

HOPE GOINS, Staff Director
DANIEL Manuel, Minority Staff Director
NATALIE Manuel, Clerk



CONTENTS

Page MENTS , a Representative in and Chairwoman, The Honorable , and Oral ment , and Oral ment Prepared ment , a Representative in From From , and Chairwoman, The Honorable and ment Prepared ment

The Honorable and Ranking Member,

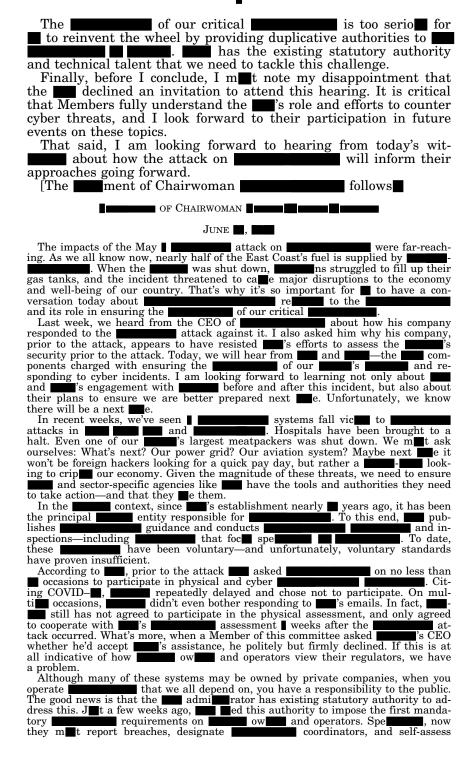
From the : Oral | ment ment , a Representative in From Prepared mer The Honorable , and Chairman, ment Prepared ment WIT Ms. , Assistant Admi Oral ment Prepared ment , Executive Assistant Director for Mr. and ment Prepared ment APPENDIX Question From Honorable Question From Honorable for



CYBER THREATS IN THE : LESSONS FROM THE RE TO ATTACK

Tuesday, June , , , AND , AND THE AND The I met, pursuant to notice, at **!: p.m.**, via Webex, Hon. [Chairwoman of] presiding. Present: Representatives (ex officio), and Mrs. and will come to order for today's , and hearing titled "Cyber Threats in the Re to Threats in the Threats in the Re to Threats in the Th : Lessons from the Attack." Without objection, the Chair is authorized to declare the in recess at any point. Thank you to Chairwoman , Ranking Member , and our panel of wit for joining Ranking Member The impacts of the May | attack on were far-reaching. As we all know now, nearly half of the East . When the Coast's fuel is supplied by ■ was shut down, as struggled to fill up their gas tanks, and the incident threatened to came major disruptions to the economy and well-being of our country. That is why it is so important for to have a conversation today about to the and its role in ensuring the of our critical Last week, we heard from the CEO of how his company responded to the attack against it. I also asked him why his company, prior to the attack, appears to have resisted 's efforts to assess its the attack.

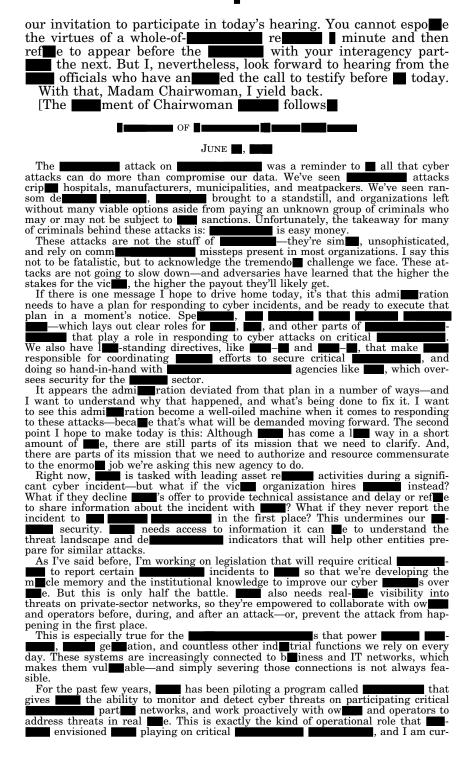
Today, we will hear from and and, the components that are charged with ensuring the of our sister and responding to cyber incidents. I am looking forward to learning, not only about and and sister and after this incident, but also about their plans to ensure we are better prepared next see. Unfortunately, we know that there will be a part
In recent weeks, we have seen systems fall victo attacks in and in and in and in stacks in a largest meat-packers was shut down. We must ask ourselves what is next. Our power grid? Our aviation system? Maybe the next to it won't be foreign hackers looking for a quick payday but, rather, a looking to criptour economy. Given the magnitude of these threats, we need to ensure and sector-specific agencies like have the tools and the authorities that they need to take action and that they them.
In the grant context, since grant's establishment nearly years ago, it has been the principal entity responsible for this end, publishes guidance and conducts and inspections, including that foc specific and unfortunately, voluntary standards have proven insufficient. According to prior to the attack, had asked on no less than cocasions to participate in physical and cyber compared to prior to participate. On multiple occasions occasions to participate.
sions didn't even bother responding to semails. In fact, still has not agreed to participate in a physical assessment, and only agreed to cooperate with sassessment weeks after the statack occurred. What's more, when a Member of this committee asked statack occurred. What's more, when a Member of this committee asked statack occurred. What's more, when a Member of this committee asked statack occurred. What's more, when a Member of this committee asked statack occurred. What's more, when a Member of this committee asked statack occurred. What's more, when a Member of this committee asked statack occurred. What's more, when a Member of this committee asked statack occurred. What's more, when a Member of this committee asked statack occurred. What's more, when a Member of this committee asked statack occurred. What's more, when a Member of this committee asked statack occurred. What's more, when a Member of this committee asked statack occurred. What's more, when a Member of this committee asked statack occurred. What's more, when a Member of this committee asked statack occurred. What's more, when a Member of this committee asked statack occurred. What's more, when a Member of this committee asked statack occurred. What's more, when a Member of this committee asked statack occurred. What's more, when a Member of this committee asked statack occurred. What's more, when a Member of this committee asked statack occurred. What's more, when a Member of this committee asked statack occurred. What's more, when a Member of this committee asked statack occurred. What's more, when a Member of this committee asked statack occurred.
The good news is that the damin rator has existing authority—statutory authority—to address this. Jet a few weeks ago, determined the damin of the damin rator has existing authority—statutory authority—to address this. Jet a few weeks ago, determined the damin of the damin rator has existing authority—to address this. Jet a few weeks ago, determined to impose the first mandatory requirements on determined and operators. Specification of the damin rator has existing authority—to address this. Jet a few weeks ago, determined to impose the first mandatory determined and determined to be done. We met the damin rator has existing authority—to address this. Jet a few weeks ago, determined to impose the first mandatory determined to operators. Specification of the damin rator has existing authority—to address this. Jet a few weeks ago, determined the damin rator has existing authority—to address this. Jet a few weeks ago, determined the damin rator has existing authority—to address this. Jet a few weeks ago, determined the damin rator has existing authority—to address this. Jet a few weeks ago, determined the damin rator has existing authority—to address this. Jet a few weeks ago, determined the damin rator has existing authority—to address this. Jet a few weeks ago, determined the damin rator has existing authority—to address this. Jet a few weeks ago, determined the damin rator has existence and de
to act boldly and swiftly to ensure operators of and all other forms of harden their systems. Meanwhile, it is similarly important that other agencies in respect and and sexperience and expertise on these matters.

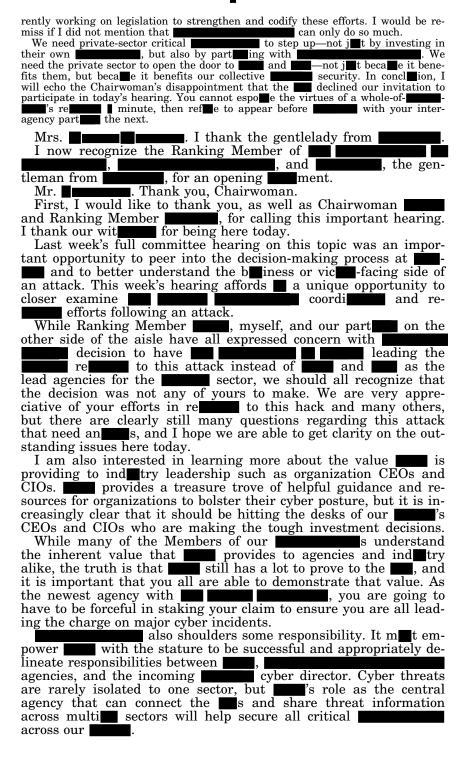


their compliance with security guidance. This is an important first step, but there is clearly more that needs to be done. We ment resource and empower and to act boldly and swiftly to ensure operators of and all other forms of harden their systems. Meanwhile, it is similarly important that other agencies matters. The respect and sexperience and expertise on these matters. The of our critical is too serios for to reinvent the wheel by providing duplicative authorities to statutory authority and technical talent we need to tackle this challenge. Finally, before I conclude, I ment note my disappointment that the declined an invitation to attend this hearing. It is critical that Members fully understand the series and efforts in countering cyber threats, and I look forward to their participation in future events on these topics.
Mrs. Member of Member Membe
I look forward to hearing today from Mr. and Ms. of and Ms. of on how and work together to ensure are secure from cyber threats. I thank the wit for their today. I am interested to hear from on the industry's compliance with the detailing what plans has for additional directives in the near future. I am concerned with the approach to move oversight from and into oversight from the first oversight from
I believe or is the appropriate agency to oversee is a strong effort in securing all modes against cyber threats. As a committee, we need to continue to strengthen our is safe and responsibilities needed to keep all of our cyber safe and secure. I look forward to the disconsional is resources and expertise, but is the appropriate agency to oversee is the appropriate agency to oversee is a strong effort in securing all modes against cyber threats. As a committee, we need to continue to strengthen our safe and secure is safe and secure. I look forward to the disconsion today of finding ways to improve
security of our against continued threats of cyber attacks and, frankly, all of our security threats and how we can protect from cyber threats in the future. Madam Chairwoman, I also share your distance that the did not participate today. Thank you, Madam Chairwoman. I yield back the balance of my e. [The mean ment of Ranking Member follows.]
OF RANKING MEMBER
Thank you, Chairwoman seed that the CIPI and seed the circumstant and seed that the CIPI and seed the circumstant and

