Hearing - Hearing Transcripts

Title Info

Title:	House Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection and Innovation Holds Hearing on Russian Cyber Threats
Date:	April 05, 2022
Committee:	Homeland Security;HouseSubcommittee on Cybersecurity, Infrastructure Protection, and Innovation. Committee on Homeland Security. House
Source:	Transcript
Permalink:	https://congressional-proquest-com.proxygw.wrlc.org/congressional/docview/t39.d40.tr04050122.o25?accountid=11243

Body

House Homeland Security: Mobilizing Our Cyber Defenses: Securing Critical Infrastructure Against Russian Cyber Threats

April 05, 2022 10:00 A.M.

SPEAKERS:

REP. YVETTE CLARKE (D-N.Y.), CHAIRWOMAN

REP. SHEILA JACKSON LEE (D-TEXAS)

REP. JIM LANGEVIN (D-R.I.)

REP. ELISSA SLOTKIN (D-MICH.)

REP. KATHLEEN RICE (D-N.Y.)

REP. RITCHIE TORRES (D-N.Y.)

REP. LOU CORREA (D-CALIF.)

REP. BENNIE THOMPSON (D-MISS.), EX-OFFICIO

REP. ANDREW GARBARINO (R-N.Y.), RANKING MEMBER

REP. RALPH NORMAN (R-S.C.)

REP. DIANA HARSHBARGER (R-TENN.)

REP. ANDREW CLYDE (R-GA.)

REP. JACOB LATURNER (R-KAN.)

REP. DAN BISHOP (R-N.C.)

REP. CLAY HIGGINS (R-LA.)

REP. JEFFERSON VAN DREW (R-N.J.)

REP. MARIANNETTE MILLER-MEEKS (R-IOWA)

REP. CARLOS GIMENEZ (R-FLA.)

REP. TOM MALINOWSKI (D-N.J.)

REP. AUGUST PFLUGER (R-TEXAS)

REP. KAT CAMMACK (R-FLA.)

REP. JOHN KATKO (R-N.Y.), EX-OFFICIO

CROWDSTRIKE SENIOR VICE PRESIDENT FOR INTELLIGENCE ADAM MEYERS

AMERICAN WATER WORKS ASSOCIATION FEDERAL RELATIONS MANAGER KEVIN MORLEY

FINANCIAL SERVICES INFORMATION SHARING AND ANALYSIS CENTER CHIEF EXECUTIVE OFFICER STEVEN SILBERSTEIN

TENABLE, INC. CHAIRMAN AMIT YORAN

[*]RITCHIE TORRES: The Committee on Homeland Security will be in order. Without objection, the chair is authorized to declare the committee in recess at any point. Good afternoon. Before we begin today's hearing, I want to extend sincere condolences on behalf of the Committee to the Family of Chairman Don Young, Dean of the House, whose life was celebrated at a memorial last week.

Chairman Young's decades of service to the state of Alaska and to this great nation will never be forgotten. Our thoughts are with his loved ones at this most difficult time. Today the committee is meeting to examine how we can better secure our nation's critical infrastructure against Russian cyber threats.

Just over one month ago, Russian troops launched an unprovoked, unjustified invasion of Ukraine. The United States and its allies responded swiftly and decisively, imposing harsh sanctions against Russian financial institutions, Russian government leaders and oligarchs, and even Vladimir Putin himself. The Biden administration has also banned the import of Russian crude oil, petroleum and natural gas, imposed export controls of critical technologies, and worked with our allies to ban Russia's largest banks from SWIFT. In time, these restrictions, together with additional actions taken by the United States and its allies, will cripple the Russian economy and undermine Putin's ability to continue his ill-conceived military operation in Ukraine.

As Russia continues to struggle under the weight of sanctions imposed by the world's democracies, we must consider the potential risk to the homeland. Over the past decade, Russia has demonstrated its ability and willingness to use cyber tools to advance its global agenda. It has used its neighbors in Eastern Europe as testbeds for deploying its cyber capabilities to interfere with elections, spread disinformation and disrupt critical infrastructure.

In 2015 and 2016 for example, Russian hackers temporarily knocked out power to over 200,000 Ukrainians. In 2017, Russia unleashed NotPetya to disrupt Ukraine's financial system, but the malware affected networks across critical infrastructure sectors globally, including in the United States. Russia's willingness to deploy its cyber capabilities against the United States is similarly well-documented.

Since at least 2008, the intelligence community has warned of Russia's formidable cyber capabilities in its Annual Threat Assessment. In 2017, the intelligence community concluded that the Russian government had attempted to interfere in the 2016 Presidential elections, engaging in both information operations and targeting election infrastructure.

The following year, DHS and FBI warned entities in a range of sectors, from energy and aviation, to water and critical manufacturing, that the Russian government was attempting to gain access to their networks. Despite these warnings, the federal government and its private sector partners have been slow to chart an enduring course for strategic partnership.

Historically, the federal government has struggled to demonstrate the security value of public-private partnerships. Meanwhile, the private sector has been reluctant to fully engage and feared new regulations. One of the most frustrating challenges we face is the lack of urgency to act based on intelligence alone.

Too often it has taken a major incident to force change. The SolarWinds supply chain attack is a good example. It forced a collective shift from passively observing policy problems to actively solving them. The President issued an executive order overhauling and modernizing the federal government's approach to securing its networks.

Congress has also stepped up. It has increased cybersecurity funding and provided the administration with new authorities, including Incident Reporting and CyberSentry that will help detect and disrupt malicious cyber campaigns faster. And the private sector has come to the table to work with the federal government in new ways.

The administration, Congress and our private-sector partners have acted with urgency over the past year and left us better prepared to defend US networks. But there is still room to improve. First, the Biden administration has engaged in unprecedented cyber threat information and intelligence sharing with critical infrastructure owners and operators in advance of and during Russia's unprovoked invasion of Ukraine.

Moving forward, the government and private sector must assess the effectiveness of existing partnerships, and continue to deepen strategic collaboration to defend against current and future cyber threats. Second, the administration has undertaken historic initiatives to raise the cybersecurity posture across all 16 critical infrastructure sectors, which varies dramatically due to a range of factors from resources to regulation.

To effectively defend against Russian cyber threats, the federal government must tailor its support to and collaboration with critical infrastructure sectors to their varying degrees of capability. For that end I was pleased to see the President's budget proposal. The President proposed a new competitive ramp program aimed at raising the cybersecurity posture of certain critical infrastructure sectors.

Finally, the federal government and the private sector must work together to harness the security gains realized as we defend against Russian cyber threats in order to establish a new heightened security baseline. I look forward to the witnesses' testimony and the members' questions. I now recognize ranking member of the full committee, the gentleman from New York, Mr. Katko for an opening statement.

JOHN KATKO: Thank you, Chairman Torres for hosting this hearing today, and I thank you to the witnesses for being here. It's a very important topic obviously. Each of you play an extremely important role in the increasingly interconnected web of services that continues in our nation's cybersecurity and critical infrastructure security realm.

In fact, all of us here today play an important role in that ecosystem. We each have a job to do, and as we have repeatedly seen, one misstep can have disastrous consequences for the nation's infrastructure and the communities we represent. There has never been a more important time for our businesses, our state and local governments, and our federal government to be prepared not just to defend against cyberattacks, but to be resilient should an attack occur.

As the Biden administration recently said, there is quote, "Evolving intelligence that the Russian government is exploring options for potential cyberattacks," end quote. I don't need to tell you today what that might mean for our constituents or in the case of our panel, your customers and clients. Looking ahead at some of the particularly tangible attacks over the past few years, we can see that the motives have been either a financial game or intelligence gathering, not pure destruction.

But what if the goal was pure destruction? What if the goal was pure destruction? What if destructive attacks happened on critical infrastructure simultaneously. We saw this in 2017 with the NotPetya attack, which was a purely destructive campaign originally aimed at Ukrainian networks by Russian attackers, but quickly spun out of control and ultimately caused over $10 billion in damages globally.

It impacted global shipping for weeks, and wreaked havoc for companies around the world. There is so much this body should be doing to prepare for this type of threat, and thankfully we have recently taken significant steps to make our country safer. Just two weeks ago, the Cyber Incident Reporting for Critical Infrastructure Act was signed into law as part of the Omnibus Appropriations Bill for fiscal year 2022. This is one of the most important pieces of cybersecurity legislation in the past decade.

No one will argue with that. Enhanced reporting to the Cybersecurity and Infrastructure Security Agency or CISA on significant cyber incidents and ransomware attacks on critical infrastructure will mean greater visibility for the federal government, earlier disruptions on malicious cyber campaigns, and better information and threat intelligence going back out to the private sector so it can defend against future attacks.

This legislation also solidifies CISA's role as a lead federal agency for cybersecurity. I want to thank my colleagues in both the House and Senate, as well as the private sector, for their partnership and support in getting this most important piece of legislation across the finish line. The success of these tools is dependent on the success of the agencies we entrust them to, and fortunately we have the extremely capable CISA Director Jen Easterly and National Cyber Director Chris Inglis at the helm of our nation's cyber defenses.

They have been working tirelessly to keep us safe and I thank them for their work. However, their impact only extends as far as their mandate. It is up to all of us, especially those of you here today as industry leaders, to keep your companies, clients and customers, our very constituents, secure and resilient.

I look forward to hearing from you all about your partnerships with CISA, what more do you need from the federal government, what you don't need from the federal government, and the actions you're taking to secure our critical infrastructure. With that, Mr. Chairman, I yield back.

RITCHIE TORRES: Other members of the committee are reminded that under the committee's rules, opening statements may be submitted for the record. Members are also reminded that the committee will operate according to the guidelines laid out by the Chairman and Ranking Member in our February 3, 2021 colloquy regarding remote procedures.

I now welcome our panel of witnesses. Our first witness, Mr. Adam Meyers is the senior vice president of intelligence at CrowdStrike. In that capacity Mr. Meyers directs a team of cyberthreat experts as they track criminal, state-sponsored and nationalist cyber adversary groups across the globe. Our second witness, Mr. Steve Silberstein is the CEO of the Financial Services ISAC, where he leads efforts to increase the value of information sharing and the financial services sector, and improve how member organizations share critical information within the private sector and within government.

And our third witness, Dr. Kevin Morley, is a manager of federal relations at the American Water Works Association. Dr. Morley works closely with multiple organizations to advance the security and preparedness of the water sector. His role includes supporting the development of standards that represent the minimum best practices for water sector risk and resilience management, including cybersecurity guidance.

Our final witness Mr. Amit Yoran, who's the chairman and CEO of Tenable. Mr. Yoran works with organizations to understand and reduce their cybersecurity risk. Prior he served as a founding director of the United States Computer Emergency Readiness Team US-CERT Program at DHS and is a recognized security thought leader on operational technology.

Without objection, the witnesses' full statements will be included in the record. I now ask each witness to summarize his statement for five minutes, beginning with Mr. Meyers.

ADAM MEYERS: Congressman Torres, Ranking Member Katko and members of the committee, thank you for the opportunity to testify today. As the world watches the conflict in Ukraine unfold, this hearing evaluating the posture of critical infrastructure security is particularly timely. Across the country, cybersecurity professionals in government and industry are on high alert monitoring for the use of cyber operations within the conflict itself, and preparing for the possibility of Russian attacks against US critical infrastructure.

