Institute for SECURITY + TECHNOLOGY

securityandtechnology.org

Testimony of

Megan H. Stifel
Chief Strategy Officer
Executive Director, Ransomware Task Force
Institute for Security and Technology

Before the Committee on Financial Services

Subcommittee on National Security, Illicit Finance, and International Financial Institutions

U.S. House of Representatives

On

Held for Ransom: How Ransomware Endangers Our Financial System

April 16, 2024

Chairman Luetkemeyer, Ranking Member Beatty, distinguished members of the subcommittee, thank you for the opportunity to appear before you today to address how ransomware is impacting our financial system. My name is Megan Stifel, and I serve as the Chief Strategy Officer at the Institute for Security and Technology, or IST. IST is a 501(c)(3) non-profit organization dedicated to outpacing emerging security risks by bridging the gap between technologists and policy makers. Prior to joining IST, I worked in policy roles at other non-profits, a sector I joined after I left federal service. I am a proud daughter of bankers; my father worked at a regional bank for over 40 years. Watching him help the bank manage risk and serve his community and customers has had a significant impact on my outlook on life. My mother was a non-profit leader, but before that she too worked for a bank.

Despite my front-row seat to the banking sector, I did not pursue a career in finance. I am a national security law and policy practitioner, a field I have been working in since 1999 when I joined the staff of the then House Permanent Select Committee on Intelligence. I left Washington to attend law school, resolved that I would return to pursue a career in national security. I was fortunate to have had the opportunity to do so at the Department of Justice, where I served in the National Security Division's Office of Intelligence and the Office of Law and Policy, and in the Computer Crime and Intellectual Property Section of the Criminal Division. I also served on detail to the National Security Council, where I helped develop and implement interagency policy efforts on cybersecurity and cybercrime. I departed federal service almost 10 years ago, but my commitment to our nation's national security has remained my highest professional priority and I am grateful to continue to support it in my role at IST.

IST's work falls in three core areas: the Geopolitics of Technology, where we are exploring how to realign incentive structures in the United States and allied nations to advance in the global techno-industrial competition; Innovation and Catastrophic Risk, where we examine how to harness innovation to increase stability; and most relevant for today's discussion, the Future of Digital Security, where we work to identify how to build trust, safety, and security into digital technologies from the ground up and manage existing risks from technologies that fail to do so.

In late 2020, in response to the growing threat posed by the escalating rise in ransomware incidents targeting critical infrastructure, IST convened the Ransomware Task Force, of which I had the privilege of serving as a co-chair. When I joined IST in late 2021, I became the Task Force's Executive Director. The Ransomware Task Force includes participants from industry, academia, civil society, and governments, including the United States, the United Kingdom, and Canada, as well as multilateral organizations such as Europol. In total, 60 plus organizations participated, including organizations represented by my fellow witnesses. In a span of four months, this coalition of stakeholders convened in four working groups and examined measures to help better deter, disrupt, prepare, and respond to ransomware.

In April 2021—three years ago this month-–we published a report outlining key actions identified by the Ransomware Task Force, organized around four overarching goals. The report detailed five priority recommendations with a series of supporting actions, constituting 48 total recommendations. The priority recommendations included the following:

1. The need for sustained, coordinated collective action, led by the United States, among governments, industry, academia, and nonprofits to meaningfully reduce the ransomware threat;
2. An intelligence-driven anti-ransomware campaign, coordinated by the White House, including the capability necessary to support operational collaboration with industry;
3. The establishment of ransomware response and recovery funds;
4. A framework for preparation, and mandated reporting of ransom payments; and
5. Closer regulation of the cryptocurrency sector due to its role in ransomware payments and resourcing, including through compliance with existing tools designed to reduce illicit payments, e.g., Know Your Customer, Anti-Money Laundering, and Combating Financing of Terrorism rules and regulations.

Ransomware attacks affect the financial services sector as they affect all of our critical infrastructure sectors, disrupting the provision of essential services and costing the industry millions. Ransomware and the financial services sector have a further relationship as well, because cryptocurrency is the lifeblood of this criminal industry, enabling attackers to get paid and to move money around to their various partners and affiliates.