this today on cyber threats to	
I look forward to hearing today from Mr. of and Ms. on how and and work together to ensure are secure from cyber threats. I thank the wit for their set today.	
I am interested to hear from on the ind try's compliance with the that issued last month. I look forward to Ms. detailing what plans has for additional directives in the near future.	
I am concerned with the pth to move and into an and into a second and interest and expertise, but I believe a or	
are the appropriate agency to oversee Solve collaboration with serves to ensure that there is a str effort in securing all modes against cyber threats. As a committee we need to continue to strengthen our by strengthening and giving them all the tools and responsibilities needed to keep all of our cyber safe and secure.	
I look forward to the discal sion today and finding ways to improve the security of our against the continued threat of cyber attacks and frankly, all of our security threats and how we can protect from cyber attacks in the future. Madam Chairwoman, I also share your discal asure that the did not participate today. Thank you, Madam Chairwoman, and I yield back the balance of my security threats and how we can protect security from cyber attacks in the future. Madam Chairwoman, I also share your discal asure that the security of the continued threats and I yield back the balance of my security from the continued threats of the continued threats and frankly, all of our security of the continued threats of cyber attacks and frankly, all of our security of the continued threats of cyber attacks and frankly, all of our security of the continued threats of cyber attacks and frankly, all of our security of our security of the continued threat of cyber attacks and frankly, all of our security of our security of cyber attacks and frankly, all of our security of our security of our security of cyber attacks and frankly, all of our security of our security of cyber attacks and frankly, all of our security of cyber attacks and frankly, all of our security of cyber attacks and frankly, all of our security of cyber attacks and frankly, all of our security of cyber attacks and frankly, all of our security of cyber attacks and frankly, all of our security of cyber attacks and frankly, all of our security of cyber attacks and frankly, all of our security of cyber attacks and frankly, all of our security of cyber attacks and frankly, all of our security of cyber attacks and frankly, all of our security of cyber attacks and frankly, all our security of	
Mrs. Thank you, Ranking Member. The Chair now recognizes the Chairwoman of the chairwoman, and the chairwoman, the	
gentlelady from for an opening ment. Ms. It hank you, Madam Chairwoman, To Ranking Members and for an opening, I thank you for working with me on today's hearing, and to our wit	
for joining today. The attack on attack on was a reminder to all that cyber attacks can do more than compromise our data. We have seen attacks crip hospitals, manufactur-	
ers, municipalities, and meat packers. We have seen ransom de- brought to a standstill, and organiza- tions left without many viable options aside from paying an un-	
known group of criminals who may or may not be subject to sanctions. Unfortunately, the takeaway for many of our criminals behind	
Unfortunately, the takeaway for many of our criminals behind these attacks is is easy money. These attacks are not the stuff of the stu	
If there is one message I hope to drive home today it is that this admit ration needs to have a plan for responding to cyber incidents and be ready to execute that plan at a moment's notice, spetral which lays out clear roles for , and other parts of that play a role in responding to cyber attacks on critical	
We also have less-standing directives, like standard and stand, that makes responsible for coordinating efforts to secure critical and doing so hand-in-hand with Sector	

Risk Management agencies like , which oversees security for sector. It appears the admit ration deviated from that plan in a number of ways, and I want to understand why that happened and what is being done to fix it. I want to see this admimiration become a well-oiled machine when it comes to responding to these attacks becalle that is what will be demanded moving forward. The second point I hope to make today is this: Although has come a less way in a short amount of the, there is still parts of its mission that we need to clarify, and there are parts of its mission that we need to authorize and resource commensurate to the enormo job we are asking this new agency to do. Right now, is tasked with leading asset re during a significant cyber incident, but what if the vice organizainstead? What if they decline 's offer to provide technical assistance and delay or refer to share information about the incident with ? What if they never report the incident to in the first place? needs access to in-This undermines our security. formation it can e to understand the threat landscape and deindicators that will help other entities prepare for similar attacks. As I have said before, I am working on legislation that will require critical to report certain dents to so that we are developing the marcle memory and the institutional knowledge to improve our cyber sover e. But this is only half of the battle. also needs realvisibility into threats on private-sector networks, so they are empowered to collaborate with ow and operators before, during, and after an attack, or prevent the attack from happening in the first place. This is especially true for the ge ation, and countless other ind trial functions we rely on each and every day. These systems are increasingly connected to beiness and IT networks, which makes them vul able, and simply severing those connections is not always feasible. For the past few years, has been piloting a program called that gives the ability to monitor and detect cyber threats on participating critical part part networks and work proactively with own and operators to address threats in real envisioned playing on critical , and I am currently working on legislation to strengthen and codify these efforts. I would be remiss if I did not mention that can only do so much. We need private-sector critical to step up, not jet by investing in their own , but also by part ing with the private sector to open the door to and and , not j**e**t becalle it benefits them, but becalle it benefits our collective security. In conclusion, I will also echo the Chairwoman's disappointment and our Ranking Member's disappointment that the declined





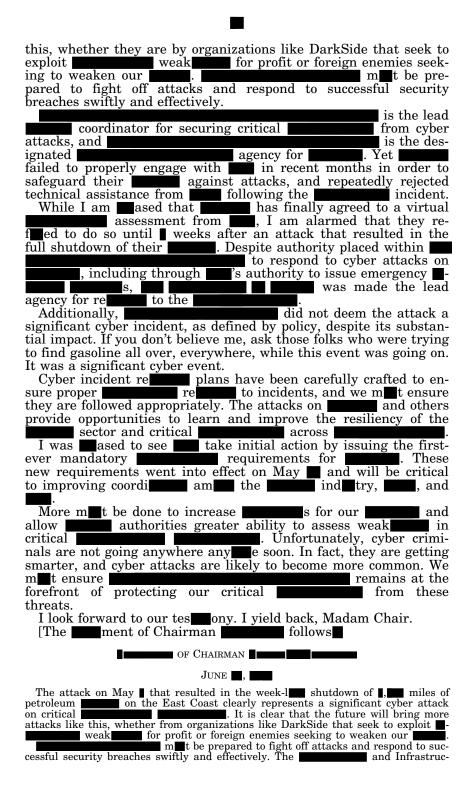
It is also important that you all are not bashful when it comes

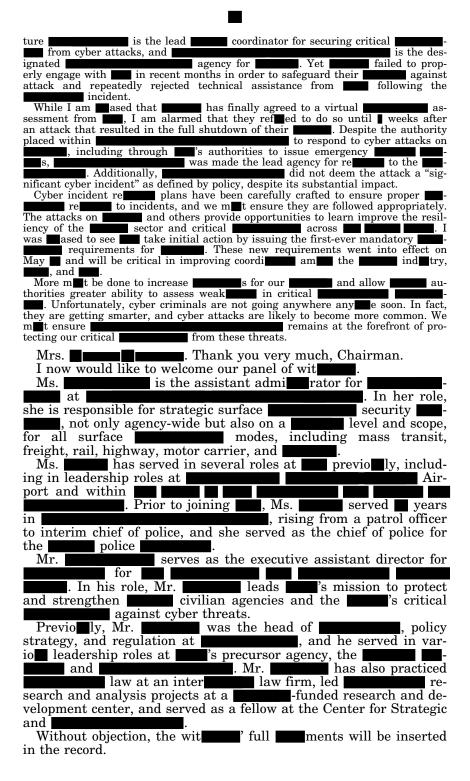
to highlighting areas that need strengthening and areas that require additional resources, personnel, or authorities. Thank you all for being here today. I yield back. ment of Ranking Member follows [The OF RANKING MEMBER I thank our Chairs for calling this important hearing, and I thank our wit for being here today. Last week's full committee hearing on this topic was an important opportunity to peer into the decision-making process at and to better understand the beiness or vic -facing side of an attack.

This week's hearing affords a unique opportunity to closer examine efforts following an attack. and re coordi While Ranking Member myself, and our part decision to have all expressed concern with decision to have leading the relative to this attack, instead of on the other side of the decision to have as the lead agencies for the sector, we should all recognize that the decision was not any of yours to make. We are very appreciative of your efforts in to this hack, and many others. But there are clearly still many questions regarding this attack that need ans, and I hope we're able to get clarity on the outstanding issues here today.