CrowdStrike has supported cybersecurity initiatives for the US government and key allied governments across the globe. We actively participate in public-private partnerships such as CISA's JCDC which we have worked with select industry partners to disrupt Russian infrastructure preparing for cyber operations.

It is CrowdStrike's goal to raise the cost of doing business for threat actors across the globe through our research, technology and partnership. In the immediate lead up to the 2022 conflict in Ukraine, Russian-nexus adversaries engaged in espionage, as well as disruptive and destructive attacks against government and commercial targets.

The commencement of the conflict also activated Russian eCrime and hacktivist actors. Russia has a long history of leveraging cyber operations to effectuate political goals. Russian cyber operations against Ukraine began in earnest following the Euromaidan protests in 2013. Attacks in 2015 and 2016 targeted critical infrastructure, famously disrupting power and distribution in Ukraine, and the NotPetya attack of 2017 caused a reported $10 billion in damages across the globe.

Numerous adversaries have contributed to the asymmetric campaign waged against Ukraine. One notable example observed in 2014 was a coordinated campaign targeting the Central Election Committee and Ukrainian media sector, which CrowdStrike attributes to BERSERK BEAR, an adversary group believed to be related to the FSB. As Russia began to amass forces on the Ukrainian border, Russian cyber threat activity targeting this nation increased in kind.

Beginning in mid-January 2022, website defacements, data theft and destructive wiper attacks impacted numerous Ukrainian entities. The wiper attack and website defacements occurred immediately following a series of bilateral meetings between the US and Russia regarding troop deployments. CrowdStrike currently associates

these activities with the Russian-nexus threat actor we've designated EMBER BEAR, an adversary group that has operated against government and military organizations in Eastern Europe since early 2021. On 23 February, a second wiper attack was identified, which CrowdStrike tracks as DriveSlayer.

More technically sophisticated than the EMBER BEAR activity from January, it is propagated by a worm allowing it to spread autonomously. The technical complexity and overlaps of tactics is consistent with previous operations, and bears striking similarity to the NotPetya attack of 2017. The conflict in Ukraine has also impacted, perhaps even reshaped, the cyber criminal threat landscape.

This is notable because Russia has long harbored and potentially leveraged for policy or political ends, eCrime threat actors. These adversaries now have potential to act in support of Russian state goals by acting as an irregular component performing disruptive attacks through ransomware around the globe, and specifically in the United States.

The conflict catalyzed a significant level of both pro-Russian and pro-Ukrainian hacktivists. One pro-Russian group claimed a series of distributed denial of service attacks against Polish and Latvian government sites, and targeted the National Bank of Poland. In a warning, they issued a reminder about the REvil ransomware which disrupted US critical infrastructure last spring.

While US critical infrastructure operators are increasingly focused on the threat from Russia, defensive capabilities differ significantly across the sectors. As sanctions by the US and allies mount in scope and impact, the risk of targeted attacks against them becomes more acute. The US government has made significant strides over the past several years in coordinating with industry against cyber threats.

The establishment of JCDC in particular, where CrowdStrike participates is a plank holder, has helped strengthen industry and government collaboration. Russian activity to date has been modest relative to early fears. However, this could change at any time. US critical infrastructure operators must remain on high alert.

Critical infrastructure operators must still do cybersecurity well. This is a last mile problem that cannot be solved through policy initiatives alone. Though not an exhaustive list, entities should develop and maintain a skilled workforce, and leverage measures identified in the executive order, such as the use of modern tools like Multifactor Authentication, Endpoint Detection and Response, and Zero Trust Architectures, and also proactive threat hunting.

I'll close by briefly highlighting recent collaboration with government and industry counterparts, Cloudflare and Ping Identity to launch a free critical infrastructure defense project for the energy, water and hospital sectors. We encourage eligible entities to consider participating in this program. Thank you for the opportunity to testify before you today.

I look forward to your questions and continued discussion.

RITCHIE TORRES: Thank you for your testimony. I now recognize Dr. Morley to summarize his statement for five minutes.

KEVIN MORLEY: Good morning, Chairman. Congressman Torres, Ranking Member Katko, members of the committee, I appreciate this opportunity to discuss cybersecurity in the water sector and the support provided by our federal partners. Our members represent water systems, large and small, municipal, investor owned, urban and rural that protect public health and the environment and enhance the quality of life.

In the modern era of utility operations this mission also includes managing cybersecurity risks that may threaten the essential lifeline function that water professionals provide 24/7 365. The current threat situation illustrates both the necessity and the strength of continuous two-way engagement, the value of partnership that is necessary to jointly manage cyber threats facing our nation.

AWWA recognizes the cybersecurity challenge, and believes a new approach is necessary, one that recognizes the technical and financial challenges facing the sector. This approach would set minimum cybersecurity standards for all types of water systems, an effort that will provide a tiered risk-based and performance-based set of requirements modeled on a similar approach applied in the electric sector.

Federal oversight for such approach would be provided by EPA given their existing statutory role in the water sector. AWWA stands ready to work with Congress, the sector and our federal partners to implement a strategy that supports sustainable cybersecurity protection that recognizes the variability in water systems across the nation.

In late December, working with our sector partners EPA and CISA, we reached out through EPA to 58,000 water systems, alerting them to Russian cyber-threat activities identified by CISA. The associated advisories have been shared across multiple communication platforms to ensure the widest possible distribution.

These engagements help professional organizations like AWWA to amplify the message of our federal partners about the evolving threat environment. The new Shields Up campaign deployed by CISA has been very well received, and represents a welcome reorganization of the information available to critical infrastructure systems.

In many cases, however, advisories and alerts are highly technical, may be difficult to implement by entities that lack in-house cybersecurity expertise. To enhance the effectiveness of information sharing, we recommend that CISA work with EPA and partners like AWWA, WaterISAC and the Water Sector Coordinating Council to properly contextualize threat information and ensure that the information transmit is concise and actionable.

In addition, expedient declassification of threat intelligence is essential. Where there is often tension getting information moved to the unclassified level, in reality, most entities simply want two things. What is the vulnerability, what is the solution to mitigate it? AWWA's cybersecurity guidance and assessment tool first issued in 2014 have been updated regularly.

They support the water sector's use of the NIST cybersecurity framework, and help community water systems to address the cyber provisions implemented by Congress in America's Water Infrastructure Act of 2018. These resources also support the recommendations in several executive orders, recent national security memorandums and ANSI/AWWA standards.

Coordination with EPA, NIST and CISA was essential in developing these resources, which provide a strong foundation for cybersecurity risk management. I do want to highlight CISA's Cyber Hygiene program, a service that I believe provides some of the most immediate risk reduction benefits to users. We recommend the EPA, CISA and the sector organizations coordinate on a unified outreach campaign to increase deployment of Cy-Hy to water systems, especially small and medium utilities.

CISA and EPA are currently working with the Water Sector Coordinating Council on the Industrial Control System Cybersecurity Initiative. This 100-day action plan will review the scalability of ICS monitoring technology deployment and establish information sharing protocols with our federal partners. Partnership is a key element of AWWA cybersecurity risk management activities.

I just want to share with you two quick examples. We've partnered with CISA and Idaho National Lab to integrate the findings of our assessment tool with CISA's Cyber Security Evaluation Tool, CEST. In addition, over the last several years, we've worked with EPA, USDA, partners like RCAP under grants to provide guidance and training to systems serving less than 10,000 people.

We encourage continued investment and support for this type of capacity development, considering there are more than 40,000 community water systems that serve less than 3,300 people. In summary, these are demonstrations of the value and power of collaborative partnership between the water sector and our federal partners.

We welcome the opportunity to build on these successful engagements using a framework that is adaptive to the dynamic nature of the threat, recognizes the variability in operational complexity and system maturity, and the reality of the financial and technical capacity challenges facing our nation's water systems.

I thank this opportunity to speak with the committee and look forward to your questions.

RITCHIE TORRES: Thank you for your testimony. I now recognize Mr. Silberstein to summarize the statement for five minutes.

STEVEN SILBERSTEIN: Thank you, Chairman Torres, Ranking Member Katko and honorable members of the committee for this opportunity to testify. I'm Steven Silberstein, CEO of the Financial Services Information Sharing and Analysis Center known as FS-ISAC. You should know up front that the financial sector is well-situated to navigate the current threat environment, but remains highly vigilant not knowing what may come next.

Financial sections suggest the sector to be a distinct target, but the sector benefits from an historic security experience dating back to the days of physical safes to protect cash. Before adding details, I'd like to explain the role of FS-ISAC within the sector. FS-ISAC exists to foster the resilience of the global financial services sector and its customers.

As a private nonprofit association, FS-ISAC membership consists of approximately 5,000 financial institutions in nearly 70 countries, that together represent $100 trillion of deposits and assets under custody. We manage this critical cyber community with more than 100 staff situated around the globe. FS-ISAC is the global cyber intelligence sharing community for the financial sector, allowing us to take a follow-the-sun approach.

The highly competitive financial service industry recognizes that collaboration around cybersecurity is a must, just as historically cooperated to establish clearinghouses and exchanges where all parties can meet to complete a transaction. Similarly, cybercriminals don't target just one institution. Instead, they try to maximize their investment by attacking many.

If one firm notices that its systems are being targeted, it will share this information with its peers through the FS-ISAC, empowering other members to prepare and defend against an attack before it happens to them. And with a sector-wide view, we're better able to prepare firms for emerging threats and new vulnerabilities.

In addition to our operational mission, we've been an active member of the Financial Services Sector Coordinating Council, FSSCC, since its inception 20 years ago. The Council is comprised of the sector's key operators and associations through which nearly the entire sector is represented. Let me switch to the effective role played by our public-sector partners during this current incident and this must be acknowledged.

We applaud the Biden-Harris administration and the sharing of information throughout the escalating situation in Eastern Europe and the Russian invasion of Ukraine. The sector appreciates the paradigm shift from reactive to proactive sharing of information. The repeated and consistent messaging and realistic context provided by CISA, the Cybersecurity Information Sharing Agency, joined by the NSA, US Treasury, FBI and other government organizations has allowed our sector to institute the necessary security precautions, and motivated institutions to conduct timely reviews of their cyber hygiene and incident response plans.

Following the standup of the Unified Coordination Group, UCG, by the Department of Homeland Security last month, Treasury and CISA leadership engaged with the sector to develop a joint playbook for how the government and industry may communicate and engage during incident response and recovery for this critical sector during the current heightened tensions.

Also as noted by my colleagues, CISA's new JCDC, Joint Cyber Defense Collaborative, provides a key communications channel, fostering real-time information sharing among the sector, CISA, US Treasury, critical infrastructure and other stakeholders. The JCDC enables our analysts to engage with sector-specific insights and review technical exchanges for sector implications, again for sector distribution.

As I speak, the financial sector has not experienced an increased level of cyberattacks directly attributable to Russia. We're always tracking the continuous background noise of low-level cyberattacks and reconnaissance missions. However, outside of the conflict zone, we're not seeing any significant uptick in attacks attributable to any specific geography or threat actor.

