Testimony of

Philip James Reiner
Chief Executive Officer
Institute for Security and Technology

Before the
United States House of Representatives
Committee on Energy and Commerce
Subcommittee on Oversight and Investigations

July 20, 2021

"Stopping Digital Thieves: The Growing Threat of Ransomware"

Chair DeGette, Ranking Member Griffith, Chairman Pallone, Ranking Member McMorris Rodgers, members of the Subcommittee on Oversight and Investigations, thank you for the opportunity to testify today on the scourge of ransomware and the pervasive threat that it poses to our critical infrastructure, public health and safety, and overall national security. It is an honor to join such an illustrious panel of witnesses here today. It is my hope that I can contribute insights to this discussion in support of the Subcommittee's investigation into what has become a national - and international - cybersecurity crisis.

My name is Philip Reiner, and I am the Chief Executive Officer of the Institute for Security and Technology (IST). I am a former Pentagon civil servant that served in the Office of the Secretary of Defense for Policy in the Pentagon for almost a decade, the last four years of which I was detailed to the National Security Council, where in my final role I served as the Senior Director for South Asia. I have been challenged over my career to devise and execute strategies meant to stop nuclear weapons from falling into the hands of terrorists, prevent attacks against the American homeland, build international partnerships in support of vast, complicated missions, and now in my role as CEO of IST, to create trusted venues where national security policymakers can directly engage with technology leaders and those engaged in trusted public-private operational cooperation. At IST, our mission is to work across these communities, bridge gaps, build relationships, and catalyze novel solutions to technology-driven emerging national security threats.

I appear before you today not just as the CEO of IST, but also as the Executive Director of the Ransomware Task Force,[1] which was convened by IST earlier this year. The effort was undertaken from January to April, with the express purpose of developing a comprehensive framework for action to combat the ransomware scourge.[2] We were extremely pleased to welcome representatives from 60+ public and private organizations, to whom IST and myself are deeply indebted - and without whom I would not be here testifying to you today on these matters. Together with this amazing group, we "sprinted a marathon" and devised 48 recommended actions across four main areas of focus: to deter attacks, to disrupt ransomware actors, to help organizations prepare, and to improve ransomware response. In the end, ransomware is a solvable problem - but currently it is metastasizing at an alarming rate.

In large part, IST stood up the Ransomware Task Force because we were frustrated with what we perceived to be a lack of coordinated action as the ransomware threat was clearly rising in 2019 and 2020. And indeed, just a week after the Task Force released its report, the Colonial Pipeline cyberattack struck. As others have testified elsewhere and spoken to at length in public fora, the priority recommendations from the Task Force include the topline need for sustained,

[1] The Ransomware Task Force. https://securityandtechnology.org/ransomwaretaskforce.
[2] Combating Ransomware. *A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force*. 27 April 2021. https://securityandtechnology.org/ransomwaretaskforce/report/.

coordinated, and collective action among governments, industry, academia, and civil society to substantially reduce the ransomware threat.

I want to make clear right up front that there are professionals - both in public and private roles - who are toiling night and day to prevent, mitigate, and respond to the ransomware threat which today leaves no domain untouched - from critical infrastructure and key resources to hospitals and schools. These information security professionals are overworked and often outgunned. Our country is indebted to them for their tireless efforts, and it is our hope to improve the odds against which they are pitted, while we aim to decrease the threat to our national security posed by these criminals. These professionals deserve every element of support we can muster.

I will focus my testimony today on three main areas: first on an overview of the topline recommendations of the Task Force report, which lays out a comprehensive framework to address ransomware; second, on steps already taken since the launch of the report in April; and third, I will highlight Action items from the the Task Force report that will require Congressional action. The most critical element of this conversation is not the report we released, but the urgent need for the adoption of its recommendations, with speed, priority, and resources. The timing of this hearing is thus incredibly important: unless the actions recommended by the Ransomware Task Force are broadly and quickly implemented, the scourge of ransomware and the threat it poses to critical infrastructure and our national security will only continue to worsen.