The Ransomware Task Force made a number of recommendations, 12 in total, in connection with the financial services sector, many of which relate to ransom payments and cryptocurrency:

Relevant RTF Action	***Description of RTF Action***	***Status***
Action 2.1.1	Develop new levers for voluntary sharing of cryptocurrency payment indicators	Some progress
Action 2.1.2	Require cryptocurrency exchanges, crypto kiosks, and over-the-counter (OTC) trading “desks” to comply with existing laws	Significant progress
Action 2.1.3	Incentivize voluntary information sharing between cryptocurrency entities and law enforcement	Some progress
Action 2.1.4	Centralize expertise in cryptocurrency seizure, and scale criminal seizure processes	Significant progress
Action 2.1.5	Improve civil recovery and asset forfeiture processes by kickstarting insurer subrogation	Some progress
Action 2.1.6	Launch a public campaign tying ransomware tips to existing anti-money laundering whistleblower award programs	Significant progress
Action 2.1.7	Establish an insurance-sector consortium to share ransomware loss data and accelerate best practices around insurance underwriting and risk management	Some progress

Action 2.3.3	Apply strategies for combating organized crime syndicates to counter ransomware developers, criminal affiliates, and supporting payment distribution infrastructure	Significant progress
Action 4.1.4	Clarify U.S. Treasury guidance regarding ransomware payments	Some progress
Action 4.2.4	Require organizations and incident response entities to share ransomware payment information with a national government prior to payment	Some progress
Action 4.3.1	Require organizations to review alternatives before making payments	No progress
Action 4.3.2	Require organizations to conduct a cost-benefit assessment prior to making a ransom payment	No progress

Just days after the report's publication, several high profile ransomware attacks occurred, leading to the disruption of fuel and meat distribution, as well as the delivery of healthcare. While these were not the first incidents to target critical infrastructure, reflecting on them three years on, it is clear that together they formed a pivotal moment. Since these incidents, significant progress has been made in countering ransomware. Much of the progress aligns with the Task Force's recommendations. And yet much more work remains. In my testimony I will outline several areas for ongoing action, and I invite the audience to visit our website to learn more about other ongoing efforts of the Ransomware Task Force's work that I will not have time to address today.[1]

Following these incidents, Congress and the Biden Administration recognized that ransomware posed an increasing national security threat, and responded. To name but a few of these actions, Congress and the Executive branch created cyber incident and ransomware payment reporting requirements, cyber incident emergency response authorities, the Joint Ransomware Task Force, a Ransomware Vulnerability Warning Pilot, and the State and Local Cybersecurity Grant Program for states and organizations. It also centralized expertise in cryptocurrency seizure, and has begun applying a range of strategies to combat the Ransomware as a Service business model, including through the Rewards for Justice program.

In a May 2023 Progress Report on the status of Ransomware Task Force recommendations since 2021, we found that 50% of the RTF recommendations (24 of the 48) have seen significant progress through legislation and policy adoption. However, the other half have seen either no known action or only preliminary known action. Next week we will publish our latest progress report. Without creating too much of a spoiler, I can share that we have not seen

[1] For more information, please see: Ransomware Task Force, Institute for Security and Technology, https://securityandtechnology.org/ransomwaretaskforce/.

further progress on the remaining 24 recommendations. With respect to the 12 financial services related recommendations, our assessment is that of the 12, four have seen significant progress, while eight have seen little or no known progress.

This is no time for stalled progress, as the stakes keep getting higher: my fellow witnesses will outline the current state of ransomware, but to summarize briefly: last year, according to Chainalysis and corroborated by the FBI's reporting, ransomware payments exceeded one billion dollars.[2] In 2021, the average ransomware payment was $312,493; in the first half of 2023, it was $1.54 million.[3] The FBI has observed an 18% increase in ransomware incidents from 2022, with adjusted losses of almost $60 million.[4] The IC3 also noted that they received 1,193 reports of a ransomware incident from critical infrastructure organizations, a 37% increase from 870 reports in 2022.[5] Frustratingly, the majority of ransomware attacks continue to leverage known vulnerabilities, often referred to as n-days, where patches are available, but have not been adopted. However, attackers have also started to exploit zero day vulnerabilities with increasing frequency—an even more troubling prospect.[6] It is clear that attackers' tactics have evolved, some assert in response to defensive and disruptive progress.[7] Today, organizations regularly confront not just encryption of their data, but also threats to release organizational and customer sensitive data, together with increasing physical threats to their employees and their families. As a result, there remains an ongoing, urgent need for concerted action by Congress, the Administration, the American people, and our partners and allies in order to defeat ransomware.