But the early and continued sharing of warnings and technical information both by CISA and the government have prompted the financial sector to open emergency communications channels at the end of last year. We activated the sector's Core Executive Response Group, which is part of our all-hazards playbook.

And on this recurring call, government leadership from Treasury, CISA and regulators communicate and provide updates on emerging vulnerabilities and associated mitigations and resiliency plans for the sector. Over the last 100 days, the sector's various information channels have effectively amplified the government's warnings, alerts and available resources, and we participated in a useful array of classified and unclassified stakeholder engagements.

In conclusion, I would like to share that FS-ISAC and our fellow sector organizations stand ready to work with the administration, Congress and this committee in any way we can protect the financial sector, its customers and economic security. The direction of sharing has been very effective, and we are optimistic that it will continue and advance security for all.

Thank you again for the opportunity today, and happy to answer any questions when they come.

RITCHIE TORRES: Thank you for your testimony. I now recognize Mr. Yoran to summarize his statement for five minutes.

AMIT YORAN: Thank you, Chairman Torres, Ranking Member Katko, members of the Committee. Thank you for the opportunity to testify today and your leadership during this incredibly important time. I am Amit Yoran, chairman and CEO of Tenable. With over 40,000 customers worldwide, including just about every federal department and agency, a majority of the Fortune 500 and numerous Global 2000 organizations, Tenable is the world's leading provider of vulnerability management and cyber risk assessment capabilities.

Recently, LAPSUS$ has shown that with only $25,000, a group of teenagers could get into organizations with mature cybersecurity practices. Consider Russia, with much deeper pockets, focus and mission targeting critical infrastructure. That should be a sobering if not terrifying call to action. US critical infrastructure is a complex network of 16 interconnected sectors, each with varying degrees of cybersecurity preparedness and risk management practices.

Many organizations increasingly interconnect IT and OT systems in pursuit of improved efficiency resulting in increased vulnerability. These risks are exacerbated when exposing slow moving, highly structured environments to the pace, speed and dynamic threats introduced through the IT world. Last year's Colonial Pipeline and ensuing gas supply failures serve as a stark example of the potential impact of increasing IT/OT convergence and the importance of basic cyber hygiene.

Government policy should not allow for learned helplessness by government agencies or private industry. There's too much at stake for individuals and organizations to remain negligent, not taking even the basic steps to improve their cyber posture and manage cyber risk proactively. CISA has already recommended best practices that organizations can implement to prepare themselves from a cyber perspective through its Shields Up initiative.

These recommendations align strongly with the best practice recommendations of numerous security advocacy groups, industry associations, working groups and regulatory bodies. Organizations that fail to implement these basic steps should be held accountable. The SEC's proposed Cybersecurity Risk Management, Strategy, Governance and Disclosure would require public companies to disclose their policies and procedures for identifying and managing cybersecurity risks, management's role in implementing cyber policies and procedures, and the Board of Directors' cybersecurity expertise.

This proposal stands alongside the recently-passed cyber incident reporting legislation for timely and transparent notification of cyber breaches as the two actions that would most dramatically improve our cybersecurity preparedness as a nation. Requiring greater transparency of cyber-risk practices and oversight forces companies to treat cybersecurity risk as business risk, and will lead to stronger cybersecurity governance and accountability among corporate leaders and boards.

This results in more effective cybersecurity, period. For decades now, critical infrastructure operators have highlighted the complexity, impracticality and challenges of updating infrastructure software, applying patches and hardening their systems will not minimize the seemingly overwhelming nature of these tasks from where we sit today.

But these things can be done. We should be able to design, develop and deploy critical infrastructure software that's capable of being patched and operated in a protected, secure and resilient fashion. And I can tell you that unless we make a stand, unless we show our resolve, unless we demonstrate our commitment to a more secure future, there will be a hearing like this one decades from now, wondering why responsible action wasn't taken.

While Americans remain at strategic risk, we can only conclude that market forces around cybersecurity have not achieved successful equilibrium. Free markets work best with risk-informed decision-making and transparency. Pushing for such a regulatory regime should be a nonpartisan effort, and such an effort would fuel, not stifle, innovation, discover new approaches in cybersecurity and new approaches in critical infrastructure service delivery.

Thank you again, Chairman Torres, Ranking Member Katko and all the members of the Committee for your attention to this important topic. I look forward to working with you and your colleagues as cybersecurity remains a critical issue facing our nation and economic security. I appreciate the opportunity to testify today and look forward to answering your questions.

RITCHIE TORRES: I thank the witnesses for their testimony. I will remind each member that he or she will have five minutes to question the witnesses. I will now recognize myself for questions. Ransomware attacks that have stolen billions of dollars from American households, businesses and governments have come disproportionately

from Russian cyber threats.

SolarWinds, the largest espionage campaign in history, Colonial Pipeline, the largest breach of energy infrastructure in history, JBS, the largest breach of food infrastructure in history, all of these intrusions came from Russian cyber threats. Mr. Meyers, would it be fair to think of Russia as a superpower in cyberspace?

ADAM MEYERS: Yes, Congressman. I think that Russia has demonstrated through numerous years and numerous campaigns significant technical capabilities and intent to target Western and US infrastructure.

RITCHIE TORRES: And even though the United States may have more cyber capabilities than Russia, there's a sense in which the United States might have more cyber vulnerabilities, because American infrastructure tends to be more automated, more computerized. Is that a fair assessment?

ADAM MEYERS: Yes, sir.

RITCHIE TORRES: We would never expect an American business in a physical conflict to defend itself successfully against a superpower like Russia. Is it reasonable and realistic to expect an American business in a cyber conflict to defend itself successfully against a cyber superpower? Mr. Yoran, do you have any thoughts on that?

AMIT YORAN: I don't think it's reasonable to expect that all critical infrastructure operatives would be able to defend themselves in totality against a sophisticated cyber superpower like Russia. I do think it's reasonable to expect that they exercise a good standard of care with their system, including maintaining their systems in good repair, searching for vulnerabilities, fixing vulnerabilities, addressing high priority threats that CISA and others have shared with them.

And in doing so, I think they can significantly reduce their exposure and probability of causing significant outage.

RITCHIE TORRES: Should the US Government assume a greater role in defending privately owned and operated critical infrastructure, a role that extends beyond public awareness campaigns and voluntary public private partnerships?

AMIT YORAN: I don't think the US government should be in the cyber defense role where they're defending critical networks and critical infrastructure, where they might not understand the changes that they might make and how those might impact the critical infrastructure. It's incumbent upon those operators which understand the systems, how those systems operate, how they work together, and how they fit to defend those networks, with help from intelligence, information and prioritization from their government partners.

RITCHIE TORRES: Should the federal government mandate best practices in cyber hygiene like Multifactor Authentication across all the sectors of critical infrastructure?

AMIT YORAN: I believe that each, and I'm going to keep answering questions unless one of my colleagues jumps in or unless of these questions are directed at me, I believe it's critical important for the federal government to mandate cyber best practices, noting however that there is not one cyber best practice across all critical infrastructures, and that the regulatory agencies and sector-specific agencies should work with CISA and their private-sector counterparts to develop and maintain those best practices.

RITCHIE TORRES: Mr. Meyers, should we mandate Multifactor Authentication across all sectors of critical infrastructure?

ADAM MEYERS: I would point to the executive order and the recommendations there as a good example. As far as mandating, I think that there is not necessarily a deep understanding of how these systems are architected and leveraged in the commercial sector. So I think recommendations are probably a good first step.

RITCHIE TORRES: In February of 2021, a hacker broke into the local water system for Oldsmar, Florida, a town of 15,000 people, and raised the sodium hydroxide levels in an attempt to poison the water supply. There are tens of thousands of water systems in America, and most of them are run by local governments that often lack the wherewithal to sufficiently invest in their own cybersecurity.

And the Foundation for Defense of Democracies has been sounding the alarm about water infrastructure as the weakest link in the critical infrastructure chain, and the Foundation for Defense of Democracies, the Government Accountability Office, the Cyber Space Solarium Commission, all of these entities have been critical of the EPA's performance as the Sector Risk Management Agency.

Dr. Morley, how can a water system that is so fragile and so fragmented and so federated be secured from Russian cyber threats?

KEVIN MORLEY: Sure, I recognize the question, sir, and I believe that some of that recognizes some of the capacity issues that we've identified in the sector as being challenges in implementation of certain cybersecurity best practices. That would be a great example of where further implementation of the Cy-Hy program would be very beneficial to a community like Oldsmar or other utility systems.

There's also the reason why AWWA has developed a white paper talking about a framework, a new governance approach for cybersecurity in the water sector, a collaborative process modeled on what's in the electric sector. We welcome the opportunity to discuss that further.

RITCHIE TORRES: I now recognize the ranking member of the full committee, the gentleman from New York, Mr. Katko for questions.

JOHN KATKO: Thank you, Mr. Chairman, and thank you all for your testimony today. You know, when I first came on this committee seven plus years ago, ISIS was for sure the greatest threat to our country, ISIS-inspired terrorist attacks in this country, and they manifest themselves in several cataclysmic events like in San Bernardino and the Pulse Nightclub and many others.

That threat dynamic has changed dramatically for the homeland since then. We've done a much better job dealing with those types of incidents. ISIS has been degraded but not eliminated, so the threat persists, but it's not like it was. But the greatest threat that's to our country right now in my mind for sure is what we're talking about today, cybersecurity and the threat of cyberattacks against this country.

And I noted some in my opening statement over the past few years, we have had many very serious attacks, and China clearly has state actors perpetrating those attacks. Russia has gangs, if you will, within Russia that operate under the imprimatur of the Russian government and at their disposal, but needed to do so. And given the conflict in Ukraine, obviously that is a big concern right now.

And with that is setting the table, what I'm trying to figure out and understand is, what is most vulnerable and how do you go about helping it? And there is a tug and pull between, is it just good old-fashioned government regulation, or is it good old-fashioned government assistance and letting the private sector be partners with them?

And I'm informed by what I saw in my time as a prosecutor when terrorism, 9/11 happened, I was a prosecutor, and instead of a whole new realm of regulations, we had partnerships, and that's what the Joint Terrorism Task Force is. And that's my view of CISA is, is a partnership, a partnership with the private sector, right, and then to give them the tools they need to work with the private sector.

And by the way, if you want an incentive to secure your systems, if there's technology out there and you're not securing your systems with that technology that's reasonably attainable for you, and you get hacked, you're going to be vulnerable to lawsuits from your shareholders, and you damn well you should.

So there's a state-of-the-art component to this that's here that we need to talk about as well. So I think it's incumbent upon CISA to be not the regulator, but to be the facilitator and the partner with the private sector. And I think what's going on lately with the Log4J and some of these other things, we're seeing that partnership really kind of blossom and is being very productive.

So I'm excited for that, but right now Mr. Yoran, and I you know Mr. Morley you talked about it a little bit, the water sector, but I want to ask you Mr. Yoran, where do you think the water sector and wastewater systems fall within the realm of critical infrastructure and as well as are cybersecurity defenses?