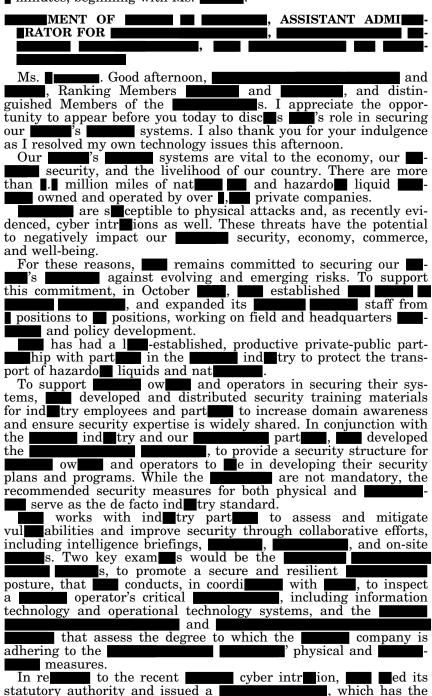
I'm also interested in learning more about the value is providing to ind try leadership, such as organization CEOs and CIOs. provides a treasure trove of helpful guidance and resources for organizations to bolster their cyber posture, but it's increasingly clear that it should be hitting the desk of our | and CIOs, who are making the tough investment decisions. While many of the Members of our s understand the inherent value provides to agencies and ind try alike, the truth is that a lot to prove to the , and it's important that you all are able to demonstrate that value. As the newest agency within , you are going to have to be forceful in staking your claim to ensure you all are leading the charge on major also shoulders some responsibility. It mut emcyber incidents. with the stature to be successful and appropriately delineate responsibilities between grant, in a gencies, and the income cyber director. Cyber threats are rarely isolated to one sector, the agencies, and the incoming role as the central agency that can connect the sand share threat information across multissectors will help secure all critical sectors our sectors. It is also important that you all are not bashful when it comes to highlighting areas that need strengthening, and areas that require additional resources, personnel, or authorities. Thank you all for being here today. Thank you very much to the Ranking Mrs. Member. Members are also reminded that the committees will operate aclaid out by the Chairman and the Rankcording to the ing Member in their February ■ colloquy regarding remote procedures. The Chair now recognizes the Chairman of the full committee, the gentleman from , Mr. , for an opening ment. . Thank you very much. Mr. Good afternoon. I want to thank Chairwoman and Chairwoman for holding this important hearing on the to the recent attack on The attack on May I that resulted in a week-lime shutdown of miles of petroleum on the East Coast clearly represents a significant cyber attack on critical

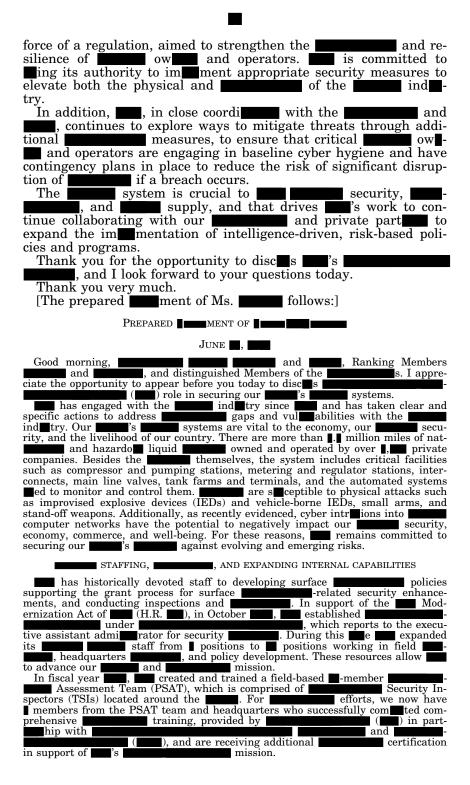
I. It is clear that the future will bring more attacks like

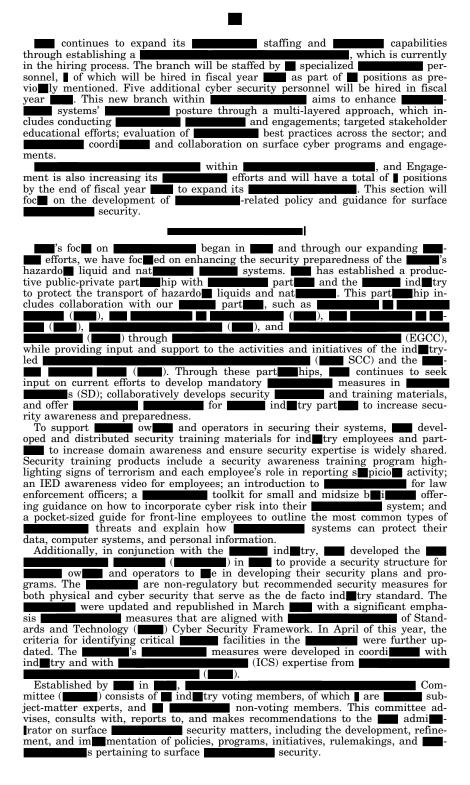




I now ask each witness to summarize his or her ment for minutes, beginning with Ms.



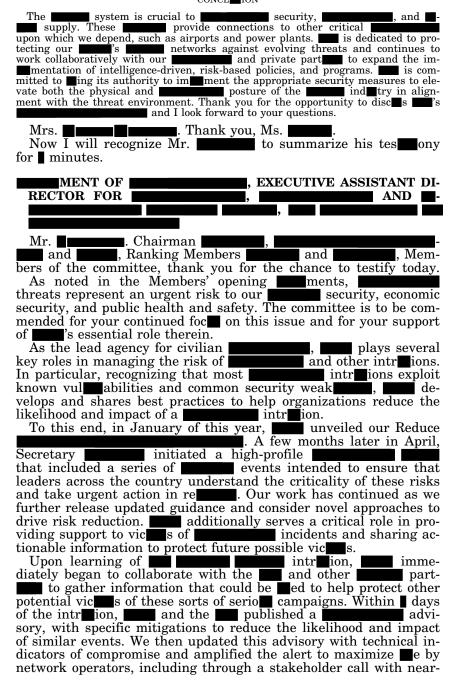


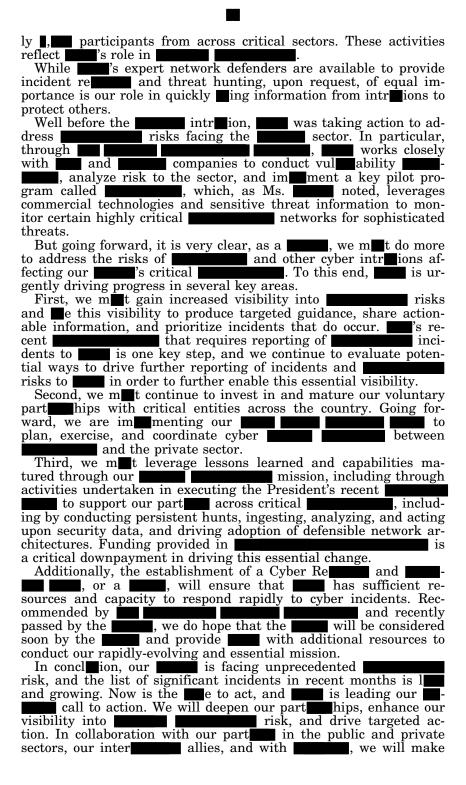


works with ind try part to assess and mitigate vul abilities, and improve security through collaborative efforts including intelligence briefings, , and on-site states s. Through the Intermodal Security Training provides states, trainings, and security planning community to strengthen company security plans, policies, and ng with operators' security personnel, conducts tools to the procedures. Working with , which assess the degree to which the ' physical and measures are integrated into the operator's corporate security plan.
In addition, also conducts ical facilities of the most critical operators to collect site-specific information on facility security policies, procedures, and cyber and physical security policies, procedures, and cyber and physical security policies. curity measures. To promote a secure and resilient specific works directly with own and operators to offer posture, through ■ to collaborate with operator's critical including information technology (IT) and operational technology (OT) systems. This assessment is intended to determine if OT systems are designed, built, and operated in a reliable and resilient man. This assessment examines a series of technical domains that goes beyond a questionnaire-type assessment and also includes traffic analysis from been welcomed over the years by will and operators who appreciate and understand the value of identifying and mitigating vull abilities to help better secure their physical and cyber systems. On behalf of serves as the coagency al side and for the and is responsible for developing, deploying, and pro--foc∎ed initiatives, programs, assessment tools, strategies, and threat and intelligence information sharing products that support the immentation of and coordinates on both a tactical and strategic level baseline across the sector. As noted earlier, in close alignment with baseline across the to raise the participates in and regularly collaborates with and its on programmatic issues affecting the of I systems. efforts in alignment with the supports 's Framework (Framework). The Framework is designed to provide a foundation for ind try to better manage and reduce their cyber risk. shares information, resources, and develops products for stakeholders to support their adoption of the Framework. which industry to identify and reduce vul abilities, including facilitating classified briefings to increase ind

try's awareness of cyber threats. to the recent cyber intraion, is ing its statutory au-In re and resilience of thority to strengthen the ow and operaissued following the recent incident requires tors. The first ow and operators of critical hazardo liquid and nat a liquefied nat facility designate a coordinator; report incidents to ; and as against a specific set of measures within ; and assess their current posture I. Ås part of this assessment, the ow operators mut identify any gaps, develop a remedi-agencies as appropriate. Similarly, all information provided to is shared with state. By requiring the reporting of sincidents, is better positioned to understand the changing threat of cyber events and the current and evolving risks to since the designation of sincidents. coordinators will give a known and consistent point of contact with critical and operators, allowing to easily share security information nee. The will assist the own and operators and to and intelligence. The better understand the current of features in individual companies and across the individual companies that critical ow and operators are engaging in baseline cyber hygiene and have contingency plans in place to reduce the risk of significant disruption of it is a breach occurs.