Cognizant of this urgency, today my testimony will focus on three ways to reduce the risk and impacts of ransomware on the financial services sector. First, financial sector resilience is essential to maintaining our roles as the world's financial leader. Second—and a corollary to resilience—-we must ensure that the federal, state, and local government entities that underpin our role as the world's financial hub have adequate resources to investigate abuse of our

---

[2] Chainalysis, "Ransomware Payments Exceed $1 Billion in 2023, Hitting Record High After 2022 Decline," February 29, 2024, https://www.chainalysis.com/blog/ransomware-2024/; Federal Bureau of Investigation Internet Crime Complaint Center, *2023 Internet Crime Report*, March 6, 2024, https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf.

[3] Sophos, "The State of Ransomware 2023," May 2023, https://assets.sophos.com/X24WTUEQ/at/h48bjq7fqnqp3n5thwxtg4q/sophos-the-state-ransomware-2023-infographic-1200-1200px_2x.png.

[4] Federal Bureau of Investigation Internet Crime Complaint Center, *2023 Internet Crime Report*.

[5] Federal Bureau of Investigation Internet Crime Complaint Center, *2022 Internet Crime Repor*t, March 10, 2023, https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf; Federal Bureau of Investigation, *2023 Internet Crime Report*.

[6] Zero days are unknown security vulnerabilities or software flaws that a threat actor can target with malicious code. A Zero-Day Exploit is the technique or tactic a malicious actor uses to leverage the vulnerability to attack a system. A Zero-Day Attack occurs when a hacker releases malware to exploit the software vulnerability before the software developer has issued a patch for the flaw. https://www.crowdstrike.com/cybersecurity-101/zero-day-exploit/

[7] Coveware, "Improved Security and Backups Result in Record Low Number of Ransomware Payments," January 20, 2023, https://www.coveware.com/blog/2023/1/19/improved-security-and-backups-result-in-record-low-number-of-ransomware-payments.

services. Third, the financial services sector has tremendous reach and can play an even greater role in helping raise our collective defenses.

Financial Services Sector Resilience Is Critical

First, the United States is the world's global economic hub and the dollar is the world's primary reserve currency. To retain this position we must not only evolve our legal, policy, and regulatory frameworks to advance innovation, we must also ensure that our financial services sector is resilient. As noted in our initial Task Force report, data around ransomware incidents remains unclear. There is, however, general consensus among the community that the number of incidents is likely an undercount. In addition to suspicious activity reports and reports to the FBI's Internet Crime Complaint Center (IC3), another source of incident data are leak sites, where ransomware gangs threaten and post data about victims. Analysis of leak site data by the Financial Services Information Sharing and Analysis Center (FS-ISAC) indicates that in 2023, financial services and insurance were the fourth most targeted sectors.[8] They further observe that experienced cyber teams are often able to withstand the attack itself, but struggle to restart operations, which erodes customer trust.

Troublingly, in 2023, ransomware threat actors exploited zero day vulnerabilities with increasing frequency. The evolution of adversary tactics to encryption-less ransomware also adds to this dark picture. This extortionware trend threatens not to lock up networks but instead to expose a range of compromised data, which can jeopardize personal privacy and intellectual property. When combined with the ongoing exploitation of unpatched or under-defended systems, it is clear that adequate staffing and training must remain top priority throughout the ecosystem.

These trends are particularly troubling for smaller institutions, which are often resource constrained and unable to adequately invest in cybersecurity.[9] A 2023 survey by Sophos observed a significant rise in the rate of ransomware attacks against financial institutions, from 34% in 2021 to 64% in 2023.[10] The same survey found that 40% of the most significant attacks in the financial sector were the result of an exploited vulnerability—such as software that could have been patched but may not have been due to resource constraints.[11]

These figures reflect two related challenges all organizations confront in achieving resilience, including against ransomware. Many organizations lack sufficient capital to tackle these challenges, let alone market recognition that they are a problem. First, as a result of policy decisions made decades ago, the market remains riddled with products running on insecure software. To address this challenge, organizations developing software need to implement vulnerability disclosure and patching programs. At the same time, organizations running the