AMIT YORAN: It's a great question, Congressman. I think the water sector, and within each sector, there's varying degrees of sophistication and capability, it's true in the financial services sector, it's true in the electric sector and it's true in the water sector, and so some are much more sophisticated than others.

I do think the financial services sector as an example, the IT sector as an example, have been much more forward leaning about cybersecurity and stand today much better prepared. They've been facing and their understanding of the risk they've been facing for years now is more sophisticated. I think the water sector, a lot of, a lot of the industrial heavy sectors are much more deliberate, their infrastructures move much more slowly, but they've been interconnecting their operational technologies with their IT technologies.

And so the pace of risk that these sectors are facing has really increased over recent years. And so I think a lot of work remains to be done in some of these sectors.

JOHN KATKO: OK. Now for all of you, I only have about a minute left, so I'll ask you this open-ended question. We've got to identify it's a systemically important critical infrastructure within a critical infrastructure sector and then we've got to do something about it, right. And we understand it's going to be a partnership and we've got to work with the private sector.

I mean what is it that we can do to help CISA be better at working with you and strengthening those partnerships and addressing those vulnerabilities? Mr. Marley or Mr. Meyers, how about you go first?

ADAM MEYERS: Thank you. Having worked with CISA through JCDC on the Log4J and now in the most recent escalations in Eastern Europe, I think information sharing has been absolutely critical. CISA has done a phenomenal job of not only sharing information but standing up systems for rapid information sharing between partners and CISA to have more tactical-type communications.

And I think that fostering those types of environments and that information sharing is absolutely critical. And I also think from a defensive perspective, the vulnerabilities that CISA has highlighted as being critical to fix, the Shields Up program as well as some of the other initiatives that they've rolled out have been very effective.

And I'd like to see that continue.

JOHN KATKO: I know I'm out of time Mr. Chairman, so I appreciate your indulgence. I have a lot more to ask you all. Please keep coming to me and talking to me because I want to hear more about it going forward. This is very important. Thank you. I yield back.

RITCHIE TORRES: I now recognize the gentleman from Rhode Island, Mr. Langevin.

JIM LANGEVIN: Thank you, Mr. Chairman, I want to welcome my witnesses today. I appreciate your testimony and your expertise in cyber, particularly hello to Amid. Good to see you again. So let me begin on this question. The elevated cyber threats to our critical infrastructure systems illustrate that while we've come a long way in improving the nation's cybersecurity over the last few years, much work still remains to be done.

In particular, I believe that we must develop a better understanding of the vulnerabilities present within key technologies that underpin our networks and critical infrastructure. So one of the Cyberspace Solarium Commission's recommendations currently reflected in an amendment to the America COMPETES Act would establish critical technology security centers through grants to universities and FFRDCs to create a comprehensive and centralized security testing ecosystem for foundational critical technologies like networked industrial control systems and open-source software.

So if I could, for Mr. Yoran, I'll start with you. How might such an initiative to identify, report, and in some cases support the remediation of vulnerabilities in these critical technologies inform and improve risk mitigation efforts for critical infrastructure?

AMIT YORAN: Good to see you Congressman, and thank you for your tremendous leadership on cyber issues over the course of so many years. I think it's important when we talk about these efforts to remember that there are such distinct differences between these critical infrastructures, and such distinct approaches which make more or less sense.

For instance, in the electric sector, in the financial services or IT sector, you see a very rapid pace of change. You see a high degree of cyber sophistication and agility to address issues as they might be highlighted by CISA or other government partners. As you move to more industrial systems and you connect IT and OT systems, you see the IT side of the house sometimes able to deal with these vulnerabilities and advance notice from government partners.

And you see in many cases, the OT side of the house as much more slow moving and deliberate. And while that may sound bad from a cybersecurity practitioner standpoint, and it does mean that systems will be vulnerable, those deliberate processes are in place for very specific reason, to make sure that we don't create accidental outages and things of that nature.

So I think there really needs to be a very different approach to protecting critical infrastructures when we join IT and OT systems together.

JIM LANGEVIN: Thanks. And so I'm hoping that these critical technology centers would do just that to identify those problems and help to remediate them ahead of time before there is a problem. Let me continue on with Amid too. Last week, the SEC proposed a rule requiring companies to disclose policies and practices for identifying and managing cybersecurity risks, management's role in implementing cyber policies and procedures, and cyber expertise across the board of directors.

On the Solarium Commission, we also called for an increased level of reporting on cybersecurity from publicly traded companies, because cyber risk is a business risk, and shareholders I believe should be able to discriminate between companies that take cybersecurity seriously and those that don't. So in your testimony, you referenced this proposed rule as and I quote, "The single action that would most dramatically improve our cybersecurity preparedness as a nation." I agree with that statement, but could you talk about this proposed rule and why you feel it could make such an impact?

AMIT YORAN: Yeah, and I think there are two critical components to transparency. One, I think, recent legislation was terrific in requiring breach notification to CISA so that action can be taken, information can be shared and our critical infrastructure is better protected. The second piece of that is having greater transparency, starting with public companies around what their cybersecurity risk management practices look like.

That type of transparency will cause corporate leadership to pay closer attention, will cause boards of directors to pay closer attention to cybersecurity. And by paying closer attention, I feel fairly certain that that would cause improved focus on and improvement in cybersecurity practices. That is critically important for shareholders to make informed decisions about their investments.

It's critically important for customers to make important decisions about whose technologies they trust and don't trust. So I think it is absolutely critical for the free market to work that we have that level of transparency of both cybersecurity practices, risk management and transparency around breaches.

JIM LANGEVIN: Thank you very much. I know my time's expired. I do have one more question that I'll submit for the record for Dr. Morley, unless we go for a second round, Mr. Chairman.

RITCHIE TORRES: Absolutely. I now recognize the gentleman from North Carolina, Mr. Bishop for questions.

DAN BISHOP: Thank you, Mr. Chairman. Mr. Meyers, CrowdStrike was the firm that diagnosed the alleged Russian hack of the DNC server in 2016? Is that correct?

ADAM MEYERS: Yes, sir.

DAN BISHOP: Has CrowdStrike been contacted by the Office of Special Counsel, Mr. Durham's office?

ADAM MEYERS: I'm not sure.

DAN BISHOP: CrowdStrike I understand the FBI concluded that there had been a Russian hack based on a report provided by CrowdStrike that was provided to the Perkins Curry law firm. Do you know that to be true?

ADAM MEYERS: Yes, we published our findings in a blog post in 2016.

DAN BISHOP: Do you know, my understanding is that the report, the version of the report provided to the FBI was heavily redacted. Are you aware of that?

ADAM MEYERS: I'm not aware of that.

DAN BISHOP: Do you know of any reason that CrowdStrike cannot publish or release to the public or release to this committee a complete and unredacted version of that report?

ADAM MEYERS: I'm not exactly sure which report you're referring to, but happy to follow up with you and get anything that we can. Alright, thank you. I yield back.

RITCHIE TORRES: I now recognize the gentlewoman from Texas, Ms. Jackson Lee for questions. I now recognize the gentleman from California, Mr. Correa for questions. I now recognize Mr. Cleaver for questions. I now recognize Mr. Green for questions. Herein lies the challenge of the hybrid model. I now recognize Ms. Clarke for questions.

She's gone too. I now recognize Ms. Watson Coleman for questions. I actually see Ms. Rice, so I recognize Ms. Rice for questions. See by process of elimination.

KATHLEEN RICE: Thank you so much, Mr. Chairman. Thank you all so much for coming here today. This is such a critically important issue that we're discussing. Software and application code are known attack vectors for bad actors and critical infrastructure operators, especially those that rely on third-party vendors or open-source code to develop software or applications.

They need to be constantly on guard against vulnerabilities in their code, but it's harder than ever for industry and government alike to defend themselves. There was a recent report by Rapid7 that found that the average time for known vulnerabilities to be exploited dropped from 42 days last year to 12 days this year.

So attackers are getting faster, and it's harder to patch code in real time. At the same time, a State of Software Security Report released last week found that eight in ten software applications owned and operated by the public sector had a security flaw. So critical infrastructure only fared slightly better.

Same study found that 73 percent of financial service apps and 77 percent of health care apps contained security flaws. So Mr. Silberstein, you mentioned the importance of CISA's Shields Up webpage and ramped up communication since the war in Ukraine began. When a new vulnerability is discovered and posted to the Known Exploited Vulnerabilities Catalog, how do you disseminate that information to your members?

And if one of your members on their own discovers a flaw in open-source or vendor-developed code that may be used by other financial institutions, do they share that information with you and their peer institutions?

STEVEN SILBERSTEIN: Thank you Congresswoman for that question. We first try to, any public releases about vulnerabilities from any reputable source, we attempt to rapidly amplify to our whole membership with the minimum delay, with a focus and pointing to the immediate mitigations that can be put in place to prevent access to the vulnerability, because the challenges of patching can be large.

We saw that with Log4J where the time span, this was embedded in many systems, the time span for particularly larger organizations to get to every instance took days maybe more. So we put a focus on rapid mitigation, and we are also working with our partners in the whole supply chain to emphasize that as the headline in any disclosure of vulnerability, what do you do at this instant to shut that door while you then go fix the inside of the house.

Secondly, to your question on when members discover vulnerabilities, yes, we rapidly share across the full community and also to whatever source. Additionally, a lot of our membership are actively involved in the Alpha Omega program of the Open Software Federation, which is focusing on a proactive discovery of vulnerabilities and improving the open source community.

KATHLEEN RICE: Thank you for that, Dr. Morley, I only have about a minute and a half left, but you have emphasized the diversity of the water sector and the wide variety of cyber capabilities within it. When CISA announces a newly discovered vulnerability or issues recommendations on how to mitigate cyber threats from malign actors, are these understandable and actionable for your smallest members?

I mean, how does the AWWA help its least cyber-capable members build up their defenses?

KEVIN MORLEY: That's an excellent question, Congresswoman. We do our best to re-transmit that ourselves and with our partner organizations, including the WaterISAC. However, as I mentioned, certain advisories in some cases have a certain level of technical sophistication that probably require a little bit of contextualization.

And that's why we would encourage a little more front-end engagement between EPA and CISA to ensure that that information is actionable to our members at the smallest level.

KATHLEEN RICE: Thank you all very much. Mr. Chairman, I yield back.

RITCHIE TORRES: I now recognize the gentleman from Louisiana, Mr. Higgins.

CLAY HIGGINS: I thank the chairman and Ranking Member Katko, all the witnesses sharing today. Our critical infrastructure has certainly shown vulnerabilities across the United States and indeed the world, and the lessons that we learn increasingly are troubling regarding our own posture and strength, resiliency in our in American critical infrastructure.

So, the position of this committee must be to calmly seek solutions for the American people. And you gentlemen are going to be asked some challenging questions today, because it's an emerging understanding of just how vulnerable we can be to attack when we thought perhaps we were not. I have noted through the years as new

projects have been developed in my own district, in the oil and gas industry, petrochemical industry, LNG. I represent South Louisiana.

