyber-targets when evaluating potential legislation and rulemaking. The potential aggregation of personally identifiable information via the SEC Rule 613 Consolidated Audit Trail or retrieving highly sensitive penetration testing and vulnerability data on regulated institutions are examples of situations where care should be taken to avoid creating new risks and creative solutions should be sought collaboratively with industry.

Leverage Authorities in the Cybersecurity Information Sharing Act of 2015 (CISA) and USA Patriot Act of 2001 to Implement More Effective Information Sharing Programs.

FS-ISAC and others in the financial sector supported the enactment of the Cybersecurity Information Sharing Act of 2015 (CISA). CISA encourages sharing for a cybersecurity purpose and includes incentives to entice entities to share information, including protection from liability claims, exemption from disclosure laws and regulatory use, and antitrust exemption. CISA enables sharing of information including: malicious reconnaissance, methods to defeat controls or exploit vulnerabilities, security vulnerabilities, malicious cybercommand and control, exfiltration of data and other attributes related to cyberthreats. Mandated by the Cybersecurity Act of 2015, the Department of Homeland Security (DHS) developed a system to automate the sharing of threat indicators on a machine to machine basis. This system is called Automated Indicator Sharing or AIS and was put into service in 2016; it is free to use.

AIS leverages two internationally recognized standards for sharing: One is the data standard called Structure Threat Information Expression (STIX™) and the other is the delivery standard known as Trusted Automated eXchange of Indicator Information (TAXII™). Threat indicators include data like malicious IP addresses, email addresses associated with ransomware, phishing or social engineering attacks, known cybercriminal campaign information and much more.

Representing its members, the FS-ISAC agreed to participate in the Automated Indicator Sharing (AIS) program on a trial basis in 2016. We have engaged in numerous collaborative technical discussions with DHS and Treasury concerning the AIS program over the past two years.

FS-ISAC and member firms have provided direct and consistent feedback to DHS regarding the early implementations of the AIS program. This feedback includes the need for DHS to strongly structure vetting of AIS participants, the need to verify the integrity of data transmitted and received within AIS, and the importance of providing context around the information. DHS has indicated it has heard the financial sector's feedback and is taking steps to incorporate that feedback and has

recently committed to delivering on improvements that add context to indicators, includes rated scoring of vetted sources, utilizes the latest version of STIX/TAXII standards, and ability for AIS recipients to screen sources and receive data only from sources that each recipient approves.

We also encourage our U.S. government partners to improve response time and the quality of shared information and analysis and to prioritize essential "lifeline" sectors in planning and event response. Focus federal resources to assist those sectors whose operation is fundamental to the national defense and economy, such as financial services, electric power and telecommunications, to mitigate against cyberthreats and to help in recovery. Continued private-public collaboration is required to develop the list of cyber-defense capabilities that can be used to respond to a significant cyber-incident affecting the nation's critical infrastructure. Ensure that the relevant members of the lifeline sectors receive the appropriate security clearances. Also, seek improvements in sharing classified information, passing clearances and collaborating with the private sector in a classified environment. Together with the communications sector and the electricity subsector, FS-ISAC led the development of a playbook for lifeline sectors, completed earlier this year. We began drilling it during Cyber Storm and the National Level Exercise and plan a Hamilton Series tri-sector exercise for it in the fall. One of the next steps involves expanding the lifeline sectors for which it would be applicable. Another is ensuring that the tri-sector playbook connects with plans the federal government would use during a significant incident. The U.S. Departments of Treasury, Homeland Security and Energy have seen the playbook, though further government socialization and coordination remains.

In addition, we encourage the U.S. government to invest further in financial services-supporting infrastructure and risk-based cyber R&D. To ensure strong investment in the cybersecurity and resiliency of key federal organizations, processes and systems essential to the functioning to the financial services system, it's important for the US Government to assign clear responsibilities and increase significantly resourcing for efforts to detect, analyze and mitigate cyber threats to the financial system. This includes a dedicated effort within the Intelligence Community and an operational-level contingency planning, indications/warnings, and exercises program. It's important to fund cybersecurity defense and R&D initiatives commensurate with the risk that cybersecurity threats pose to the nation's security, including funding to identify risks and mitigation techniques for emerging Internet of Things (IoT) and quantum computing technologies.

Finally, we encourage the Financial Crimes Enforcement Network (FinCEN) to provide greater clarity on legal protections for financial institutions that want to share information in accordance with the USA Patriot Act. On November 30, 2016, FinCEN participated in a FS-ISAC-sponsored webinar about information sharing on suspected money laundering. This interaction helped anti-money laundering (AML)-regulated financial institutions better understand FinCEN's views of the potential risk mitigation opportunities available by sharing information about suspected money laundering under section 314(b) of the USA Patriot Act. Since the webinar, many of the financial institution executives who participated in the webinar, which was open to all AML-regulated financial institutions, have asked for written confirmation of the information that FinCEN officials provided verbally. Financial institutions indicated that written confirmation is necessary to encourage financial institutions to leverage the authority provided under section 314(b) of the USA Patriot Act. If FinCEN provides written guidance about what suspected money laundering and terrorist financing information can be shared with an association of approved financial associations under the USA Patriot Act Section 314(b), then financial institutions that are members of an approved 314(b) sharing information association would file Suspicious Activity Reports (SARS) with more actionable information. In turn this might enhance the U.S. government's efforts to investigate, extradite and prosecute transnational cyber criminals.

FS-ISAC provided a list of six questions and our understanding of the answers to FinCEN on numerous occasions and is still waiting for a response. FS-ISAC would like to request that FinCEN publicize the answers so financial institutions can reference these answers. This would provide financial institution executives with much needed assurances of FinCEN's views and thus encourage greater information sharing about suspected money laundering by financial institutions pursuant to section 314(b) and other U.S. laws that authorizing the sharing of suspected money laundering and suspected terrorist financing.

Establish Cyberdeterrence and Response Capabilities and Encourage Adoption of Global Cybernorms

The Congress and Administration should articulate how the U.S. government will respond to certain types of attacks and how these actions might impact the financial-services sector and other critical infrastructure sectors. The US government should also increase efforts to extradite and prosecute cyber criminals. Attacks on the financial services industry and critical infrastructure should be considered a violation of an explicit global norm; violations of this norm should be pursued vigorously. The US Government should also enable and expand cross-sector, real-time and actionable cyber threat information sharing and situational awareness. The US government should also continue to engage with the global community to develop and adopt international norms of behavior that discourage targeting of financial institutions and other critical-infrastructure sectors.

Support Efforts to Develop a Technology-Capable Workforce

The US government should partner with the private sector and academia to develop education and training programs to meet the business needs of today and tomorrow in addressing the significant shortage of cybersecurity professionals and the education system in producing enough skilled cybersecurity professionals.

CONCLUSION

The financial sector has made a significant investment in cybersecurity, risk reduction and resilience. However, threats, vulnerabilities and incidents affecting the sector continue to evolve. Individual firms have responded by making significant investments in technology and risk reduction improvements at their respective companies. Collectively, the sector has made improvements in information sharing and made strides in focusing on systemic risk, mutual assistance, enhanced resiliency and consumer protection. While more needs to be done, including additional collaboration with government and global partners, the financial sector is making good progress and on balance has invested heavily to protect the sector's assets and consumers' information from adversaries and cybercrime.