To clarify, when I assert that the ransomware problem will only continue to worsen if not addressed in a comprehensive fashion, it is instructive to highlight recent attacks against the Colonial Pipeline Company[3] and the information technology management platform provider Kaseya.[4] The Colonial Pipeline example is instructive in that it is relatively clear that the Darkside criminal group behind the attack likely had no idea their extortion target was such a critical element of U.S. energy infrastructure. The "ransomware as a service" business model provides ransomware capabilities to would-be criminals who do not have the skills or resources to develop their own malware. This creates distributed opportunities with a low barrier to entry to conduct ransomware attacks, which may occur indiscriminately and without consideration for the consequences of the victim in question.[5] What happens when a ransomware attack shuts down water treatment facilities for a large metropolitan city, or attacks against healthcare systems escalate even further? These are not hypothetical assertions of possibility - it is simply only a matter of time that these attacks will happen if we don't take concerted action now.

---

[3] Sanger, David E, and Nicole Perlroth. "Pipeline Attack Yields Urgent Lessons about US Cybersecurity." *New York Times*, 14 May 2021, www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html.
[4] Satter, Raphael. "Up to 1,500 Businesses Affected by Ransomware Attack, U.S. Firm's CEO Says." Reuters, 6 July 2021, www.reuters.com/technology/hackers-demand-70-million-liberate-data-held-by-companies-hit-mass-cyberattack-2021-07-05/.
[5] Palmer, Danny. "Ransomware as a Service Is the New Big Problem for Business." ZDNet, 4 Mar. 2021, www.zdnet.com/article/ransomware-as-a-service-is-the-new-big-problem-for-business/.

The Kaseya incident is doubly instructive. As part of the Ransomware Task Force process, we took time as part of a sub-working group to game out some of the worst case scenarios. One imagined scenario was a ransomware gang massively scaling the distribution of their malicious payload through the exploitation of a vulnerable managed service provider - an increased level of sophistication with devastating effect on a much larger scale than previously seen. That is what we've just witnessed in the attack against Kaseya - except it was this scenario on steroids, targeting the information technology (IT) management capabilities provided to a range of Managed Service Providers (MSPs), instead of an attack against just one. Now that this use case has been proven effective, other criminal groups will follow suit - likely with even more critical companies compromised through supply chain-style ransomware attacks. Ransomware actors have every incentive to continue escalating their tactics to find the situations most effective at extorting ransoms, ones that put enormous pressure on essential functions. These are not scenarios we are ready to withstand.

As mentioned above, ransomware is not a new threat. This is a long-standing type of cybercrime and malware attack. People have been working to stop these attacks for years. The dynamic has drastically changed, however, and ransomware is no longer just an economic cybercrime. Today it has become a malicious form of online activity that has immense real world effects: it has taken on the scale and virulence of a threat to our national security, to our societal and economic well being, to our critical infrastructure, and to our public health and safety.

The costs of ransomware also go far beyond the ransom payments themselves, incurring much broader societal harm. Cybercrime is typically seen as white-collar, but while ransomware is profit-driven and "non-violent" in the traditional sense, that has not stopped these attackers from routinely threatening supply chains, risking human lives by shutting down hospitals with critical patients, diverting vital public resources, threatening the loss of data/privacy, disrupting schools and colleges, exposing the data of minors, placing entire cities under siege, and extorting exorbitant and destructive ransoms in the millions of dollars. These criminals, on the whole, do not care who they victimize - whether it's a gas pipeline, a managed service provider, an elementary school, or a large hospital system. They do not care if people die - and it is clear based on the medical literature that these attacks against hospitals and health care systems increase the risk of severe outcomes for patients unable to receive care. These criminals clearly do not care if essential services are disrupted. In fact, they count on it - the more desperate the victims, the more inclined they may be to pay the ransom.