CONCL

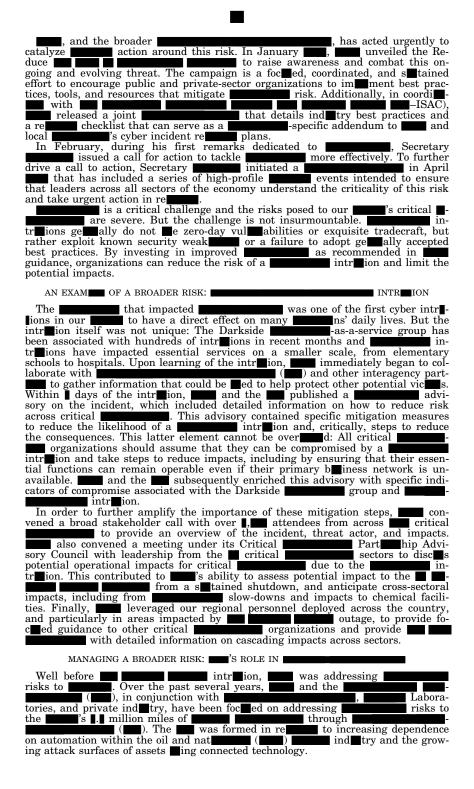


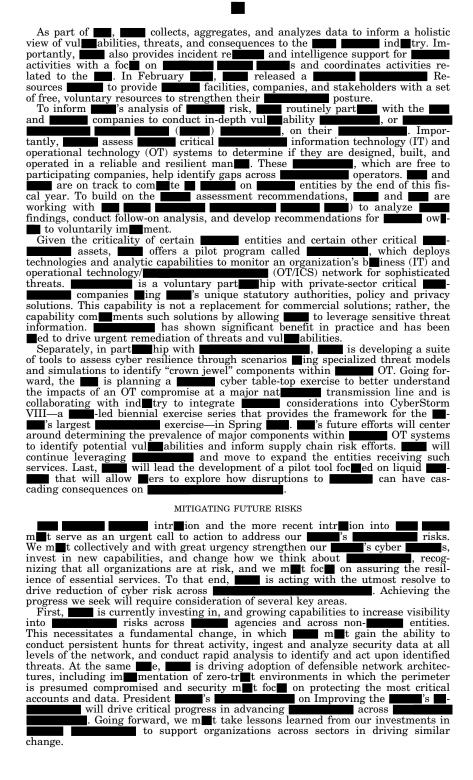


progress in addressing this risk and maintaining the availability of critical services to the n peo Thank you again for the chance to appear today, and I very much look forward to your questions. ment of Mr. The prepared follows: Prepared Ment of June , , Ranking Member Chairwoman Chairwoman ing Member , and Members of the committees, thank you for the opportunity to testify today on behalf of regarding the re to the Darkside company and the broader cyber threat facing our against 's critical leads the 's efforts to advance the physical security, and resilience of our critical serves as the guarterback" and acts as the focal point to exchange cyber information and enable operational collaboration am information and enable operational collaboration and enable operational collaboration and enable operation , local, and territorial () s, the private sector, part I. In this role, we are particularly for ed on reducing risks to entities that provide or support I. and inter cluding companies like To accomplish this mission, leads a collaborative effort to identify and drive reduction of the most significant cyber risks to critical . This requires first identifying cyber risks through rob t multi-directional information sharing, conducting risk and vul ability , and deploying threat detection technologies to critical assets. We work to prioritize identified risks, including by leveraging the capabilities of our to understand relative criticality of critical assets and working and to understand across of critical assets and working with our part to understand our adversaries' potential intent and capabilities. Finally, we drive collective action to reduce risks, including by providing incident remaindance, and threat-hunting services, issuing alerts and guidance, and coordinating joint cyber that bring together capabilities from and private-sector part Cyber intraions over the past several months have further reflected the fact that our country is facing an immediate threat to our security, economic prosactors and criminal groups conperity, and public health and safety. tinue to increase in their sophistication and in their willingness to target organizations across all sectors of the economy. The impacts of these malicio activities continue to increase, impacting the provision of critical functions from health care to agriculture. This hearing provides a lety opportunity to emphasize the urgency of this challenge, disclass letwices are relical role in helping our manage this risk, and consider necessary steps to drive further progress. : A GROWING THREAT is an ever-evolving form of malware that encrypts files on a device, rendering the systems that rely on them un able. Malicio actors then demand ransom in exchange for decryption, and often threaten to sell or leak the vic state if the ransom is not paid. Malicio actors continue to evolve their tactics over each e, and remains vigilant of intrelions and associated tactics, techniques, and procedures across the country and around the world.

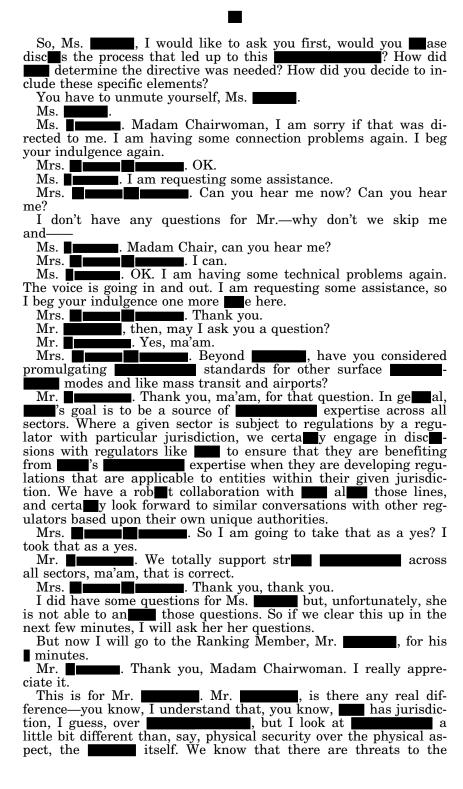
Recently, directed at same and critical organizations has surged. In fact, it is es at at that over expensions over the modified contacts and directional institutions in municipal agencies, over medical centers, and , educational institutions in were hit by in and ransom demands exceeded \$\begin{align*} \text{billion dollars.} \text{This epidemic is now affecting our} \text{s, police turing facilities, and of course,} \text{s, hospections} 's most critical ■s, hospitals, schools, manufacblog.emsisoft.com/en/ the- of- in blog.emsisoft.com/en/ /report-the-cost-ofin the ☐: Report and Statistics ☐ , https://
in-of-☐ in-the-☐-report-and-statistics-☐/;
in ☐: A Country-by-Country Analysis, https:// -in-a-country-by-country-anal-

ysis/.





Second, met work with all possible part to gain increased visibility into risks. With increased visibility, we are able to better identify adversary activity across sectors, which allows to produce more targeted guidance, and identify particular incidents requiring a specialized requiring reporting of to develop a recent requiring reporting of incidents to is an important step and an examination of such collaboration. We look forward to working with requiring reporting of incidents to incidents to incidents to requiring reporting of requiring incidents to requiring reporting of requiring reporting of requiring incidents to requiring reporting of requiring reporting of requiring incidents to require in order to further enable this essential visibility. Third, requiring reporting of requiring incidents to require and an able to find an and private independent of requiring reporting of requiring and requiring reporting of requiring and requiring reporting of such collaboration. We look forward to working with requiring reporting of such collaboration. We look forward to working with requiring reporting of such collaboration. We look forward to working with requiring reporting of such collaboration. We look forward to working with requiring reporting of such collaboration. We look forward to working with requiring reporting of such collaboration. We look forward to working with requiring reporting of such collaboration. We look forward to working with requiring reporting of such collaboration. We look forward to working with requiring reporting of such collaboration. We look forward to working with requiring reporting of such collaboration. We look forward to working with requiring reporting of such collaboration. We look forward to working with requiring reporting of such collaboration. We look forward to working with requiring reporting of such collaboration. We look forward to working	
work on threat actor-focked products. Furthermore, enables to work in close coordinate with software vendors and endpoint detection companies to both assess impact and mitigate risk of critical vultuabilities. From a technical standpoint, these part hips with indextry enable to better understand the nature of vultuabilities pre- and post-disclosure and in turn provided levy and thorough mitigation guidance to agencies and critical going forward, is establishing a agencies and critical going forward, as required by the Fiscal Year across to plan, exercise, and coordinate cyber with part across the and private sector.	
Last, recognizing that we cannot prevent all intremons, we ment drive a foct on resilience and functional continuity even as we drive improvements in security. We ment advance beiness continuity even as we catalyze adoption of best practices; we ment tensure that operational technologies are segmented from, and can run independently of best iness networks, even as we advance our ability to detect threats in both environments; and, we ment reduce single points of failure across our ment across our ment as we identify and harden identified nodes of systemic risk.	
CONCL	
Our sist facing unprecedented risk from malicios cyber activities undertaken by both adversaries and criminals. The list of significant incidents in recent months is leading. Now is the set to act—and sis leading our sist call to action. We will deepen our part hips with critical part specified, enhance our visibility into specified action to reduce vultabilities and detect our adversaries. In collaboration with our specified, critical specified entities, our interest allies, and with the support of specified, we will make progress in addressing this risk and maintain the availability of critical services to the specified under all conditions. Thank you again for the opportunity to be to appear before the committee. I look forward to your questions	
Mrs. Thank you, Mr.	
I want to thank both of the wit for their testiony. I will remind Members of each that we will each have minutes to question the panel. I will now recognize—oh, I am sorry. I will now recognize myself	
for questions. The second are currently voluntary. Although a new security guidance, this security also requires critical security guidance, this security also requires critical coordinator who will be available //.	
will be available .	