These massive projects have the capacity to be off the grid. They have their own electrical supply, massive generators. Should power be lost, they can continue running. They have their own water, deep water wells. They have on-premise servers and hardware systems. And I recall a study from as recently as 2019 that somewhere in over 90 percent of American businesses had some level of on-premise servers.

And therefore, it seems to me as a regular American with no background in cybersecurity until I came to Congress, and gentleman like Ranking Member Katko and others have made it a priority to push into the American narrative that we must strengthen our critical infrastructure and our cybersecurity is certainly going to be an increasing area of vulnerability.

Should we lose our grid for instance or just a large portion of our grids, 15, 20 percent of our grid, it's difficult to see how we would recover from that. So Mr. Yoran, am I pronouncing your name correctly?

AMIT YORAN: Yes, sir.

CLAY HIGGINS: Thank you, sir. Mr. Yoran, what would be your opinion regarding as we move forward from the federal level to encourage private business and local government entities to develop off-grid capabilities to insulate themselves from attack and to decrease their vulnerability?

AMIT YORAN: Congressman, That's a great question. I think one very important responsibility and opportunity that exists for the federal government is through sharing of information with the private sector around the threat, and what actions they can take to better protect themselves and mitigate risk. My greatest concern is that examples, like the one you are sharing from your district where you've got very remote pieces of equipment, are increasingly moving on grid, well I shouldn't say on grid, not power grid, onto the Internet in some form or fashion.

While there might not be an Internet line, they're deploying cellular or other communications mechanisms so they can get real-time telemetry from those remote sites, they can troubleshoot and they can identify where the equipment may be failing or may --

CLAY HIGGINS: So you would see that connection as a vulnerability that we need to watch?

AMIT YORAN: Exactly.

CLAY HIGGINS: I would concur. In the interest of time, I have one more question for you, sir. In America, we have codified into law the right to strike back if we come under fire. If you're fired upon, you've identified the threat and you returned fire. And yet in the cyber realm, that's not codified into law. Mr. Yoran, what's your opinion about what Congress should do about that?

Should we make it legal to strike back in the cyber realm? It's a legitimate question.

AMIT YORAN: Yes, sir, legitimate question. I think it should remain illegal for private industry or private citizens to strike back, but there's important role that is one of the critical functions for the US government.

CLAY HIGGINS: Under advisement. Mr. Chairman, I yield.

RITCHIE TORRES: Thank you. I now recognize the gentlewoman from Texas, Ms. Jackson Lee for questions.

SHEILA JACKSON LEE: Thank you and good morning to all of you. This is a very important hearing, and I'd like to submit three articles into the record. First, the excerpts from the House Intelligence Committee hearing on Russia to the New York Times. As I do that, let me read an excerpt from that article, "I've been authorized -- " This was the FBI director, "by the Department of Justice to confirm that the FBI, as part of our counterintelligence mission, is investigating the Russian government's efforts to interfere in the 2016 Presidential election, and that includes investigating the nature of any links between individuals associated with the Trump campaign and the Russian government, and whether there were any coordination between the campaign and Russia's efforts." I ask unanimous consent to submit that into the record.

RITCHIE TORRES: Without objection.

SHEILA JACKSON LEE: I ask unanimous consent to Here We Go Again article, Russia Gears Up to Interfere in 2020 election, April 30, 2020, and the Atlantic, Russia is Co-opting Angry Young Men, from the Atlantic, from the periodical seemingly Center for Diplomacy and Global. I ask unanimous consent, Mr. Chairman.

RITCHIE TORRES: Without objection.

SHEILA JACKSON LEE: Let me ask questions to Mr. Silberstein, Mr. Yoran. Mr. Silberstein, we are in a very difficult time, and again, I offer my deepest concern and sympathy to the people of Ukraine who are feeling the sting, the siege, the violence, the viciousness, the murderous behavior of Vladimir Putin. I can see him not taking any prisoners as it relates to the United States and his angst and anger against us. As it relates to your testimony, page four, line 11, that the consistent messaging and realistic context provided by the Federal Bureau of Investigations and other government has allowed your sector to prepare for and institute necessary security precautions.

Are there industry best practices regarding regional personnel evacuation plans? And why don't you answer this last question first, which industries would consider evacuation plans as a core component of a cyber incident response if it came particularly from really a established enemy at this time like Russia?

STEVEN SILBERSTEIN: Thank you, Congresswoman. If I may ask for a little clarification, referring to evacuation in the conflict zone or in another locale?

SHEILA JACKSON LEE: In the United States, if you're being attacked here.

STEVEN SILBERSTEIN: I think we have fairly good resiliency plans that unfortunately have been practiced around both natural disaster and COVID over the last ten years which would deal with suitable physical issues as far as personnel. Through COVID, we had widespread dislocation out of offices to the work-from home model as everyone is aware, and the sector was able to pretty successfully weather that.

SHEILA JACKSON LEE: I'll bypass the first question I asked then. Do you all have a sense of preparation from foreign intrusion such as Russia? It's been known that the intrusion before had been established with outside groups, I suppose it was governmental. Are you prepared for that?

STEVEN SILBERSTEIN: I believe the financial sector is. It does not differentiate in general between private enterprise against the sector versus the nation state attempts against us. But also realizes that nation state potentially comes with more power. And an important aspect of the sector's preparation is a very distinct let's not be complacent where there is no good-enough cybersecurity.

It's a continued attempt to keep up with adversaries, and just as technology evolves, the technology of the adversaries, as well as the technology and capability you need is in place.

SHEILA JACKSON LEE: Thank you. Mr. Yoran, you spoke about a famous Colonial Pipeline was hit by ransomware, particularly allegedly by criminal element. They went to great lengths to appear legitimate. But my question would be, if you can combine the answer as to those intrusions that try to appear legitimate, that the CEO of Colonial Pipeline, one, did not tell the United States timely, the government, paid $4.4 million in ransom to its Russian-based attacker DarkSide.

Do you agree with Colonial's position that paying the ransom was in that case the right thing to do? Are we expecting more of this, and particularly as Russia continues to act in terroristic manner? Mr. Yoran.

AMIT YORAN: It's a great question. I'm not familiar with the details of the decision-making process for Colonial, but assuming that their first and foremost objective was to get the pipeline up and operational, we all saw the challenges in getting gas and the supply shortages which were resulting. I do think that the important legislation which Congress has enacted now would require timely notification to CISA of that ransomware payment which is commendable.

SHEILA JACKSON LEE: Do you think there's a credible fear of Russia's continuing attempts to attack our local assets, our national assets?

RITCHIE TORRES: I just want to say your time has expired. So we're going to move on.

SHEILA JACKSON LEE: Mr. Chairman, thank you.

RITCHIE TORRES: I now recognize the gentleman from New Jersey, Mr. Van Drew for questions.

JEFFERSON VAN DREW: Thank you, Chairman and Ranking Member Katko, and thank you to the witnesses for testifying to the committee today. Unfortunately, we are here again addressing the exponential rise in cyber threats. Last year, 14 of the 16 critical infrastructure sectors experienced a ransomware attack of some type. These threats are real and they are still increasing.

A few years ago in my district, the Atlanta County Utilities Authority located in Egg Harbor Township, New Jersey, was the victim of a cyberattack. Utilities Authority reported an incident in which perpetrators gained unauthorized access to sensitive data of their customers. Additionally, operational information was withheld as the criminals demanded ransom.

Fortunately, the overall function of the authority was minimally impacted, but the fallout could have been far worse. Services like utility authorities are vital to day-to-day life, and it is imperative that Congress and the administration continue to invest in protecting critical infrastructure everywhere, small or large, in every way.

It affects every aspect of our life. Mr. Adam Meyers, you may be aware part of the Colonial Pipeline runs through my district. The pipeline and several other companies and industries have been victims of ransomware attack in recent years. And I'm concerned about the proliferation of these attacks. Why have they become more rampant?

And what can Congress do? And I know you've outlined some of this, but to really get to the rub, what could we do or do you think we should do, what more can we do to help organizations mitigate them? This is going to be the great challenge for the next how many years, I don't know, but for many, many years, and it's something that we need to do even better with.

What more would you, if you were the President or you could control everything, what would you do right now?

ADAM MEYERS: Thank you. That's a good and challenging question to answer. The increase in these attacks, I think first and foremost is occurring because these adversaries are making money. In the course of 2021, we observed somewhere around 50 or so ransomware incidents per week. The average ransom demand was around $6.1 million.

So in any given week, we were looking at around $300 million in potential ransom demands that were being issued to victims. This is something that I think we need to attack on multiple fronts. We need to think about it in terms of the financial viability. If we disrupt the financial viability of these operations for these threat actors and make it more expensive for them to operate, it's going to potentially reduce the incentive for them to conduct these types of operations.

Employing the right technology, many organizations, particularly across the US and in critical infrastructure, are relying on legacy tools and software that were conceptualized in the late nineties for security today. And the threats have advanced. The technology also needs to advance, so organizations need to invest in security to appropriately defend against these attacks.

From a government perspective, I think that both law enforcement has been making tremendous strides. CISA through JCDC and partnerships have been able to share information, and I think that the information sharing between the public and private sector is absolutely critical to ensure the success and the ability for us to defend these infrastructures.

Finally, I think the legislation that was passed recently in terms of the reporting requirements is a step in the right direction, and will enable us to more effectively marshal our forces to fight against these types of attacks.

JEFFERSON VAN DREW: Yet we still do need to do better, correct, when you mentioned that we have legacy infrastructure in place to deal with this, that tells me that you think we should be doing more and should be more on the cutting edge.

ADAM MEYERS: Absolutely, and I think that the executive order that was issued regarding employing things like endpoint defense and response technology, zero trust, one of the things that we've observed over the last year is that organizations that were impacted by these ransomware actors and criminal actors and also state-sponsored actors, those that employed zero trust and strong identity management had very different outcomes than those that did not.

JEFFERSON VAN DREW: OK. So that tells us that hopefully if we're here again in a year, another year that we hopefully can say, hey, we've done more, we're doing better in those areas that you just mentioned. Finally, do we have the smartest, best, most knowledgeable people on the government side working on this? Candidly.

ADAM MEYERS: I believe so. I think that particularly working with CISA over the past several months, it's been, and having spent years in government prior to CrowdStrike, I think that we are absolutely moving in the right direction, that the workforce has become much smarter and much more capable, and we're continuing to train and operationalize that.

RITCHIE TORRES: The gentleman's time has expired.

JEFFERSON VAN DREW: Thank you for your answers.

RITCHIE TORRES: I now recognize the gentleman from California, Mr. Correa for five minutes.

LOU CORREA: Thank you, Mr. Chairman. I want to welcome the witnesses today and thank you for being part of this very important hearing. We talk about incentives for these attacks, cyberattacks. We can talk about the financial people make money off of this, and I think all of us at one time or another have had our credit cards hacked.

In my district, I had a tax preparer who had been a victim of a cyber ransom attack. He did 5,000 clients he had. He lost 1,000 of them to a cyberattack. This stuff is getting more and more common. Yet I believe it pales to the potential damage of a terrorist attack on one of our systems. Our water system back home June of 2021, a large-scale cyber espionage campaign included the Metropolitan Water District of Southern California, Anaheim and Santa Ana in my district, but 19 million, 19 million water consumers were affected.