[8] FS-ISAC, Inc., "Navigating Cyber 2024," March 2024, https://www.fsisac.com/navigatingcyber2024.
[9] Gogolin, Fabian and Lim, Ivan and Vallascas, Francesco, Cyberattacks on Small Banks and the Impact on Local Banking Markets (April 8, 2021), at 2-3. Available at SSRN: https://ssrn.com/abstract=3823296 or http://dx.doi.org/10.2139/ssrn.3823296.
[10] Puja Mahendru, "The State of Ransomware in Financial Services 2023," Sophos News, July 10, 2023, https://news.sophos.com/en-us/2023/07/13/the-state-of-ransomware-in-financial-services-2023/.
[11] Mahendru, "The State of Ransomware in Financial Services 2023."

vulnerable software need to pay attention to patches and implement a patching program that takes a risk-based approach to patching the most critical software to them first. They can use the Known Exploited Vulnerabilities Catalog maintained by CISA to do so.[12]

Additionally, companies leveraging technology need to drive towards resilience through shifting security left in their development cycles, including by moving to secure by design and secure by default approaches.[13] As the Chair and Deputy Chair of the Cyber Safety Review Board recently observed: "All technology companies must prioritize security in the design and development of their products." These approaches will not eliminate vulnerabilities, but they are proven to drive them down, which can also reduce security costs across the ecosystem. Secure by design and default are core elements of responsible innovation. In order for us to have a more stable and resilient future driven by technology innovation, companies developing these secure to market products should be recognized and rewarded for outperforming their first to market peers.[14]

Congress and the Administration should continue to explore how to better incentivize organizations across the ecosystem to develop and maintain their networks and products in the most secure and resilient manner possible. Failing to do so will only result in more of the same – or worse – for consumers and our national security.

Departments and Agencies Must Be Sufficiently Resourced to Support this Resilience

Second, because we know where there are weaknesses the worst of society will work to exploit them, we must ensure that federal, state, and local agencies have sufficient resources and expertise to enforce the rule of law, which is also central to our dominance on the world's financial stage. Malicious actors, including ransomware actors, abuse U.S.-based and other jurisdictions' financial and technology services in multiple ways. For the purposes of today's discussion, I will focus on ransomware actors' nexus to the financial sector.

The Ransomware Task Force placed a high priority on the need for disruptive actions to defeat ransomware and noted that greater regulatory enforcement and reporting will help inform and scale disruption. In short, until we have a secure by design driven ecosystem, in order to defeat ransomware, we must be able to follow the money, and timely and relevant information is essential in doing so. In my testimony in the last Congress before the Senate Committee on Homeland Security and Government Affairs, I noted that to meet the risks of tomorrow, the government and the private sector must be able to gather useful information and disseminate it to the right people within a meaningful period of time. Those sharing the information also need

[12] "Known Exploited Vulnerabilities Catalog | CISA," Cybersecurity and Infrastructure Security Agency, https://www.cisa.gov/known-exploited-vulnerabilities-catalog.
[13] Message from the Chair and Deputy Chair, "Review of the Summer 2023 Microsoft Exchange Online Intrusion," Cyber Safety Review Board, March 20, 2024, https://www.cisa.gov/sites/default/files/2024-04/CSRB_Review_of_the_Summer_2023_MEO_Intrusion_Final_508c.pdf.
[14] *See* Megan Stifel, *Securing the Modern Economy, Transforming Cybersecurity Through Sustainability*, *Public Knowledge*, April 2018, https://nationalsecurity.gmu.edu/wp-content/uploads/2018/04/Securing-the-Modern-Economy-Stifel.pdf.

to keep in mind that a specific piece of information may be of different value depending on the receiving agency's or organization's mission.

I further noted that the limited operational collaboration and scale of information-sharing among and between government agencies and private industry partners has inhibited cooperation on disruptive actions against criminals. In particular, the lack of comprehensive information about ransomware attacks continues to frustrate the private sector's ability to protect itself, inform policy development, and help take collective action against ransomware actors.

The disruptive actions taken in recent years via coordinated action between departments and agencies to seize cryptocurrency assets and malicious actor command and control infrastructure could expand significantly if clear, concise, actionable information is made available to appropriate organizations as early as possible in the payment killchain. When the government receives or disseminates that information many days and even weeks following an incident and/or payment, often the window for disruptive action may have already closed.