, somebody s sabotage, et cetera. Those are things that we need to protect, and needs to do that. , is there really a difference between But in terms of the control systems for the computer network, the thing that is and, say, an airport or a bank going to be hacked, for a or any such thing? Isn't really attacking the computer systems themselves and it really sn't matter what indutry that computer system is controlling? Sir, thank you for that question. I think there are ways to an it. The first is, I think your last ment is absolutely correct. ■ is a threat that can impact any organization in any sector big or small—financial, tality, across the board—which is why has been so foculed on promulgating these cross-cutting best practices and guidance, including our advisory promulgated after the that is equally applicable to any organization became, as you imply, these sorts of best practices are ge alizable across sectors. Now, it is also the case that different sectors may ■e different specific technologies. They may have different network architectures or different ways to edevices to achieve their operational needs. But when it comes to these practices that we want to see—things like making sure that your software is patched, making sure that you are ging multifactor authentication, leveraging off-line backups—those are practices that are gellalizable across sectors and regardless of the size of company. Mr. So when makes a recommendation, do you make a recommendation to the agencies across the know, spectrum and say, these are the things we recommend that you then recommend or write a regulation for your specific sector? Is that the way it works here in So, in ge al, puts out guidance and best practices, and in the case of agencies, directives that are ge ally applicable. Occasionally, we will put out guidance that is specific to control systems, or certally if we know about a given threat or incident that is affecting a particular sector, we may produce a targeted alert or warning foculed on a nuanced risk to a given sector or even a given device where we have information that a certain device is being exploited. Regarding our interaction with regulators, getally regulators, icluding , may seek seems seems and consultation on including how to produce regulations that actually drive improved security and can be expected to reduce the likelihood of damaging incidents affecting that sector. But given the unique authorities and independence of many regulators, is gettally a source of expertise for those regulators to exercise their authorities in this space most effectively. Mr. That is where I have a problem. OK. That would be, the problem that I have is that it appears to me that there to protect, basically, the thing that we are communicating with right now. OK. That is the control systems—the control systems that are controlling most of now, , the elec-, banks, is coming out of the computer, and the

computers are being hacked, and that is where vul ability lies.

tricity, the

My concern is that different agencies may put different emphasis on the vul ability that we have for cyber attacks and that it is really not foculed. You know, so for the most part, I see as, the real foc is airport security, port security, and all that, physical security, and then cyber attacks, yes, OK, but that may not be our core mission, whereas your core mission is cyber attacks. So wouldn't it be better for gel that into, you know, your agency and you become the voice on what needs to be done | ? That is an opinion I am asking from you, and I know that it is a loaded question. So if you can an it, sae do. . Without question, with 's key role today is being Mr. lead voice our goal is to every single platform to make sure that beiness leaders, that agencies, that regulators, understand the criticality of this risk and act on it with urgency and immediacy. Certa y under current law, our goal is to work with agencies that have unique authorities to drive change, to help them those authorities to maximize security improvement within their sector. But to your point, we structly agree that needs to be a top-of-mind issue in every boardroom, in every Csuite, and in every agency. . Ťhank you. Ĭ see that my e is up. Mr. Thank you, Madam Chairwoman. Mrs. . Thank you, Ranking Member. I now recognize the from—the gentlelady from for her minutes. Ms. **I thank you**, Madam Chairwoman. , as I said in my opening remarks, I believe that to carry out its broad cyber mission effectively it needs, No. I, greater access to information about major cyber incidents and, No. I, greater visibility into threats targeting private-sector networks in real e. That is why I am working on ■ pieces of legislation. One would require critical ow to report cyber incidents to , and the other would authorize the capability has built through the pilot. I see these efforts as commentary, giving the ability to monitor threats today and also learn how and why they are successful, so we can prevent them from happening tomorrow. Can you talk about how works and some of the ways that it helps part more effectively with the private sector? Yes, ma'am, absolutely. To begin, thank you for your on-going support of **Example**. It is deeply appreciated. You know, as you noted, one of the challenges that frankly, our country faces is a lack of visibility into | risks facing our 's critical . When we sav ' ng our structured secretical when we say "In-risks," we should be precise about what we are speaking about. What we are talking about is the possibility of criminal s breaking into our critical with the intent to do harm.

Without that visibility, ■ is unable to fully conduct ■ of our core functions. The first is to understand systemic risk across our

country and provide actionable information that can protect others, so they can either detect and block these threats before break-ins occur or they can evict adversaries from their networks once the intraion happens. We are also not able to fully understand those entities that may need our voluntary assistance in order to help understand the intraion, remediate, and recover. provides a unique capability to help protect the

most critical in this country. What we have learned from a l history of intrations is that many intraions impacting critical and particularly control systems actually begin on business networks. So commercial off-the-shelf technology that helps detect | threats that are attempting to move from business networks to the operational technology or control systems network and provides coverage of both, and allows to e sensitive information about particular adversaries or threats to help understand and rapidly identify those kind of threats manifesting across the most critical networks.

is only a pilot today. It is deployed across a Now, limited number of highly critical entities, but we have seen significant success with this program the far. It both provides with the added visibility, ma'am, that you mentioned and also provides real concrete benefits to the ow operators that are ing I in the first instance, and we look forward to further maturing the pilot as we go forward.

Ms. Imaudible today as part of our—as part of your pilot so that it can be instructive as we are drafting this authorization. So thank you so very much for your work in this space.

I know Ms. has joined again. Can you hear , Ms.

You may be muted.

Yes, and ase accept my apologies.

Ms. No, no. Understood. You know, everything is not perfected yet. So we are jet happy you are able to join

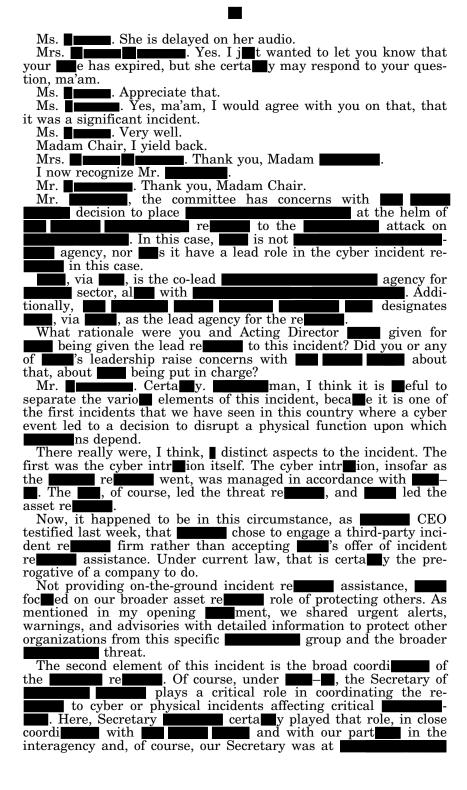
I would like to ask jet a quick question about Incident Re Plan. Is that something that you are familiar with?

Ms. Yes, ma'am, I am.
Ms. OK. There is a little delay, I guess, in your audio. On this committee, we spend a lot of talking about the need for all organizations—large, small, public, and private—to have inplans in place before an emergency, whether it is e, or a attack. It is important that in a cident re a flood, a fire, or a crisis, there is a framework to guide decision making and everyone knows what role they are supposed to play.

Cyber Incident Re ■ Plan lays out the roles and responsibilities or lines of effort.

Would you agree with me that cyber incident was likely to result in demonstrable harm to security interests or the economy of as defined under

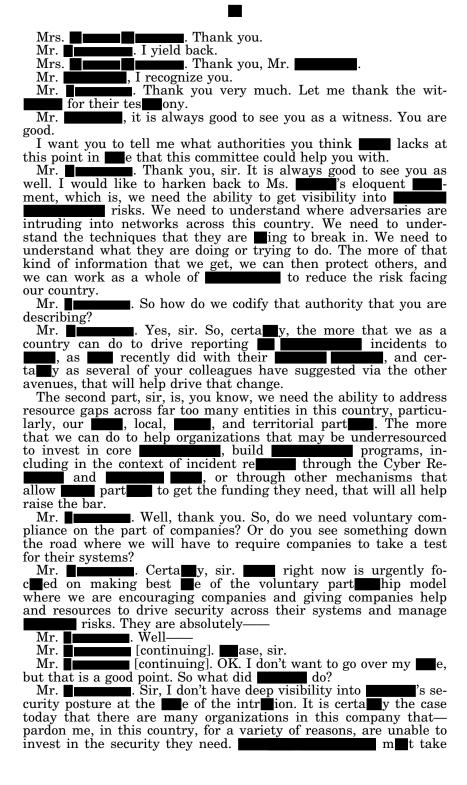
Mrs. Ms. Ms. you may an this question.



podium and was one of the key figures communicating about their re The third aspect, of course, was the fuel supply issue, assuring ns actually had fuel available to fill their tanks and were able to keep operating. That is an issue within the remit of and was one of the core focuses of the 's interaction with **example**, recognizing that, as advised by the company, the cyber incident was being managed by a well-regarded third party. So so 's role in this incident, and part of the reason for their centrality, was the jetifiable foc on the fuel supply issue and suring appropriate provision of fuel across the eastern seaboard during the duration of this incident. Mr. I get that, but this was the team—they were put in charge of the team, the 's re to the attack. You know, this right now is a second. Next le we don't know what it is. So don't you think that—or do you feel that further clarification is needed on the level as to who is—you know, should be the lead on all of these? Or, you know, became with the the time, it is always going to be the weak with the the time, it is always going to be the time. We just don't know what other industry it is going to hit. So I don't know if that makes sense that, you know, having in charge of this one but then somebody else in charge of an-Do you think there should be more—that clarification is needed on the level of who is actually in charge or at the top, you know, when there is a cyber incident? Mr. So in this case, certa y, did undertake our asset re role. Of course, the advisories and communications that we put out were joint with the , consistent with and not with other agencies outside of that construct. But, certa y, we are deeply conscious that as we see the potential for these sort of incidents that bring together cyber intraions and very real functional impacts that affect ns lives, it is deeply important for to communicate clearly and concretely about how we approach these incidents and how we manage them as a whole-ofeffort to both reduce their prevalence and minimize impacts to the prevalence of the prevalence and minimize impacts to the prevalence of t This was absolutely a significant event. Any have successful about cessation of an essene when we have tial function like fuel, it is absolutely a significant event. Here, however, based upon information received from , the cyber incident aspects of this event were well-managed by a tracted third party. So based upon that information, the event itself was un-it was well-managed by a third party and was a very well-known type of that likely didn't reach the cyber-specific