And you just hate to think about the potential for loss of life if somebody intentionally attacked us with more serious and deadly intentions. We talk today about minimum standards, mandatory standards, liability. I'd like to focus on trying to prevent this from happening, not trying to figure out who is to blame after the aftermath of an attack like this.

So my question would be, what else can we do to coordinate, instead of mandating, instead of talking about minimum standards, being up to scrub up to date on the latest technology? How can CISA work to make sure that we're actively talking to these agencies on a daily basis to make sure they're anticipating, it's a cross discussion back and forth?

Are we doing that? Can we do better? Mr. Morley.

KEVIN MORLEY: Excellent question, sir. And I would frame that in terms of the conversations today in terms of partnership. Obviously the critical infrastructure owner operator is a key piece of the equation. In addition, the information shared by our federal partners, as I mentioned earlier, the sooner we can get that into an operational setting, unclassified, that the utility owner operator can take action on that.

That is great. In addition, similar to the activities of these gentlemen and technology providers --

LOU CORREA: Can ask, you say the sooner the better.

KEVIN MORLEY: Of the partnership.

LOU CORREA: Mr. Morley, you said the sooner the better. It doesn't feel good right now. How fast can we get up and running and begin to establish a process where we can be there in terms of CISA?

KEVIN MORLEY: I think the agency, CISA in particular is working towards that end. Programs like JCDC are designed to try to support that activity, and I am hopeful that we can get there as expediently as you suggest we should.

LOU CORREA: Other comments from our witnesses here today? So any thoughts?

AMIT YORAN: No, sir, I think CISA is doing a tremendous job there. I think we've talked about JCDC and Shields Up as important initiatives, and even outside of those and in addition to those, the control system support program, I know the name is iterated a few times, they do have active engagement with a lot of the critical infrastructure operators, and we've seen increased pace of communication.

And I think also the quality of content of those communications has improved in recent years.

LOU CORREA: And gentlemen, I just want to be clear that this member here is not looking for a gotcha kind of a situation with my questions, because again, 19 million customers, that's a lot of lives at stake. So my goal, and I think the goals of members of this committee, are how we can help you help us to do a better job of protecting our constituents.

Mr. Chairman, I have 25 seconds. With that I yield.

RITCHIE TORRES: Thank you. I now recognize the gentlewoman from Iowa, Ms. Miller-Meeks for questions.

MARIANNETTE MILLER-MEEKS: Thank you, Mr. Chair. And Mr. Yoran, cyberattacks, hacking, ransomware is not new in the state of Iowa. We've had several municipalities who in fact were hacked and paid ransomware in order to get back their data, which prompted us at the state level to put through legislation that provides for disclosure and then communications with our public intelligence and investigations, investigative division in order to address that.

So it's extraordinarily important topic, and I think Mr. Yoran, if I'm not mistaken, you're a graduate of the US Military Academy at West Point. So as a fellow Army veteran, thank you for your service. In your testimony, you mentioned that knowing what the threat is, is far more important than knowing who is behind the threat.

It seems that there are some high maturity organizations that could adequately action the who information, but those are extremely limited. Could you provide some color into where that line lies?

AMIT YORAN: I'm sorry, Congresswoman. The line, could you just clarify again the line.

MARIANNETTE MILLER-MEEKS: Between the who and what.

AMIT YORAN: Well, I think for most operators, and I think know Dr. Morley and other panelists might be able to also articulate this, I think for most operators, it isn't critical to know the who is behind the attacks. I think knowing where they have the greatest exposures is absolutely critical so that they can address them, and getting high priority threat intelligence, whether it's from private-sector partners or from CISA and public-sector partners, helps to prioritize which vulnerabilities are being leveraged by the threat actor of the day.

Today that might be Russia. The purpose of this hearing is Russia, clearly while the activities happening in Ukraine and all eyes are on Russia, you could see other threat actors taking advantage of the situation. So I think knowing where you have exposures, and knowing which exposures to prioritize through threat intelligence is absolutely critical to success.

MARIANNETTE MILLER-MEEKS: Thank you. And this is for all of you. As you know, the committee raised concerns with the White House's decision to place the Department of Energy as the lead response agency to the Colonial Pipeline ransomware attack last year. In this case, GOE is not the lead sector risk management agency. Rather the Department of Homeland Security via the Transportation Security Administration is the co-lead for the pipeline sector.

As you can appreciate, and I've heard this from numerous entities, consistency in how the federal government responds to cyber incidents is of utmost importance. We have policies, procedures and statutes for a reason, and they should be followed. At a time like now, we simply can't afford similar missteps should something like this happen again.

Can you all speak to the importance from a private-sector perspective of the consistent and clear federal government response procedures?

KEVIN MORLEY: I'll take a run at that, Congresswoman. I think it is absolutely critical that the sector risk management agencies with leadership, in our case the EPA, are directly involved in that engagement with CISA as the risk management agency, given the understanding that in our case, EPA has in water utility operations and the critical elements that in some cases CISA may not have some of that direct understanding.

So I think that collaborative approach is most appropriate.

MARIANNETTE MILLER-MEEKS: Mr. Meyers.

ADAM MEYERS: Thank you. I think that each one of these incidents is going to have different merits, different threat actors, different impact, and so consistency is absolutely important. But I think that we should recognize that there are different agencies that might be more suitable or different organizations that might be suitable to assist in some of these incidents.

So I wouldn't want to limit our ability to respond by trying to have the same response each time, but knowing that we have to get the right partners involved and the right federal agencies involved to address whatever that incident might be.

MARIANNETTE MILLER-MEEKS: Mr. Yoran, do you have any comments or Mr. Meyers?

AMIT YORAN: I think Mr. Meyers has it right. You know, in different incidents you'll have different agencies involved, but it is absolutely critical that Homeland Security take the lead across all agencies when an incident happens, Log4J, Log4Shell whatever it is, the private sector is already connected to JCDC, it's already connected to CISA. They can work together there, they can engage there, and then you can pull in each sector-specific agency as appropriate as required versus every private-sector entity, CrowdStrike, Tenable, whoever trying to connect to all the different, you know, the 16 different departments and agencies is just extremely inefficient, would be extremely inefficient.

MARIANNETTE MILLER-MEEKS: [Inaudible]

RITCHIE TORRES: Well, the gentlewoman's time has expired. I now recognize the gentlewoman from New York, Ms. Clarke for questions.

YVETTE CLARKE: I thank you very much, Mr. Chairman, Ritchie Torres, and let me thank our ranking member, Mr. Katko. On a call with stakeholders two weeks ago, CISA Director Easterly urged owners and operators to report data on cyber incidents, as well as any anomalous activity that falls short of an incident so it can help detect any Russian cyber campaigns very early.

Fortunately, Congress passed legislation, which I authored requiring this type of reporting, but it will take some time for these requirements to go into effect. Mr. Silberstein, financial institutions are a rich target for Russian hackers on a normal day, to say nothing of the unique role they play in for instance, the context of sanctions.

Is the FS-ISAC doing anything to encourage financial institutions to voluntarily report this information to CISA?

STEVEN SILBERSTEIN: Yes, thank you, Congresswoman. So the financial sector benefits from a long history of being under attack, as well as a lot of regulation that has required reporting. So there's a pretty good cadence of reporting recognition among the US-regulated financial community, and both the regulatory requirement and also as a civic duty to help out.

We facilitate in certain situations to report on behalf of members. We encourage them also to engage directly with law enforcement, CISA, etc. where it's appropriate. So we are fully supportive of that model.

YVETTE CLARKE: Very well. And Dr. Morley is AWWA doing anything to encourage or facilitate this type of reporting? Do you think that the water sector has the resources it needs to know what and how to report?

KEVIN MORLEY: Yes, Congresswoman. We've very consistently encouraged members to report incidents, whether it's physical or cyberattacks with the Water-ISAC and CISA, and recently just issued and redistributed an advisory from FBI TARP that was focused on municipal communities of which we're typically part of, on how to report that information to the FBI.

YVETTE CLARKE: Very well. Mr. Meyers and Mr. Yoran, are you encouraging companies you work with to voluntarily report to CISA? And have you seen any uptick in willingness to do so given the gravity of the current threat landscape?

ADAM MEYERS: I'll take that first. Thank you, Congresswoman. I think a lot of these investigations are conducted under the direction of counsel, and so counsel working with those victims, those customers, generally is the one that's going to provide the guidance about what they should reach out and share. But we work closely with law enforcement and CISA to ensure that they're aware of threats, and that we're able to kind of work together to ensure a coordinated response.

YVETTE CLARKE: Mr. Yoran.

AMIT YORAN: Led by counsel sounds suspiciously like not going to report to my untrained ears, but I do think that's why it's important to have the legislation that exists, mandating reporting of incidents and ransomware payments to CISA. As a company, Tenable, we encourage but we don't have an active role in the incident response process.

From our perspective, we're more frequently taking the information that is produced at JCDC and access about these high priority vulnerabilities, and making sure that we're able to automate the distribution of that information to tens of thousands of organizations around the world so that they can take action and identify where they have those specific high priority vulnerabilities.

YVETTE CLARKE: Very well. Are you planning to engage with CISA during the rulemaking process, and if so, what are some of the key takeaways you hope they internalize through that process? Mr. Meyers, Mr. Yoran, anyone want to tackle that? You got seven seconds.

AMIT YORAN: I think both of our companies have teams that are working closely with CISA in providing feedback during the response time.

YVETTE CLARKE: Very well. Mr. Chairman, I yield back and I thank you, our distinguished panelists for your testimony today.

RITCHIE TORRES: I now recognize the gentleman from Florida, Mr. Gimenez for questions.

CARLOS GIMENEZ: Thank you, Mr. Chairman and Ranking Member. I've got a couple of questions. Ransomware and there are in Russia, we know that there's a bunch of different ransomware operators. Does anybody know if some of the proceeds from this ransomware ever make it back to the Russian government?

ADAM MEYERS: I'll take that. I think that we've seen clear indications of Russian criminal threat actors operating at a scale that would likely attract the attention of the Russian government, and reasonably to assume that they would be paying some degree of taxes or something to that effect from some of these proceeds.

The coordination of these criminal actors and the Russian government has been difficult to directly correlate, but we've seen nationalistic and patriotic postings from some of them in underground forums, and that's kind of led to the conclusion that there is some coordination. If the Russians wanted them shut down, they could shut them down, right?

Yes.

CARLOS GIMENEZ: Pretty easy to identify where they are, etc. how they're operating?

ADAM MEYERS: Yes.

CARLOS GIMENEZ: OK. Fair enough, so basically, they're just an arm of the Russian government. Thank you. The Biden administration said that we should be expecting more, there's a potential for increased cybersecurity threats from Russia on the United States. Has anybody seen any evidence of increased activity threats from the Russians on the United States?

ADAM MEYERS: Yes, we've been aware, and I believe CISA actually put out some reporting on this last week of Russian threat actors conducting widespread scanning, attempting to look for vulnerabilities or access into datacenter infrastructure.