Thus, while significant progress has been made, governments still need to do more to support the private sector in order to not only defeat ransomware, but wherever fraudsters and other criminals turn to next.

At IST, we have been working to better enable operational collaboration to support implementation of the Task Force's related recommendations. In 2022, IST published a map outlining the ransomware payment process by entity type.[15] As depicted in that map, multiple types of entities can have visibility on ransomware actors and the payments they receive as part of their criminal activities. In order to further refine our analysis, last spring IST launched a Ransomware Payment Map Mini-Pilot that detailed the resourcing phase of ransomware incidents. The paper outlined four cases of ransomware attacks, following their path through the ransomware ecosystem and identifying the tools, services, and entities that they leveraged as they prepared for and carried out attacks. The Mini-Pilot sought to identify which types of disruptions could be most effective in adding friction and how they could potentially be applied to the broader cybercrime ecosystem.[16] It also serves as a basis for our ongoing work to identify legal and policy barriers frustrating collective action.[17]

This week we will publish the next phase of our research "Information Sharing in the Ransomware Payment Ecosystem: exploring the delta between best practices and existing

[15] Zoë Brammer, *Mapping the Ransomware Payment Ecosystem: A Comprehensive Visualization of the Process and Participants*, *Institute for Security and Technology*, November 2022, https://securityandtechnology.org/wp-content/uploads/2022/11/Mapping-the-Ransomware-Payment-Ecosystem.pdf.
[16] Zoë Brammer, *Mapping Threat Actor Behavior in the Ransomware Payment Ecosystem: A Mini-Pilot, Institute for Security and Technology*, May 2023, https://securityandtechnology.org/virtual-library/reports/mapping-threat-actor-behavior-in-the-ransomware-payment-ecosystem-a-mini-pilot/
[17] Brammer, *Mapping Threat Actor Behavior in the Ransomware Payment Ecosystem: A Mini-Pilot.*

mechanisms."[18] The report first describes in detail a ransomware attack scenario exercise conducted by IST's RTF Payments Working Group. Next, it compares the results of this exercise with recent collaborative operations, including the Hive disruption operation, the Emotet botnet takedown, and the Colonial Pipeline ransom payment recovery. The report then outlines existing formal federal information sharing mechanisms in the United States, maps these mechanisms atop the ransomware payment ecosystem map, and identifies gaps that, if addressed, could clarify the information environment and help scale disruptive operations. Finally, the report delineates steps that the United States and its partner governments can take to bolster information sharing with the private sector to help scale existing best practices.

Collectively, this research has found that many entities depicted in the payment map have obligations to report to the government information about ransomware incidents. Most organizations in the United States that are obligated to report do so. However, in our experience, U.S. government departments and agencies lack sufficient resources to adequately leverage this visibility to the fullest extent. That challenge is even greater outside the United States.

Internationally, members of the Financial Action Task Force (FATF) have worked to implement Recommendation 15,[19] which effectively harmonizes countries' regulations regarding suspicious activity reporting for virtual assets and virtual asset providers. As this subcommittee knows, ransomware is a global problem, and many countries experiencing ransomware or harboring its actors are not FATF members or lack the resources to fully comply with their FATF commitments.[20] This inconsistent approach creates gaps that malicious actors continue to leverage. The United States and its partners can work to close these gaps by helping build and scale legal and investigative capacity abroad and more adequately resourcing domestic agencies to leverage the financial and other intelligence available.

When considering which partners and allies to support, members of the International Counter Ransomware Initiative should be a top priority. The Initiative, established in 2021 and comprised of 50 plus member states and organizations,[21] has committed to tackling ransomware on a global scale through coordinated efforts, including building cyber capacity, launching information

[18] Zoë Brammer, *Information Sharing in the Ransomware Payment Ecosystem: Exploring the Delta Between Best Practices and Existing Mechanisms*, April 17, 2024, https://securityandtechnology.org/virtual-library/reports/information-sharing-in-the-ransomware-payment-ecosystem/.

[19] For more information, see: Financial Action Task Force, "Public Statement on Virtual Assets and Related Providers," June 21, 2019, https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Public-statement-virtual-assets.html.

[20] For more information, see: Financial Action Task Force (FATF), "Virtual Assets: Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers" June 27, 2023, https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2023.html. See also: Financial Action Task Force, "Status of Implementation of Recommendation 15 by FATF Members and Jurisdictions With Materially Important VASP Activity," March 2024, https://www.fatf-gafi.org/content/dam/fatf-gafi/publications/VACG-Table-Jurisdictions-2024.pdf.coredownload.pdf.