What has changed to make ransomware a significantly more virulent threat than it was before? A few factors can be clearly identified:

1. The affiliate "ransomware as a service" business model has created efficiencies and deniability through the distributed, outsourced specialization of tasks
2. Vast increases in digital attack surfaces, offering almost neverending opportunities for exploitation of vulnerabilities, including through increasingly distributed operations due to rise of work from home during the COVID pandemic
3. Anonymous, ubiquitous, and decentralized payment infrastructures have made cross-border payments vastly more efficient and inexpensive, while significantly increasing the challenge of tracing the laundering of digital currencies
4. Massive increases in computing power and access to distributed cloud resources exacerbated the pre-existing challenge posed by botnets, and
5. Finally, with each of these capabilities, actors are more able to operate with impunity from safe havens out of the reach of law-enforcement in the nations where attacks occur

This is important to make clear: efforts to mitigate ransomware have been effective in some cases. But the nature of the threat itself has evolved to such an extent that our response must evolve as well - the criminals rely on the seams between our Departments and Agencies, our classifying these types of attacks only as crimes instead of national security threats, and the gaps between public and private abilities to collaboratively prepare and respond.

Ransomware criminals have also come to count on there being no sustained follow through on disruptive activities: for example, the public-private effort to disrupt the Emotet infrastructure[6] earlier this year was an immense success in its breadth and creativity. However, criminals were almost immediately reconstituting the technical infrastructure that had been disrupted.

Despite the dire reality and complexity of the current situation, I believe, and the Ransomware Task Force agrees, that this is a solvable problem. There is no single solution to this set of challenges: this is an international cybersecurity crisis that demands that countries and companies work closely together on a range of historically difficult tasks. The combination of the actions needing sustained attention compound the challenge in blunting the trajectory of these attacks. Ransomware has become too large of a threat for any one entity to address, and the scale and magnitude of this challenge urgently demands coordinated global action.

The Comprehensive Framework to Combat Ransomware

In response to the overall challenge, the Ransomware Task Force process resulted in 48 recommended actions within four focus areas. We debated the most effective framework and determined those four focus areas to be the most salient as part of a comprehensive approach:

[6] Federal Bureau of Investigation. "FBI, Partners Disarm Emotet Malware." News release, 1 Feb. 2021, https://www.fbi.gov/news/stories/emotet-malware-disrupted-020121.

1. **Deter ransomware attacks through a nationally and internationally coordinated, comprehensive strategy:** ransomware can be deterred if conducting an attack becomes more risky, less likely to succeed, and more costly. This includes holding criminals accountable, promoting international prioritization and collaboration, and eliminating safe havens where criminals operate with impunity.
2. **Disrupt the ransomware business model and decrease criminal profits:** ransomware can be disrupted when threat actors are pushed out of the business and the appeal to new threat actors is reduced. This includes increased targeting of the criminals themselves, their technical infrastructure, and the cryptocurrency payment process they rely on for funds.
3. **Help organizations prepare for ransomware attacks:** organizations will be better prepared for an attack with clear directives, adequate resources, and the right incentives. This includes providing a single, clear ransomware framework for preparation and response, and incentivizing businesses and governments to increase their cyber hygiene and defend their networks.
4. **Respond to ransomware attacks more effectively:** better information sharing and victim support will improve our collective resilience to ransomware. This includes providing greater resources for victims, enhanced reporting mechanisms, and clear guidelines for what to do after a ransomware attack.

At its core, the intent is to do all we can to disrupt the ransomware business model. These goals are interlocking and mutually reinforcing. For example, actions to disrupt the ransomware payments system will decrease the profitability of ransomware, thereby helping to deter other actors from engaging in this crime. In a similar vein, many actions taken to better prepare organizations for ransomware attacks, such as informing them about the risks, will also improve their ability to respond, while understanding more about how organizations are responding to ransomware attacks will help improve organizations' collective preparedness. Thus, this framework should be considered as a whole, not merely a list of potential disparate actions.