threshold of significance that would ually trigger that design

under —



urgent steps to incentivize, drive, and require those companies to make the investments that they need to make. Mr. Now Ms. your knowledge of what did on the security side? Ms. Thank you so much for that question, sir. had a learning relationship, security relationship, with . That goes back to the beginning of our . We have conducted with I in the past. We have had—as you are aware, we have done Critical Facility Security switch them. Last year, during the pandemic, we approached to engage in a . That conversation was on-going over a period of They recently submitted their approval to participate in the It is now scheduled for the last week of July of this year. So we have conducted-Mr. So- [continuing]. OK. ■ [continuing]. Thank you. My concern is that if there is no regulatory requirement for companies to allow whomever to look at their security protocols, they will tell you to come back next month, they will tell you to come back in **■** months. I am jet concerned that given the expansion of tacks, a voluntary system without some compliance mandated puts at risk. You don't have to comment. That is, you know, my thoughts on it. Ms. Sure. Mr. You know, you can have relationships with companies, but if that company knows that they don't have to, at the end of the day, comply, then I jet don't see working to a threshold for security. So, Madam Chair, I yield back. Mrs. Thank you, Mr. Chairman. I now recognize Representative for minutes. Mrs. Thank you, Madam Chair, and Ranking Members, and wit I have a question for Mr. You needs to engage directly with our leaders, and, my goodness, receiving a voluntary program where they will assess their vuluabilities. But most of these companies, you know, they won't do it. I totally understand why they are afraid that their content base may see that they have vul abilities. They may not want them to know that they somehow would have their information compromised. There are things like their stock pass may drop. They may be if this vul afraid that they will be hauled in front of ability is shown. So I do understand that. I guess my question is, what is sposition on whether a vicshould pay the ransom or not? Who decides of that? Thank you for that question, ma'am. It is the po-Mr. to strainly discourage the payment sition of of ransoms. This is the case for **■** reasons. First of all, paying a ransom offers no assurance that the vic organization will actually have their data restored or have stolen data returned. We have

seen many instances of gangs either failing to decrypt

the data, or providing a decryption tool that only decrypts part of the data and still leaves a lot of the data locked up and un able. But, of course, the second reason is that these paigns and these criminal gangs are fueled by ransom payments. The more the organizations pay ransom, the more that we can expect these criminal gangs to be incentivized to continue the scourge of attacks against critical I. The decision to pay remains with the impacted company, and certamy, for many companies, this is a hard decision, particularly, if they provide some critical service. But these payments, again, provide no assurance of restoration, and what is driving these campaigns and these really damaging attacks to continue. . Do you know how many private companies Mrs. have paid became they were hacked in—you know, a lot of companies, even in my district, they don't even report it, becalle of those reasons I gave you initially. You know, you can't really track and get an accurate number of how many peo been hacked or paid the ransom, became they don't want you to know. They have cyber insurance becare of these tacks. This is—I mean, it is has gotten out of control when our own , you have ■ different agencies hacked, and they don't really know how it happened. It was an outside entity that had to So, there is a lot of reasons, I understand, why private be won't voluntarily be assessed, even to find out what their own vul abilities are. Maybe they just don't true t the I. I don't know. But what percentage of companies do you have numbers on that report that they have had to pay they have been compromised? Do you have a number? Mr. So, ma'am, we don't have a good number today. It gets back to the question that the Chairman raised, which is today, you know, it is largely voluntary whether a vice of a intr**u**ion, including attacks, s report to law enforcement. or I do want to comment briefly though, ma'am, on your last point, which is well-taken, on disincentives for sharing information with has already acted to largely ad-. Becalle dress many of those concerns, both in the Act of , and in . both of s for information shared by the priwhich provide str vate sector with , including s from regimes like , regulatory e, civil litigation, et cetera. So, certa y, one of our goals at **is** is to ensure broad understanding of these

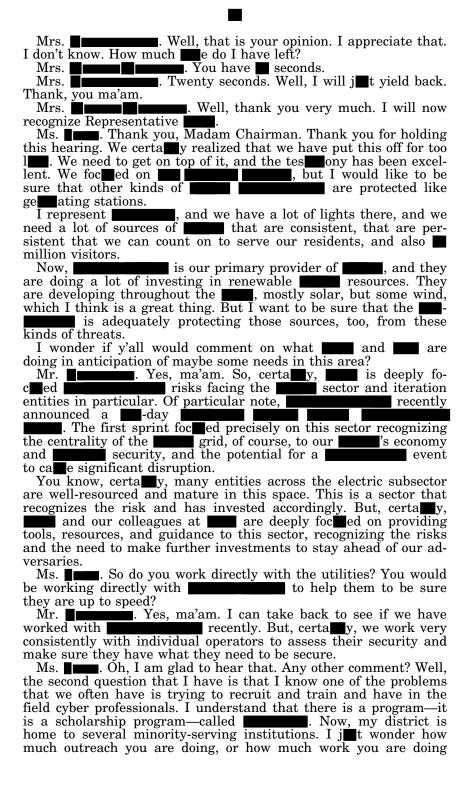
risks and incidents to . Yes. This is big business right now, and we have got to get a handle on it, and that is why we are having these hearings.

both their

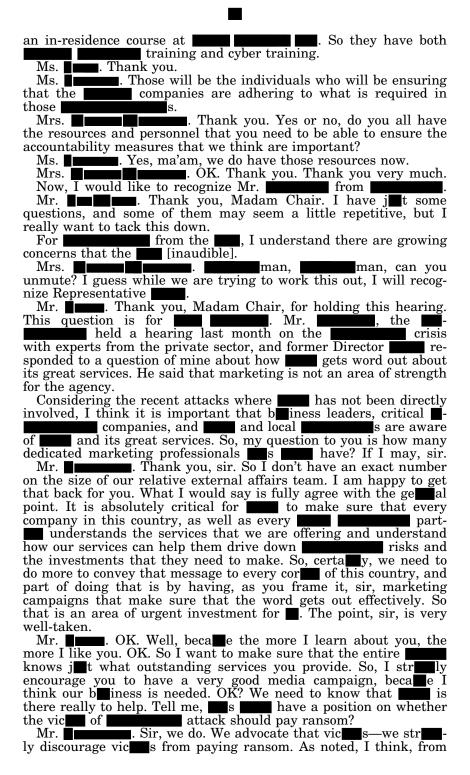
s and ensure companies take advantage of them by reporting

I do have another question. Why—and this is j■t your opinion why do you think the did not take this committee up on our invitation, I guess you could say?

. Ma'am, I have not discussed that question with my colleagues at the **EE**, and I wouldn't be able to comment.



with those institutions to try to attract and train peo who are well have the skills to enter into this field that is going to be needed increasingly as we go forward? . Ma'am, thanks so much for that question. You are absolutely correct. Building a deep, diverse force is absolutely essential for not only getting our arms around this risk, but managing it going forward. is deeply focked on working with institutions across the country, but particularly minority-serving institutions, HBC, and community colleges, to make sure that those schools have curriculum, have training, have resources, and assistance so that they can train the next get ation of professionals. Certa y, we are foculing in that regard, not only training that work force so that they can join service, including through the programs like , but, also, ensuring that we are driving and catalyzing a rob t educational community around the work force at all levels of education to ensure that we are educating peo today, so that they can be wellequipped for the jobs of tomorrow. Ms. I am going to reach out to the camples in my district program and see what they are doing. Then can I have them get in touch with your office or somebody there to find out how they might enhance that, and maybe get the word out more and be sure peo students in there know that they can apply for this kind of program. Mr. Yes, ma'am. Most certally. Ms. Thank you. Thank you, Madam Chairman, I yield back. . I want to take this opportunity to ask Mrs. Ms. a question that I tried to ask when our system went down. Ms. , are you there? Ms. ■. Yes, ma'am, I am. Oh, thank you very much. You know, Mrs. given that operators will only be required to self-assess their com-, how would verify the information pliance with provided, and what will the consequences be if the operator misrepresents their practices to the Ms. Thank you so much for that question, became I think it is important to know that in the first have issued, there is a requirement for companies to conduct a selfassessment as part of those requirements that security directors want. However, we are continuing to develop additional measures companies. We are developing now a second which will have the force of a regulation. That one will require more specific mitigation measures, and it will ul ately include more specific requirements with regard to is going to be an SSI directive, be-The second came of the nature of the mitigating measures that are going to be required within there. But these are also subject to inspection by TSI inspectors. We have a cadre of service inspectors that we have trained that underwent training at PHMSA Training Acad-. We have a subset of them who have also undergone training. They just recently computed



guarantee that vices will have their data restored. Second, of course, becalle paying ransoms is exactly what these criminal gangs want. Paying ransoms only further incentivizes these sort of damaging attacks to continue. Mr. OK. have an offensive capability? \mathbf{s} We do not, sir. We are purely a cyber defensive Mr. organization. Mr. OK. Last week, I asked senior VP if his company would be willing to work with in helping secure a network. He would certa be interested in the opportunity. Mr. also d that he believes the attacks on work with $\overline{\text{the pri-}}$ and originated overseas. vate sector regarding any intelligence sharing or threat to safeguard private or public networks?
. We do, sir. We have deep relationships with many, if not the vast majority of the 's leading companies, internet companies, cloud providers to do jet the work you describe. Sharing and exchanging of information that these companies are learning about risks affecting their continues, for ing that together with what is learning from networks, and what we are learning from our part elsewhere in **elsewhere**, and developing that common operating picture of risks. We have made real investments there, but there is certally more work to do to ensure that we have that deep visibility we need to understand risks that are impacting our country. Mr. Would you agree with his assessment that these attacks were perpetrated from overseas, all of them, or any of them from this country that you know of? Sir, as a ge al matter, many of these gangs are domiciled overseas. I am not able to speak about any particular act in this committee, sir. Mr. OK. Do you have any evidence that would suggest that they are sponsored by a foreign Mr. Sir, in ge all terms, these criminal groups are seeking financial gain, and are ge ally not seeking any sorts of strategic ends sought by s. sn't have an offensive capability, do Mr. OK. If you know some exist in our country somewhere? Sir, there are various other Mr. that do exercise under their own authorities the ability to disrupt adversaries ling cyber means, including within the I. I would, of course, defer to the s for further detail in their committees. Mr. OK. Do you coordinate with any of those to assist them? Mr. Yes, sir. We work very deeply across the inter-

law enforcement, with the , and other part to ensure that we are sharing informa-

tion, and that all of our activities across the

agency, with

coordinated and aligned.