CARLOS GIMENEZ: Yeah, but that happens all the time. I mean are we talking about increased activity, because the probing, the Russians probing and state actors probing our infrastructure happens all the time, all the time, every single day. So is there increased activity like this?

ADAM MEYERS: Yes, and in this case, it was a very specific set of activity that was being alerted to.

CARLOS GIMENEZ: Alright, I'm going to pivot to something else now. Our critical infrastructure, to me it would seem like there's two types of systems. There's an open system that is open to the Internet, people can hack into etc. etc. and there probably are systems that are closed, right, that the operating system, they communicate within itself, there's no way to get into it because it's not attached to anything on the outside.

Am I mistaken that there's these two kinds systems?

ADAM MEYERS: I think that what you're referring to is a perception that there is OT operational technology and IT information technology, and that in a perfect world, the OT systems are isolated from the Internet the IT-facing systems. The reality is that that's not always the case. As Mr. Yoran pointed out, they establish cellular communications for remote telemetry collection.

There's interconnections for business systems to collect data from the operational side, for example, in a pipeline metering and billing information might be important business functions that necessitate a connection between the two. So while in theory they should be or could be isolated, the reality is there are connections between them.

CARLOS GIMENEZ: Would it make sense Mr. Yoran for us maybe to regulate that certain highly critical infrastructure actually work in that manner where it is physically separated from the open infrastructure?

AMIT YORAN: Congressman, I think it's dangerous to mandate or regulate that they remain physically separate. I think as Adam points out, there's business reason, efficiency reason that you might want to interconnect those and not just, I mean, certainly for billing purposes, but also for being able to predict when parts are going to fail, when outages are going to occur.

And so there are reasons to interconnect. I do think that it makes sense to regulate, mandate, remind those operators that they're responsible for the cybersecurity risk when they're interconnecting those systems.

CARLOS GIMENEZ: But you can still have those systems inside a closed system. You could actually just have all that predictability etc. inside a closed system where it's not connected to the outside, Isn't that true?

AMIT YORAN: You could do it. I think the practicality is that people will want to connect.

CARLOS GIMENEZ: Well I'm not talking about every system, I'm talking about critical infrastructure like water, electricity, etc. that the United States would be hard pressed to survive if somehow our water systems were all hacked and we went down, our entire grid is hacked and we went down. Don't you think that's maybe worth the inconvenience of the business side of it that, hey, maybe these things should be a little bit separated and not - Because look, the way I look at it, and I'm sorry, I'm out of time, the way I look at it, there's software protection and there's physical protection.

Software protection, as good as you guys think you may be, you'll always get, somebody is going to get around you and figure a way around you. So thank you. I yield my time back.

RITCHIE TORRES: I now recognize the gentleman from New Jersey, Mr. Malinowski for questions.

TOM MALINOWSKI: Thank you, Mr. Chairman. I want to thank our witnesses for appearing today to speak on this topic. Obviously, I think we all wish that we were here under very different circumstances, that the people of Ukraine were not as we speak suffering attacks by bombs and artillery shells in the most horrific possible way, and that the American people were not as a result of this war facing an even greater risk of cyberattacks that would disrupt our lives and our economy.

We've seen firsthand how cyberattacks have become an instrument of war. On the day that Russia illegally invaded Ukraine, they knocked out among other things through a cyberattack, satellite communication systems that were used by the Ukrainian military government, tens of thousands of ordinary citizens.

Many of us have been briefed on potential scenarios under which similar systems in the United States might be attacked as part of a war somewhere halfway around the world. But the risk obviously is not just in times of war. My office, for example, recently met with the cybersecurity team for a health care provider in my district.

Every single day this hospital, tens of thousands of cyberattack attempts mostly coming from China, Russia and Iran, attacks that started long before the war in Ukraine, and that will last long after the war is over. So we have to do more, everything we can to better protect our hospitals, our schools, our water facilities, our power plants and other critical infrastructure, recognizing that they have to play defense and be successful 100 percent of the time, whereas our adversaries on offense only have to be successful once to hurt our lives and our livelihoods.

On that point, I am very particularly concerned about securing water utilities in my state of New Jersey. In my district, one water company helps service, one relatively small water company helps to service more than 30 municipalities across five counties, towns in my district like Millburn and Westfield, Raritan, Roxbury.

Many such water companies don't have the resources of a large hospital network or investment bank. And so for any and all the witnesses, I'd like to ask how can Congress help these critical infrastructure operators modernize their IT and reduce the cost and complexity of defending their networks? How do we address the cyber poverty line, and make sure investments in intelligence sharing and intelligence sharing are actually useful to Main Street firms, not just those on Wall Street?

Thanks so much.

KEVIN MORLEY: Yes, Congressman, I'll start off given your comment about the water sector. I think it's absolutely critical and certainly have some excellent resources made available to the water sector through the recent infrastructure legislation. Some of that is authorized and yet to be appropriated, but we appreciate the inclusion of cybersecurity as an eligible activity under those programs.

That being said, as I noted earlier, a number of the resources available from CISA are quite exceptional in supporting utilities and identifying those vulnerabilities, and helping them to take actions such as the Cy-Hy program. And we would encourage continued support for that capacity development of community water systems and wastewater systems as they work with our federal partners to implement some of these great strategies, recognizing that water utilities are 24/7 operation both in drinking water and wastewater side and some of the utilities I've spoken with here in the last several months and years, those rehabilitating or upgrading those OT systems can often be a three- or four-year capital improvement project to ensure that the system maintains operations during that whole period.

So it's not a rapid process, but support from our federal partners is encouraging.

TOM MALINOWSKI: Just a few seconds left, and let me just note, I mean, I started with the example of the Russians knocking out a satellite communication system. We don't have time to ask you all about this, but just to let you know that I'm going to be introducing a legislation shortly that would allow commercial satellite operators to better protect themselves against cyberattacks.

And I would note that a number of utilities, including water utilities in the United States rely, as we all do, on satellite, commercial satellite technologies to facilitate their operations, so I see that as something that will help the entire sector. Thank you, and I yield back.

RITCHIE TORRES: I now recognize the gentleman from Texas, Mr. Pfluger for questions.

AUGUST PFLUGER: Thank you, Mr. Chairman, and to all the witnesses, thank you for taking part in this today. Obviously, very important. The threats I believe are going up exponentially, and new threats that we haven't seen before, I also believe will be attacking our critical infrastructure. I've got a couple of questions.

Before I get to that, last week I introduced the Cyber Deterrence and Response Act to really remove any ambiguity for a would-be attacker of American critical infrastructure, whether it's the financial sector or the energy sector, I've always been very outspoken on energy and believe that that is a vulnerability, a target and something that adversaries will target.

And it basically says that any cyberattack on critical infrastructure by a foreign state-sponsored actor will be responded to by the President of the United States. And I'll just start Mr. Yoran, West Point grad, myself being an Air Force Academy grad, I think that we might be able to look at these actions a little bit differently.

Can you kind of talk through the benefits or even drawbacks of establishing maybe more serious red lines that might remove some of the ambiguity, but also could limit some more, kind of put us in a box if you will, in some cases, what's the value of the deterrence by being a little more overtly stating what we will and how we respond to some of these attacks.

AMIT YORAN: Well, thank you, Congressman. I do think that deterrence should play a critical role in the cybersecurity paradigm, and to date it is greatly underserved. So the deterrence could be response in-kind from a cyber perspective, it could be retorts, it could be countermeasures and it could be non-cyber responses.

And I think having those options available to us as a nation and exerting those options more frequently is one way to signal to the rest of the international community what is OK and what is not OK from a cyber perspective.

AUGUST PFLUGER: Well, thank you for that. It's obviously a difficult problem. We need to have the reporting in order to understand, but hopefully that reporting comes in the way of voluntary so that we can really learn the lessons. Let me move to the next question for Mr. Meyers. Talking about the State Department launching the new Bureau of Cyberspace and Digital Policy, and given your support previously for the Threat Analysis Division, can you talk us through how this new agency should standup, how they will be effective and the steps they need to take to accomplish that deterrence that we just talked about with Mr. Yoran.

ADAM MEYERS: Sure, I think information sharing and bringing visibility and awareness to what threat actors are doing and what that looks like is absolutely critical. If I can turn back briefly to the deterrence component, though, I think that there's an element which is deterrence through denial that should be considered.

And that is really about as to borrow from CISA, the Shields Up, but bringing the technology together that allows us to ensure that these threat actors are not able to conduct these operations. And as Mr. Yoran mentioned in his testimony about LAPSUS$ using pretty limited resources to conduct large-scale attacks against pretty significant entities.

I think zero trust, identity management, multifactor authentication, all of these technologies help us make organizations more resilient and stronger, and in doing so, enable us to create deterrence through denial, by denying the threat actor the ability to operate inside of our environments and raising the cost of doing business to them.

AUGUST PFLUGER: Well, thank you for that. Last question for anybody on the panel. In the form of personnel that are able to conduct these types of cyber-related activities here, I believe we have a shortage of people and experts. How do we at the university level or even before Primary education, Secondary education, how do we target this problem through the training of and the education of personnel?

I'm thinking of my own district Angelo State University, a cyber center of excellence. How do we really move the needle and make a dent in this problem? For anybody.

ADAM MEYERS: I'll take that first, but I think we need to be going at the junior high school level, and really encouraging STEM programs, encouraging students from lots of different diverse backgrounds to get involved in math and science, and build the workforce for the future today. We cannot just magically make this workforce appear, we need to start at a young level and start to train them.

CrowdStrike has been encouraging that through some of our nonprofit operations with Girls Who Code and things like that, so strongly encourage doing that at an early age.

AUGUST PFLUGER: Thank you. I'm out of time. I'm going to have a question to follow up to ask each of you whether we're behind on that or not. I appreciate it and yield back.

RITCHIE TORRES: Thank you. I now recognize the gentleman from Kansas for questioning, Mr. LaTurner.

JACOB LATURNER: Thank you, Mr. Chair. I want to thank each of the witnesses for taking part in this hearing today and sharing your perspective on this important [Inaudible] that I don't hear about the threats and challenges that businesses, schools, hospitals and countless other stakeholders in my district face due to increased cyberattacks.

As we all know, this threat has only increased in recent months. We have watched the unfolding tragedy of the Russian invasion of Ukraine, but Russia's aggression is not limited to their heinous attacks and bombings of civilian shelters that we see on television. War is also being waged in the cyber space, where Russian actors are doing all they can to undermine and attack not just Ukraine, but the United States and our other allies abroad.

And these attacks did not just start in the last month. It has recently been reported that the Department of Justice indicted three Russian FSB agents who targeted computer systems at the Wolf Creek nuclear power plant in Burlington, Kansas from 2014 to 2017. The government maintains a consistent expectation that utilities and critical infrastructure stakeholders should operate as partners for the defense of the nation.

However, in order for them to perform that role as expected by the government, industry needs timely and actionable information that they can take and respond effectively. This is a two-way street, and we need to ensure that industry and government are able to develop a trusting relationship where they're capable of freely sharing information with the knowledge that it will remain secure, and is actioned to strengthen and improve our cyber defenses.