The only area where I and other Task Force members did not come to a concise conclusion was in regard to the payment of ransoms. The question of whether to prohibit payment of ransoms has become increasingly pressing, and was raised by every working group in the Task Force. Practical implementation of such a ban would be challenging at this time: the ecosystem is vulnerable, and without steps to shore up defenses and disrupt ransomware criminals, it would be overwhelmed with attacks. Simply banning payment in the immediate term will do little to stop ransomware attacks, and place significant onus on victim organizations.

The Ransomware Task Force did not reach consensus on recommending a prohibition on paying ransoms. However, it did develop a proposed phased approach to potentially reach prohibition which members agreed would be necessary to obtain the desired impact. The Task Force

concluded that the most reasonable and effective approach would be a multi-year, conditions-driven approach based on milestones, with prohibitions beginning within two years. The priority considerations must be the timeline, the phasing of steps, and victim protection and support. Proposed milestones, such as hardening security of critical infrastructure, should be pursued concurrently. If pursued vigorously, the necessary milestones could be met much more rapidly than the proposed timeline.

The overall topline recommendations from the Ransomware Task Force report are below. These priority recommendations are the most foundational and urgent; many of the other recommendations were developed to facilitate or strengthen these core actions:

1. Coordinated, international diplomatic and law enforcement efforts must proactively prioritize ransomware through a comprehensive, resourced strategy, including using a carrot-and-stick approach to direct nation-states away from providing safe havens to ransomware criminals.
2. The United States should lead by example and execute a sustained, aggressive, whole of government, intelligence-driven anti-ransomware campaign, coordinated by the White House. In the U.S., this must include the establishment of 1) an Interagency Working Group led by the National Security Council in coordination with the nascent National Cyber Director; 2) an internal U.S. Government Joint Ransomware Task Force; and 3) a collaborative, private industry-led informal Ransomware Threat Focus Hub.
3. Governments should establish Cyber Response and Recovery Funds to support ransomware response and other cybersecurity activities; mandate that organizations report ransom payments; and require organizations to consider alternatives before making payments.
4. An internationally coordinated effort should develop a clear, accessible, and broadly adopted framework to help organizations prepare for, and respond to, ransomware attacks. In some under-resourced and more critical sectors, incentives (such as fine relief and funding) or regulation may be required to drive adoption.
5. The cryptocurrency sector that enables ransomware crime should be more closely regulated. Governments should require cryptocurrency exchanges, crypto kiosks, and over-the-counter (OTC) trading "desks" to comply with existing laws, including Know Your Customer (KYC), Anti-Money Laundering (AML), and Combatting Financing of Terrorism (CFT) laws.

Encouraging Actions Are Being Taken - But More is Needed

Since the launch of the Task Force's recommended comprehensive approach in April 2021, it has been encouraging to see international, national, and industry steps taken in the direction of some of the recommended actions. Most immediately, the announcement from the White House on

July 15th that it has launched an interagency Ransomware Task Force is extremely encouraging. From the list of 48 recommendations in the Task Force report, my personal assertion is that this is the most critical step necessary in order to move all elements of national power in the right direction: that the United States needs to execute a relentless, sustained, well resourced, international counter-ransomware campaign that leverages all tools of national power: diplomatic, economic, intelligence, law enforcement, and military. While the announcement from the White House indicates the process is just getting started, it is encouraging to know top-down leadership has been instituted. The areas of focus as part of that effort will apparently also include a number of priority areas recommended by the Task Force: coordinating with international allies, disrupting ransomware operators, improving visibility into the cryptocurrency ecosystem, developing ways to halt ransom payments, promoting resilience among critical infrastructure providers, coordinating interagency ransomware resources via http://stopransomware.gov, and using the Rewards for Justice program to offer cash payments for tips leading to arrests of ransomware operators. These are all really fantastic steps in the right direction as part of an overall, coordinated, whole of government effort.