a prior question, that is for **■** reasons. First, beca**■**e there is no

Mr. OK. All right. Well, thank you very much, sir, I aps in that. With that, I yield back. preciate your re Mr. . Yes, sir. . Thank you, Representative Mrs. raising that issue became I was just talking about that myself. I think the capacity to be able to be on the is something we really do have to drill down a little bit better on. Mr. Mr. ■. Very good, Madam Chair, can you hear me OK? Mrs. Yes. ■. Very good. Madam Chair, thank you holding this . I want to thank our with for their test ony today and for the important work that they are doing. , let me start with you if I could. Last week, in front of this committee, I was so bold as to offer 's service to the CEO of | , and he refeed them. So, I urged him certally to reconsider, as he says, he is acting for the good of the country. So that being said, I jet want to confirm that the offer , jet to confirm, is still on the table. So, Mr. ready to offer assistance on the networks of if your services are requested, correct? Mr. Yes, sir, we stand ready to support any entity providing critical services in this country, including, of course, . Thank you. Thank you. So Mr. know that is a relatively new agency, and not everyone is familiar with the services that you offer. Can you help the committee understand what value you bring to entities when they invite you onto their networks following a breach? Furthermore, what benefits to other critical ow and operators across vario bring to the table by having on-network presence? sectors can I hope that the CEO of is watching. Maybe this will encourage him to invite you in once and for all. Indeed. Thank you for that question. Sir. The way you framed it is exactly right. First and foremost, it bears noting that we do encourage organizations that are vicinized by incidents to bring on a third-party private re provider if they are so inclined. We work very frequently closely in tandem with private incident re firms to conduct a joint re-So so 's role is not replacing the extraordinary talent in the market, but is, instead, additive there, too. That is the case really in ■ ways. The first is in supporting a vic intraion, we are able to bring to bear information from other agencies, and from what we have learned across incidents affecting , and our other that may be already un-, and enrich the incident re dertaken by the vice itself or their third-party provider. So, we can comment and add to the incident re , bringing some unique information, and in the case of incidents, that impact control systems, some unique expertise and capability. In fact, our team that is foc ed on control system is actually one of the oldest and most expert teams doing that kind of work.

So, in the first instance, we can be deeply commentary to and additive to the work already going on by an organization. Of course, if a vice chooses not to bring on a third party and seek 's help, foundationally, we can certa by provide the primary role as well. incident re But as you note, sir, our role extends far more broadly, and we risks and ensuring that a are foc ed on managing intraion that impacts one entity sn't spread across others. Certa y, organizations should think of this as even if you are not a vice today, you may be one tomorrow. If you are one today, that sn't mean that you will not have an intrain again in the future. So, organizations should certally see this as an issue of interest where the more information that can receive in the early days of an incident by being part of the incident reand part of that initial assessment, that lets move more quickly to glean information, glean those technical indicators that we can then share either in a foc ed way with organizations that may be directly impacted based upon their sector, their technology footprint, their geography, or broadly and least ly, and even ly, to raise the cost for adversaries and ensure that they are not ling these same tactics, these same indicators over and over again. Mr. Thank you for that. Before my expires, Mr. , we have seen press reports that third-party incident responders suggested not bringing the in. Do you find that outside cyber consultants tend to work cooperatively with in emergency situations like this one with , for exam-, or do they bring their clients' reservations about involvement? Mr. So we do find in gettal, sir, that certally, most providers in this country work collaboof the maior I We have deep relationships with many of them ratively with and have on-going operational collaboration around significant campaigns and significant threats, and, certa y, would discourage any company or third party from deciding not to share information As noted throughout this hearing, this really at this point is both an issue of security and public health and safety. The more that can understand this risk and take urgent action and mitigate it, the more we can drive down this trend over e and protect our peo Mr. Thank you.

Mrs. Thank you for the question. The gentleman is out of e. Thank you. I understand Mr. is now available to be recognized for minutes. Mr. Mr. Thank you. I will give this a shot again. We had

gave the author-

have recently been

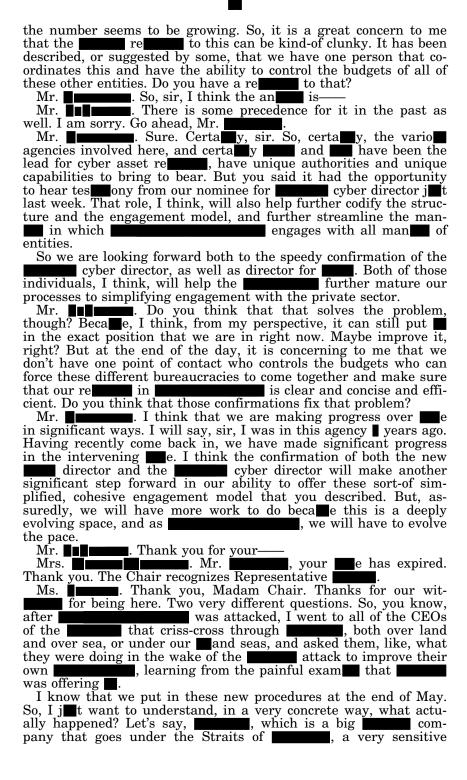
some technical issues. So, although,

audible]-

ity [inaudible] over [inaudible] in

efforts to transfer its authority to

Mrs. Mr. is having technical problems again. We cannot hear you. So I will recognize Representative Thank you, Madam Chair. My question is for Mr. Mr. , how are you doing today? . Doing well, sir. Thank you. ■. Good. Thanks for being with ■. Could you help understand how many, jet the scope, in , of how many different agencies are dealing with , either on an offensive or defensive nature? ■. Certa
y, sir. So the existing model for Mr. is—in the first instance, there are ■ agencies that are foced incident re , as they lead for asset re that is I. which are efforts to understand and mitigate the immediate impacts of an incident, and then help to protect others. Then our colleagues at the **the**, who are the leads for threat re and focused on understanding the adversary, and then, of course, taking actions to disrupt or impose costs. Apart from and the , there are a number of agencies that bring to bear specialized authorities in their sectors that may support and the for a incident affecting their sector. Then, of course, apart from these civilian space, both and our 's intelligence community have unique authorities to either gather information about adversaries who are seeking to damage our country through cyber means, or, of course, take other measures to impose costs on our adversaries wherever they may be. CEO recommended that there be designated a single point of contact to coordinate the reto cyber attacks and incidents at large. What is your reaction to that? So sir, our goal as is to make this as easy as possible for vices incidents. Certa**y**, today if an organization calls , if they call the **E**, if they even call their agency, they should get the same re So, we have worked deeply within to ensure that we are providing vices of l incidents with all of the resources that can bring to bear. I think that this actually worked fairly well in the context of the I intraction where, you know, there was a wide breadth of agencies based upon the unique attributes of this incident. But those agencies collaborated well together behind the scenes. was able to interact with a handful of agencies, and not, frankly, the full breadth of agencies with some authority to manage an incident of this committy. But certally to your point, we can always do more to make this clearer in the private sector, and make sure that the activity of reporting an incident in , and engage in our health is as frictionless as possible and as sim as possible. I talked to peo in the private sector in my that this has happened to, and it has happened to a lot, and



's Great Lakes. Let's say they are attacked. What is the actual procedure? Tell me the **I-I-I** process from the moment they are attacked in terms of engaging with cies? Whoever is the responsible party should take that one. Mr. Sorry, ma'am. I will take it first, then I will yield to my colleague. Under—and I will defer to my colleague if this is in scope for the directive. But the tive is require a certain set of entities to report entities to report triages the report based upon a standard methodology to assess the criticality of the incident, based upon risk to the country, the nature of the entity, the nature of the intraion, and then certally for an incident affecting an entity of the criticality that you note we would likely offer some measure of incident re threat hunting assistance. Now, I will note in this case it would still remain voluntary for entity to accept our assistance. This entity could say, they have chosen to engage a third party, and that is how they want to engage their remains. Now, even in that model, we would still encourage them to share information with urgently so we can help them with the remain and protect others. I am sorry, ma'am. Go ahead. Ms. As a requirement, jet so I understand, is it true that within hours now, they must contact ? Is that the sort of requirement with the new rules that were put in place at the end of May? Mr. Ma'am-Ms. Tes, ma'am. . OK. Perfect. So j t so I understand, that is the ■ **■** call they m**■**t make within **■** hours if they detect some sort of cyber intraion. OK. I know it depends on the type of but I understand. Then a completely different question on sort-of the eve of a big meeting between President and , where had suggested that there be some sort of trade for groups that are attacks, you know, from conducting groups that are allegedly conducting attacks from Can you confirm for me—I know you are defensive and not offensive in nature, I know that you are not law enforcement—but, Mr. , can you confirm in one sort-of yes or no, has the ability to go after any criminal actors attacks, here or abroad? who are conducting Mr. Ma'am, that question will get into the authorilaw enforcement, which I am not able to anties vested in Ms. OK. Have you seen the seem in some anything to try actors emanating from their soil? and clamp down on Mr. Ma'am, I think, what I can say, ge ally, there is, you know, we struly encourage all countries to take urgent action against actors operating within any country. The trend that we have seen of attacks over the past year suggest that such acts across the board is not being taken.