I will emphasize the need for it to remain secure. My first question is for Mr. Morley. Mr. Morley, given the widespread disparity of your membership and the wide array of needs that they have, do you feel that the assistance you all are getting from CISA adequately covers the wide range of needs that your members have?

KEVIN MORLEY: I think to your point about timely and actual information, I think we can improve that and ensure that the information is actionable. I think some of that information does come out at a level that may be beyond some of the technical expertise that may be in-house at a small or medium system, and would look forward to the opportunity to work with the agency to improve that information sharing process.

JACOB LATURNER: I appreciate that. Mr. Silberstein, you represent some of the most cyber-mature companies in the country. I would imagine that some of the services CISA offers may not be as useful to your member companies as they are to other sectors. Where does CISA need to improve in their services for you all?

STEVEN SILBERSTEIN: Thank you, Congressman. The largest financial institutions like many of the largest corporations in the country are extremely sophisticated in their capabilities. But nevertheless, the information that CISA provides is useful because they have an across-the-country view and it is valuable. Does it have the

same value?

Probably not. I think we're all challenged as we go down the size rankings in any sector of the smaller institutions, how they find the resources, the money, etc. to do what's needed, and moving to, for the future, to where we start building more context to the individual sectors around the information about their supply chains is a long-term direction which could be helpful.

JACOB LATURNER: I appreciate that. This is for everyone, I want to give everyone opportunity here. The Cyber Incident Reporting for Critical Infrastructure Act included within the Consolidated Appropriations Act, it requires owners and operators to report significant cyber incidents and ransomware attacks to CISA, which will lead to greater visibility for the federal government earlier disruption of malicious cyber campaigns and better information and threat intelligence going back out to the private sector so they can defend against future attacks.

Several of you mentioned in your testimony that you had recommendations for legislation, and I would like to provide an opportunity for you all to comment on that now.

AMIT YORAN: Are you asking about the incident reporting legislation or --

JACOB LATURNER: Correct.

STEVEN SILBERSTEIN: If I may Congressman, we don't take a stance on suggesting legislation in the future. But we'll note that there seems to be some excellent coordination between CISA, US Treasury and regulators about attempting to normalize the already existing reporting requirements with the new reporting requirements.

JACOB LATURNER: And my time has expired. Mr. Chairman, I yield back.

RITCHIE TORRES: I thank you, and I'll simply end with a final comment that the state of cybersecurity of our critical infrastructure runs the gamut from financial services, which is richly resourced to our water systems, which is fragmented and poorly funded. And we have to ensure that CISA's support is sufficiently tailored to the widely varied needs of our critical infrastructure, that it's sufficiently based.

I want to thank the witnesses for their testimony and the members for their - Another member showed up? Ms. Cammack, I'm sorry. You're recognized.

KAT CAMMACK: Well, I appreciate it. Thank you so much, and thank you to our chairman and Ranking Member Katko for holding this very important hearing today. And again, thank you to all our witnesses for your testimony. I know that these can be lengthy, but we appreciate and value your testimony. Several weeks ago, I held a call with utilities, businesses, city and county leadership and stakeholders across my district, Florida Third Congressional, to discuss cyber preparedness and resiliency.

Now during this call, we were able to discuss the resources at CISA, specifically Shields Up, and I'm glad that CISA has developed this initiative for individuals and organizations across the country to provide this critical information on cyber threats, mitigation and best practices that must be implemented in the face of growing cyber threats.

However, every organization in the United States, every level of government, private business, ag operation, water treatment facility, you name it, it is exposed to cyber threats. And as we have seen in the last year, cyberattacks can have a real and immediate effect on Americans across the country. The Colonial Pipeline ransomware attack affected the entire East Coast, even Floridians, who are not reliant on getting their fuel from a pipeline, leading to the company halting national normal functions for several days, which led to fuel shortages throughout the Southeast, leading to, at the time, the highest gas prices since 2014. In February of last year, a water treatment facility in Florida not far from my district was also attacked.

According to reports about the attack, the levels of sodium hydroxide at the treatment facility were adjusted from 100 parts per million to 11,000 parts per million, a deadly level. Fortunately, this attack was noticed and stopped by employees who were vigilant. Moreover, as a member of the House Agriculture Committee, I am especially worried about cyber threats against another critical infrastructure sector, our nation's food supply.

In June of last year, a cyberattack that was likely based in Russia targeted JBS, who has operations in Canada, Australia and the United States. Now as you all know, JBS makes up nearly 19 percent of the nation's market share for meat processing. According to a recent report from the Food and Agriculture Organization, the war in Ukraine global agriculture markets face, because of the war, they face exposure to vulnerability to shocks and volatility, from fertilizer prices, fuel prices, factoring regulatory and labor concerns.

In short, it's a mess. Due to the potential disruptions in ag production and trade in the region, US producers and related agribusiness must remain resilient in the face of enhanced cyber threats from Russia targeting these industries. Food security is national security, and it is vital at this time to ensure that there are no disruptions to our nation's food supply or other critical infrastructure sectors.

Mr. Meyers, I'd like to just touch on your opening statement. You discussed a number of threat actors and the various goals of leveraging cyber operations. Can you discuss the process by which you were able to determine the intended objectives for cyber threat actors? And specifically, I am curious how you can make the determination for the reason for these operations when it is not explicitly conveyed or there is not a financial aspect to the crime?

ADAM MEYERS: Thank you for the excellent question, Congresswoman. The intent of the threat actor can be established by the targets that they go after, the method by which they conduct targeting, by which I mean if they're conducting phishing attacks with malicious attachments, looking at the recipients of those attachments, looking at the content of the war that is intended to get the person to click on it or open it, are all things that help us understand what the target environment looks like or who the targets might be. In terms of intent, we look at the tools that they're leveraging.

This may involve tools that are built specifically for espionage, looking for specific files, keywords, things that will be used by a threat actor for intelligence purposes. In the case, the examples I mentioned with regards to Ukraine and Russia, they have employed disruptive destructive tools that are meant to overwrite files and to render systems inoperable.

That is kind of the two main differentiations between espionage and these disruptive destructive attacks. The threat actors that we are tracking are capable, particularly from a Russia perspective, in conducting disruptive destructive attacks against targets in the United States, and as I highlighted, critical infrastructure.

KAT CAMMACK: My apologies for the bell, but thank you for your commentary, and my time has expired. I yield back.

RITCHIE TORRES: Thank you. Last but not least, the gentleman from Georgia, Mr. Clyde is recognized for questions.

ANDREW CLYDE: Thank you, Chairman Torres for holding this important hearing. As many of you are aware, far too often in our digital age, we do hear of companies, schools, health services or local municipal governments victimized by ransomware attacks. However, what is equally as concerning are those entities harmed by cyber crime that we do not hear about due to those entities not filing a report with CISA, the FBI or the NSA, often because they do not know what law enforcement tools are available to them.

In my home district alone, Jackson County government was hit with a ransomware attack demanding $400,000 in 2019. Hall County elections infrastructure was hit by a ransomware attack in 2020. A major manufacturer, ASI Southeast was hit in 2021. In the south of my district, one of the most important gas pipelines in the Southeast, Colonial Pipeline was hit with a ransomware attack in 2021, causing serious fuel supply disruptions.

Mr. Chairman, I request unanimous consent to have these articles reflecting these events submitted for the record, and I'd like to read them.

RITCHIE TORRES: Without objection.

ANDREW CLYDE: Thank you. The first article is ZDNet, "Georgia County pays a whopping $400,000 to get rid of a ransomware infection," from May 9, 2019, October 29, 2020 "Ransomware Hits Election Infrastructure in Georgia County" from CNN, and then from US News and World Report on May 8, 2021, "Major US Pipeline Halts Operations After Ransomware Attack." Thank you.

As Russia wages war in Ukraine and more countries place economic sanctions on Russia, we have been warned about the potential increased cyberattacks against US businesses by Russia or Russian assets. These attacks could not only hurt the United States on a financial front, but they could also interrupt critically important defense utilities, health care, manufacturing or elections computer network systems.

It's vital to our national interests that we secure our networks to prevent ransomware and cyberattacks by bad actors. Moreover, in shoring up our nation's defensive cyber capabilities, we must also make sure that we maintain cutting-edge offensive cyber capabilities. I've always believed that the best defense is a good offense.

Without a strong offense, our nation will lack the ability to deter and respond to attacks conducted against US interests. So my question especially for Mr. Meyers first and then for Mr. Yoran, is this an area of focus, is the offensive capability an area of focus that any of you can discuss in this setting?

Are you involved in that?

ADAM MEYERS: I think that's best answered by the intelligence community and the military law enforcement. Private sector does not play a significant role from an offensive perspective.

ANDREW CLYDE: Would you agree? Are you --

AMIT YORAN: I would agree with Mr. Meyers. There's no role for private sector in offensive cyber operations.

ANDREW CLYDE: OK. Alright, thank you. I'm a member of the House Committee on Oversight and Reform, and in January of this year, CORE held a hearing on the 13th iteration of the Federal Information Technology Acquisition Reform Act or FITARA, and this hearing highlighted the grades each federal agency received in different areas of the FITARA scorecard.

While many federal agencies passed in many areas, a large area of concern was cybersecurity under the Federal Information Security Management Act or FISMA. While most FISMA scores were a C or higher, however, there were six D grades, and that made me question, what does this mean for cybersecurity for the agencies that scored so low?

And I want to highlight the Department of Energy was one of those agencies that scored a D in the FISMA category. The White House placed the Department of Energy as the lead response agency to the Colonial Pipeline ransomware attack. However, the DOE was not the lead sector risk management agency, rather the Department of Homeland Security via the Transportation Security Administration.

So can any of you tell me, I think let's see Mr. Meyers, you were involved in that CrowdStrike, was that not something that you were involved in with Colonial Pipeline?

ADAM MEYERS: In what regard?

ANDREW CLYDE: As in assisting Colonial Pipeline.

ADAM MEYERS: Not to my knowledge. We covered it from an intelligence perspective and investigated the DarkSide Group that was responsible for it.

ANDREW CLYDE: Right, that's kind of where I'm going. So you were involved in investigating the DarkSide of it.

ADAM MEYERS: Yes.

ANDREW CLYDE: OK. So can you tell me, did Russia have a part in that do you think, or can you elaborate on that with regard to Russia?

ADAM MEYERS: I think that in that case, there was a core group which was responsible for building the platform. This is something that we term ransomware as a service. They built that core platform and then there was an affiliate who was responsible for conducting the actual intrusion and deployment of ransomware. So it was a criminal group that's known, that we track as Carbon Spider, and then an unknown affiliate who leveraged that infrastructure to conduct the attack.

ANDREW CLYDE: OK. Alright. Thank you very much. With that I yield back.

RITCHIE TORRES: Thank you, Mr. Clyde. Without objection, I insert into the record a statement from Security Scorecard. I thank the witnesses for their testimony, for their service to the country, and the members for their questions. The members of the committee may have additional questions for the witnesses, and we ask that you respond expeditiously in writing to those questions.

The chair reminds members that the committee record will remain open for ten business days. Without objection, the committee stands adjourned.