Additionally, the Ransomware Task Force's call for leader-level prioritization of ransomware in many ways has been heeded - exemplified by President Biden's repeated assertions that ransomware is a top priority for his Administration, as well as the White House's inclusion of ransomware as a top three priority during President Biden's summit with Russian President Vladimir Putin. Increased political, diplomatic, economic, and law enforcement pressure on President Putin to take action against those groups acting with impunity from Russian soil was a topline recommendation of the Task Force. As it entirely remains to be seen as to whether the Russian leader will ever take action against these groups, it is a powerful signal to both the international community that this is a national level priority, and begins the process of sending the necessary deterrent signal to the ransomware criminals themselves that they will no longer be left to simply get away with these crimes. The prioritization of ransomware by the leadership in the United Kingdom[7] and as was expressed by the G7 leaders in June of this year continues the necessary trend of making declarative policy that the trajectory of these attacks must be dampened.[8] Those declarations need to be followed up with strategies and action plans - most of which can be taken from the recommendations of the Task Force and repurposed for national decision making around the world.

Additionally, in June the U.S.-EU Ministerial Meeting on Justice and Home Affairs included the launch of a U.S.-EU joint working group on prevention and enhanced law enforcement

[7] National Cyber Security Centre. "Cyber security sector leaders to appear at CYBERUK." News release, 5 May 2021. https://www.ncsc.gov.uk/news/leading-figures-from-uk-politics-to-appear-at-cyberuk; Corera, Gordon. "Foreign Secretary issues warning to Russia on ransomware." *BBC News*, 12 May 2021, https://www.bbc.com/news/technology-57084943.
[8] Reuters Staff. "G7 demand action from Russia on cybercrimes and chemical weapon use." Reuters, 13 Jun. 2021, https://www.reuters.com/world/europe/g7-demand-action-russia-cybercrimes-chemical- weapon-use-2021-06-13/.

cooperation to address the rise of ransomware attacks in the United States and Europe.[9] Again, these are positive steps in the right direction, but it remains to be seen what work will be undertaken and with what areas of focus.

As all these steps have been undertaken, the U.S. Department of Justice and the Department of Homeland Security from early on initiated their own internal ransomware-focused task force efforts. The recommendations in the Task Force report were for U.S. Departments and Agencies to ramp up actions against the ransomware threat through prioritization and resourcing solutions, which is exactly what can be seen by these sets of actions. The Department of Justice has continued to engage in an internal effort to prioritize ransomware response and investigations, exemplified by a wallet seizure and the recovery of extorted funds in the Colonial Pipeline instance.[10] The DOJ elevation of investigations of ransomware attacks to a similar priority as terrorism shows the level of intensity these criminal activities now will be addressed with - and how the necessary resources will be made available as well. These are exactly the types of steps recommended by the Task Force. As noted above, the Department of Homeland Security took the initiative to launch www.stopransomware.gov,[11] which is directly in line with the Task Force recommendation to consolidate resources into a one-stop-shop / single source of truth, and focused its first cybersecurity sprint on ransomware. These steps are but a part of the clear emphasis that DHS and its leadership are placing on this pernicious threat.

Additionally in line with the recommendations of the Task Force, the National Institute of Standards and Technology (NIST) released an initial ransomware profile based on the Cybersecurity Framework, with a public call for comment, and hosted an initial workshop on July 13th, 2021 to garner insights from partners and the public.[12] Finally, also in line with the recommendations put forward in the Task Force report, seven large U.S.-based insurers combined forces to establish a consortium called CyberAcuView[13] to share data and broaden the industry's collective understanding of the threat so as to more effectively underwrite cyber insurance policies going forward. The threat is so significant that we need to see many more such actions, but these are all moves in the right direction. Follow through will be key.