[21] For more information on current CRI members, see: https://counter-ransomware.org/aboutus.

sharing mechanisms, and adopting commitments to fight back against ransomware threat actors. Notably, among the 50 plus CRI members, 27 are also FATF members. These countries can serve as partners in assisting jurisdictions that seek to improve their adherence to anti-money laundering best practices, as well as pressuring the governments of countries that serve as ransomware actor safe havens.

Make no mistake, CRI members view the United States and its peers as leaders in the fight against ransomware. We must lead by example at home in order to maintain leadership abroad. Congress should adequately resource enforcement departments and agencies in order to ensure a resilient financial ecosystem.

Leverage the Reach of Financial Services to Help Raise Collective Digital Resilience

Third, the financial services sector can play an even greater role in raising our collective digital defenses. As I noted at the outset, the Task Force called for a sustained, aggressive, public-private collaborative anti-ransomware campaign. It also called for nationwide, government-backed awareness campaigns. The financial services sector can help advance implementation of both of these actions.

Over 80% of U.S. households are "fully banked."[22] This means that financial institutions are in contact with a large percentage of our population. Moreover, a majority of consumers continue to report a high degree of trust in their banks.[23] This privileged position is an opportunity some institutions have seized upon to communicate the importance of good cybersecurity. During Cybersecurity Awareness Month, many banks run cybersecurity awareness campaigns. Doing so not only protects the banks themselves, it also protects their customers.[24] Awareness campaigns should be encouraged and expanded given the evolving tactics ransomware criminals employ to evade detection.

The U.S. Department of the Treasury recently noted that ransomware actors may use accounts belonging to money mules.[25] In the United Kingdom, the Don't Be Fooled campaign partners law enforcement and banks to educate consumers about the dangers of money laundering and the signs of money mule recruitment.[26] A similar approach with an expanded scope–including

[22] Federal Deposit Insurance Corporation, "2021 FDIC National Survey of Unbanked and Underbanked Households," Updated July 24, 2023, https://www.fdic.gov/analysis/household-survey/.
[23] Anna Hrushka, "Trust in banks remains steady, while fintechs have ground to cover: survey," Banking Dive, Nov. 23, 2023, https://www.bankingdive.com/news/trust-banks-fintechs-digital-survey-crisis-morning-consult/698627/.
[24] ISG, "How Banks Can Drive Revenue and Security Awareness with Internal Security Operations," February 14, 2023, https://isg-one.com/articles/how-banks-can-drive-revenue-and-security-awareness-with-internal-security-operations.
[25] Department of the Treasury, "2024 National Money Laundering Risk Assessment," Department of the Treasury National Money Laundering Risk Assessment, 2024, https://home.treasury.gov/system/files/136/2024-National-Money-Laundering-Risk-Assessment.pdf.
[26] National Crime Agency United Kingdom Financial Intelligence Unit, "Money Mules Special Edition," 2023, https://www.nationalcrimeagency.gov.uk/who-we-are/publications/675-sars-in-action-issue-22/file.

boosting preparation to avoid paying ransoms–could be considered in the United States. For example, when it comes to cybersecurity, banks have been the leading edge in driving adoption of multi-factor authentication.[27] More Americans are now willing to use it in connection with other activities they conduct online. Given the reach the financial services sector has together with its perception as a trustworthy messenger, Congress and the Administration should explore avenues for the government and financial services sector to partner to further drive adoption of known cybersecurity best practices. Doing so will help better protect the American people, the financial services sector, and collectively raise our national resilience.

In conclusion, I want to thank the Committee for inviting me as a civil society representative to participate in today's timely hearing. Civil society plays a critical role supporting multiple essential societal functions. Today, the Internet and other digital technologies underpin these functions; securing this connectivity is essential for social and economic growth and national security. We value this and similar opportunities to raise awareness about threats to these functions and how, with the support of philanthropy, civil society can contribute to collectively combating them.

I look forward to your questions.

[27] Fight Cybercrime, "MFA Consumer Sentiment Report," November 2023, https://fightcybercrime.org/wp-content/uploads/2023/11/CSN_MFAConsumerSentimentReport.pdf.