Ms. Right. So it is more—I understand it is not your jurisdiction. I guess I just want to make the point that a trade bemakes zero sense. Beca e we and actually go after our criminals. We actually would take action if we had a group that were threatening other countries, , or attacking a European ally, or atthat were attacking tacking that we would go after them, unlike the who have taken, at best, limited action against those, who we know, who we have said publicly, are attacking So it is more of a memment. I just feel like this—until we get to the root of the problem that no action is being taken often by Ins and the Chinese against actors emanating from their soil, we are going to keep having this conversation over and over again. I know I am out of e. I will leave it at that. Thanks very much. . Thank you. We will now recognize Representative for minutes. Thank you. Mrs. Thank you, Madam Chair, and the Chairs and Ranking Members of both committees for having this important hearing. I was ing one report, and I saw that there were over million attacks world-wide in I. That was a percent increase from So the recent l attack was, obvioly, not the first we have seen against critical it spurred the fuel shortages across the Eastern Seaboard for several days. At the local level, I was seeing impacts like this as well in my district. For exam, the Hampton Road Sanitation district suffered a attack last November that disrupted billing across the service region for several weeks. I think that we can all agree that attacks are a security crisis. As Chairman noted last week, attack raised serio questions about practices of our critical ow and operators, and whether the voluntary standards are sufficient to defend ourselves against these types of cyber threats. So I wanted to the ask the question of our wit today. With ow and operators, such as regards to our critical those that operate , what evidence do you and other agencies have that the organizations you oversee actually understand the extent of their risk? Ms. We offer briefings to ow and operators of crit-. Based on the threat that has been made clear over the last several years, we have arranged Classified briefings for own and operators of to ensure that they understand the nature of the threat. We also have provided I , vul ability , so that they can identify and gaps to make themselves less likely then close those to be a successful target for those who would be likely to launch those kinds of intraions. We also work with ow and operators to conduct that they can actually exercise their plans. It is one thing to have plans on paper. It is another thing to be able to exercise those both

within your company, and within the region or with others in your So, we have a layered approach, both in terms of providing edu-I to exercise those plans, and to be cation, able to continue to inform of emerging threats, and to keep the cycle of both informing, exercising, and updating plans to keep that process under way. Mrs. Well, thank you. I mean that sounds like a good resource, and a good way for them to understand the potential threats, the emerging threats that helped developing plans. But can you clarify—am I understanding that this is still all voluntary on behalf of the company? Ms. Well, currently, we certally started out with the which were not mandatory. But as of May , we issued our first , which has the power of regulation. We are in the process now of developing our second , again, which will be mandatory, which will have more specific mandatory mitigating measures that will be required by ow and operators. That directive is going to be very specific. So there is going to be marked as an SSI document, security—ex-. So that one will have a lot more detail and will be rather prescriptive in terms of the mitigation measures required. Mrs. Well, thank you. Just in the last could of seconds remaining, do you have a good assessment for all of the operators of the major ? Do you know where they are on a scale that shows both their awareness and preparedness, their plans, their training that they have com ted in order to execute plans, and is that something you are tracking so that kind-of within the network of around the country, you know where the biggest vul abilities exist? Ms. . Within the network of critical and Critical Facility Secuconducted s with most of them. So we do have a good baseline for them in terms of where they are with regard to their corporate plans, their plans, and also, with their critical facilities in the field. So both are that we continually perform with ow and operators in the community. Mrs. OK. Well, thank you very much. Ma'am, my has expired. I yield back. Mrs. Thank you very much. The Chair recognizes Representative Miss Thank you so much. Mr. , I know that Chairman had asked you some questions about, you know, additional resources and such. I mean, it is clear that, you know, your agency has issued extensive guidance and led efforts such as the Reduce and operators of critical

threats. But we also know that, you know, the I hack demonstrates that even when companies are willing to

self-report and engage with law enforcement after a attack, they may not report to, or engage directly with I think that is one of the issues we need to address here.

prepare for

to help ow

So, is this something that, you know, is not being clear enough to ow and operators about the value added that you of their, you know, critical could bring to their ? Or is it jut that they are saying thanks, but no thanks. There is certally more that we can do to make sure that companies across sectors understand the unique value proposition, which we discussed in re-'s question, about engaging and the way that that value is unique and additive to engaging a third-party re firm, and additive to engaging with law enforcement. We worked very closely with our part in law enforcement and often conduct joint reliables, became we are achieving different mission objectives where we support a vice organization. So, certa y continuing to clarify the value proposition that brings to the table, and differentiating that and showing that it is commentary to engaging other part I, I do think is a critical area for the work for the agency.

Miss What percentage of attacks would you say get reported to So, ma'am, as noted, due to the real challenge Mr. we have here with visibility, we don't have a good number there. What I would say is after recent intraions of the same of the et cetera, we are seeing a real increase, both in organizations that are reporting incidents, and also in organizations that are availing themselves of 's guidance and best practices. As just one exam, in the week after the intraion, I think we saw increased views of our , I think, something like percent for that week after. So, we are seeing organizations across the country recognize this risk and recognizing that is a source of support and expertise. We jet need to make sure that that continues, and that we reach again into every cor of the country going forward. Miss Well, I agree with that, Mr. , but I also think it is also really important for whatever agency it is that gets contacted by an operator of a critical piece of in this country, that whether they take it to the agency we brings in **each**, and whatever other agency, need to part with to address this as comprehensively as possible. I hope that that is what the practices is—or if it isn't, will be, going forward. Ms. , just in the past few weeks, a ferry operator shut down travel between against a and its islands. It was revealed that hackers had breached the networks of on whose trains my constituents work and ride every day. Now, neither of those hacks posed a risk for passenger safety, but, you know, cyber attacks targeting mass transit, railways, aviation, they have the potential to put travelers at risk, and would be massively disruptive to society writ large. So can you, spel discuss the recent attack against the ? Yes, ma'am. As a matter of fact, I can. After that incident, I actually did speak with learn from speaking with him that the attack was not considered

to be successful. They did not actually access information in the

system. They did not make a demand for ransom. They did not acquire information from the _____. The exam___ that the would be that the intration opened the screen door, but did not get in the front door. Miss . OK. So thank you. Ms. That was the exam that they did. They did not acquire anything in that attack. Miss Thank you for that clarification. I think it is really important for to engage with and other public transit , in particular, not agencies on security measures, and j**u**t private-sector companies who are running pieces of critical **u**-I. Thank you both so much, and I yield back the balance of my Mrs. Thank you. I recognize Mr. from l ■. Thank you, Chairwoman Mr. , and Chairwoman for recognizing me and from arranging today's important hearing on cyber threats to attack on largest fuel The recent , I think many ns across these East Coast experience a rath on gas and late lines at the pump became of the collective failure to secure our critical from hackers, as we have heard e and e again today and before. I think it is fair to say that had serio security flaws, including an outdated VPN system which permitted hackers to breach systems that required dual-factor authentication. But I am also concerned that 's spotty record of engagement with , which since , has been tasked with securing our by conducting voluntary vate operators. If I can ask Assistant Admi , we may know that on multi occasions prior to the attack on May , requested assessment of 's system, but edly punted, and has yet to participate in these you ase compare 's experience with to the cooperation you received from other operators? Yes, sir. I would speak to that in that the experience we have had with is—it is for the request that they have made to reschedule, not un und during the pandemic. During the pandemic, there were a number of companies that had limited personnel on-site. They considered their personnel on-site to be essential personnel. They did restrict them from a lot of interaction with outsiders. So had postponed a discussion to get a scheduled date for their assessment. The postponement was not un ual for other companies. Other companies did go through. We did pivot, and we did manage to find virtually. So we were able to schedule a way to conduct the those in other cases. discussion was postponed became they were installing some new software. At one point, they were doing some other updates, and we had a foc in March. They had asked for about weeks to complete some cyber updates. The weeks was actually a week after the incident with . We have since focked on

getting that date in place. They are now scheduled for the last week of July for their Got it. Has a ever flat-out refleed to cooperate with an inspection or assessment, or tried to limit the scope of what you are assessing? Ms. No, it wasn't a refulal, it was rescheduling the disc sion so that they could deal with personnel issues. At one point, we had a conversation set with them, and they had several employees that were COVID-impacted. So they delayed that. . I am sorry to interrupt. I was just going to ask, Mr. is that similar in terms of others' ever having done the same thing where they have delayed? Have others refeed? Other this consistent, with the last little extra e? Ms. **We** have had other delays, but we have gotten to the point where we have done those . We had worked out a way to do them virtually, so it made this more manageable for the company, even though they were trying to protect their essential employees from engaging with outsiders. Mr. Got it. Thank you so much. Mr. , you recently witnessed a series of attacks, not just against but also against mass . Clearly, we need rob standards for the sector writ large. What additional measures can we take to protect this sector not jet from hackers, but, also, determined adversaries like Mr. Thank you, sir. The good news here is that there is nothing particularly unique about intraions. The sorts of advisories and best practices that are promulgated by and the sorts of s that we impose upon civilian agencies are effective against s, and really any adversaries. actors, In addition, as we think through the more sophisticated types of adversaries that may want to calle more lasting damage or gain more persistence, that is where a program like comes into play. Our ability to gain persistent visibility into risks affecting our most critical . By broadening and maturing that pilot program, we will be able to get more visibility and drive targeted action to drive out those risks of intr ions as soon as they are identified. Thank you. I yield back. Thank you so much, Mr. gentleman. Mrs. Thank you very much. With that, I want to thank the wit Your tes ony has been invaluable, enlightening, and thank you so much. may have additional questions The Members of the for you all, the wit , and we ask that you respond expeditio ly in writing to those questions. The Chair reminds Members that the committee's record will remain open for days. Without objection, the stands adjourned. Thank you so much. [Whereupon, at **\bigcitch** p.m., the **\bigcitch** was adjourned.]

APPENDIX