---

[9] Underwood, Kimberly. "U.S. and EU To Collaborate Against Ransomware." *The Cyber Edge*, 24 Jun., 2021, https://www.afcea.org/content/us-and-eu-collaborate-against-ransomware.
[10] Department of Justice. "Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside." News release, 7 Jun. 2021. https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside.
[11] Department of Homeland Security. "United States Government Launches First One-Stop Ransomware Resource at StopRansomware.gov." News release, 14 Jul. 2021, https://www.dhs.gov/news/2021/07/14/united-states-government-launches-first-one-stop-ransomware-resource.
[12] National Institute of Standards and Technology. *Cybersecurity Framework Profile for Ransomware Risk Management (Preliminary Draft)*. By William Barker, Karen Scarfone, William Fisher, and Murugiah Souppaya. NISTIR 8374 (Draft). Jun. 2021. https://csrc.nist.gov/publications/detail/nistir/8374/draft.
[13] CyberAcuView. "Consortium of Leading Cyber Insurers Announce the Launch of CyberAcuView." News release, 17 Jun. 2021. https://cyberacuview.com/press-release-june-2021/.

A particular point of contention has been the use of offensive cyber actions to address the ransomware threat. The Task Force recommended that national governments, working closely through coordinated action, should consider all tools of national power. In my personal opinion, the authorities typically relied upon to address ransomware attacks are not commensurate with the level of harm these attacks are currently causing nor sufficient to deter their continued increase going forward. That does not mean that new authorities are needed to provide the options necessary to deter these activities. Rather, through the recommended interagency coordinated Joint Ransomware Task Force, the U.S. government can more effectively take advantage of the array of authorities and other tools that are already available.

The Ransomware Task Force report makes clear, for example, that while the Computer Fraud and Abuse Act (USC Title 18 §1030) is perhaps an appropriate tool for prosecuting some ransomware attacks, it can be made more powerful when combined with alternate tools of national power and already existing prosecutorial options. The Task Force recommended Action 2.3.3, for example, stated that any federal counter-ransomware framework should "apply strategies for combating organized crime syndicates to counter ransomware developers, criminal affiliates, and supporting payment distribution infrastructure." This could include other federal statutes covering Racketeer Influence and Corrupt Organizations (RICO - Title 18 §1962), money laundering, commercial extortion, homicide - and even terrorism. The Department of Justice's recent internal memoranda to this effect point to a move in this direction already. These could potentially add significant deterrent value to an overall counter-ransomware strategy.

In my personal opinion, the full U.S. response to ransomware attacks must expand beyond reliance on USC Title 18 for criminal investigation and prosecution. The authorities provided under USC Titles 10, 31, and 50 should all be invoked as necessary to provide more effective and robust options to deter and disrupt ransomware actors and the infrastructure used to attack U.S. critical infrastructure and hold our public health and safety hostage. Title 31 allows the Treasury Department, through the Office of Foreign Asset Control (OFAC), to put financial sanctions on foreign entities that have conducted or facilitated cyber attacks against U.S. organizations. Titles 10 (military authorities) and 50 (intelligence authorities) can improve domestic cyber defenses by putting the United States on the offensive. They could be invoked to take an "active" or "forward" defensive posture to proactively disable and disrupt foreign-based cyber threats - as was seen as part of coordinated interagency activity during the 2020 Presidential elections.

Finally, the Intelligence Community must be used to augment and support these counter-ransomware actions, in sequenced and coordinated operations as part of an overall national strategy, as has been done in the ongoing fight against transnational terrorist threats. There are clear differences between the two sets of challenges - ransomware vs. counterterrorism - but structural similarities exist. This all again points to the need for a top-down, intelligence-driven coordinated effort that deploys all tools of national power.

It is important to note that deploying and executing offensive cyber operations through the appropriate authorities will primarily be successful in that they can create a window of opportunity for other actions to take place. By no means, however, will Title 10 and 50 actions alone eliminate the ransomware threat. As noted, the ransomware actors will quickly reconstitute, and other actors will rise to take the place of those who may end up taken into custody. New groups will coalesce with new tools in response to disruptive actions - which points to the clear need in the window of time that is created for assertive action to shore up defenses and raise the level of seriousness that is afforded to cyber hygiene. Cybercrime persists in large part due to poor cyber hygiene - thus the rest of the applicable solutions recommended by the Task Force must be implemented as well.

Priority Considerations for Congress

Within the Actions recommended by the Ransomware Task Force, a number can be highlighted that are items that will necessitate Congressional action, and I would like to highlight them here:

1. Action 2.1.2. Require cryptocurrency exchanges, crypto kiosks, and over-the-counter (OTC) trading "desks" to comply with existing laws
2. Action 2.2.2: Clarify lawful defensive measures that private-sector actors can take when countering ransomware
3. Action 3.3.1: Update cyber-hygiene regulations and standards
4. Action 3.3.2/3: Require local governments and managed service providers (MSPs) to adopt limited baseline security measures
5. Action 3.4.2: Expand Homeland Security Preparedness grants to encompass cybersecurity threats
6. Action 3.4.5: Investigate tax breaks as an incentive for organizations to adopt secure IT services
7. Action 4.1.2: Create a Ransomware Response Fund to support victims in refusing to make ransomware payments (incentivize non-payment of ransoms)[14]
8. Action 4.2.4: Require organizations and incident response entities to share ransomware payment information with a national government prior to payment

Congress will have a critical role to play here in implementing these proposals, and the Institute for Security and Technology looks forward to working with members of this Committee on advancing legislation pertaining to these proposals. Ransomware succeeds in large part due to a broad underinvestment in cybersecurity by both industry and government. As noted, this highlights the need for strengthening the incentive structures, but also to redouble outreach

[14] The United States Innovation and Competition Act of 2021 (USICA), passed in June 2021, includes the creation of a Response and Recovery Fund, the funds from which could be utilized for asset response and recovery purposes in the event of a significant cyber incident. See United States Innovation and Competition Act, S. 2160, § 4251-4252, 117th Cong. (2021), https://www.congress.gov/bill/117th-congress/senate-bill/1260.

through entities such as NIST and the Small Business Administration - which requires greater resources. When considered in light of the scope of the threat from ransomware, this outreach and resources become all the more important as small businesses drive our economy.

It is important to note that conversation as part of the Task Force process focused on the clear need to ensure the recommendations were not perceived as condoning "hackback" activities, but it was also clear from an industry perspective that expectations of what defensive actions can be taken under CISA 2015 could be further clarified. This would provide greater levels of confidence to an array of different stakeholders interested in playing as proactive a role as possible in efforts to disrupt ransomware criminal network behaviors.

Finally, this set of recommended Actions point clearly to the challenge of raising the bar for expectations from industry - and from government - in terms of the level of commitment and resources applied against these threats and the vulnerabilities that drive them. The scale and breadth of the ransomware threat demands a reprioritization of attention, effort, and resources at the same levels we once saw for counterterrorism. The need to establish the right investment structures would be greatly assisted if the steps recommended in the Task Force report were undertaken, to include those listed above that would likely require Congressional action.

Conclusion

The actions detailed in the Task Force report need to be enacted together as soon as possible, and must be coordinated at a national and international level. If this framework is implemented in full, the international community could see a decrease in the volume of these types of attacks in one year's time. With every recommended action we worked through the practical implications, and in most cases we presented immediately actionable recommendations. Ransomware has become too large of a threat for any one entity to address, and the scale and magnitude of this challenge urgently demands coordinated global action - no one can do this on their own.

The Institute for Security and Technology offers a unique perspective on these issues, as a neutral 501c3 non-profit that straddles the national security and technology communities. Our ability to translate between both public and private leaders across domains through deep, trusted interactions allows for creative solutions and the ability to work directly with both federal leaders and industry partners on the implementation of necessary actions. We are privileged to provide this platform to facilitate communication and cooperation between the government and the private sector in our common interest to collectively defend against ransomware attacks.

This bears repeating - Congress has a vital role to play here. We welcome the opportunity to inform the work of this committee in this capacity and stand ready to assist as needed.