

CYBER THREATS IN THE [REDACTED]: LESSONS FROM THE [REDACTED] RE [REDACTED] TO [REDACTED] [REDACTED] ATTACK

[REDACTED] [REDACTED]
BEFORE [REDACTED]

[REDACTED],
[REDACTED],
AND [REDACTED]

AND THE

[REDACTED]
AND [REDACTED]
[REDACTED]

OF [REDACTED]

[REDACTED]
ONE HUNDRED SEVENTEENTH [REDACTED]

FIRST SESSION

JUNE [REDACTED], [REDACTED]

Serial No. [REDACTED]-[REDACTED]

Printed for the [REDACTED]e of [REDACTED] [REDACTED] [REDACTED] [REDACTED]



Available via the World Wide Web: <http://www.govinfo.gov/>

[REDACTED] PUBLISHING OFFICE

[REDACTED] PDF

[REDACTED] : [REDACTED]

[REDACTED]

[REDACTED], [REDACTED], *Chairman*

SHEILA [REDACTED], [REDACTED]	[REDACTED], [REDACTED]
[REDACTED], [REDACTED]	[REDACTED] McCaul, [REDACTED]
[REDACTED], [REDACTED]	CLAY HIGGINS, [REDACTED]
J. LUIS CORREA, [REDACTED]	MICHAEL GUEST, [REDACTED]
ELISSA [REDACTED], [REDACTED]	DAN BISHOP, [REDACTED]
[REDACTED], [REDACTED]	[REDACTED], [REDACTED]
[REDACTED], [REDACTED]	RALPH NORMAN, [REDACTED]
[REDACTED], [REDACTED]	MARIANNETTE [REDACTED], [REDACTED]
[REDACTED], [REDACTED]	[REDACTED], [REDACTED]
DINA [REDACTED], [REDACTED]	ANDREW S. [REDACTED], [REDACTED]
[REDACTED], [REDACTED]	[REDACTED], [REDACTED]
[REDACTED], [REDACTED]	JAKE [REDACTED], [REDACTED]
VAL [REDACTED], [REDACTED]	[REDACTED], [REDACTED]
NANETTE DIAZ BARRAGÁN, [REDACTED]	KAT CAMMACK, [REDACTED]
[REDACTED], [REDACTED]	AUGUST PFLUGER, [REDACTED]
[REDACTED], [REDACTED]	[REDACTED], [REDACTED]
TOM [REDACTED], [REDACTED]	
[REDACTED], [REDACTED]	

HOPE GOINS, *Staff Director*
DANIEL [REDACTED], *Minority Staff Director*
NATALIE [REDACTED], *Clerk*

[REDACTED] [REDACTED], [REDACTED],
AND [REDACTED]

[REDACTED], [REDACTED], *Chairwoman*

SHEILA [REDACTED], [REDACTED]	[REDACTED], [REDACTED],
[REDACTED], [REDACTED]	<i>Ranking Member</i>
ELISSA [REDACTED], [REDACTED]	RALPH NORMAN, [REDACTED]
[REDACTED], [REDACTED]	[REDACTED], [REDACTED]
[REDACTED], [REDACTED]	ANDREW [REDACTED], [REDACTED]
[REDACTED], [REDACTED]	JAKE [REDACTED], [REDACTED]
[REDACTED], [REDACTED] (<i>ex officio</i>)	[REDACTED], [REDACTED] (<i>ex officio</i>)

MOIRA [REDACTED], [REDACTED] *Staff Director*
[REDACTED], [REDACTED] *Minority Staff Director*
[REDACTED], [REDACTED] *Clerk*

[REDACTED] AND [REDACTED]

[REDACTED], [REDACTED], *Chairwoman*

[REDACTED], [REDACTED]	[REDACTED], [REDACTED],
DINA [REDACTED], [REDACTED]	<i>Ranking Member</i>
[REDACTED], [REDACTED]	[REDACTED], [REDACTED]
[REDACTED], [REDACTED]	RALPH NORMAN, [REDACTED]
[REDACTED], [REDACTED] (<i>ex officio</i>)	MARIANNETTE [REDACTED], [REDACTED]
	[REDACTED], [REDACTED] (<i>ex officio</i>)

ALEX [REDACTED], [REDACTED] *Staff Director*
[REDACTED], [REDACTED] *Minority Staff Director*
ALICE HAYES, [REDACTED] *Clerk*

■ COMMENTS

The Honorable [REDACTED] [REDACTED], a Representative in [REDACTED] From [REDACTED], and Chairwoman, [REDACTED], [REDACTED], and [REDACTED]:

Oral [REDACTED]ment

Prepared [REDACTED]ment

The Honorable [REDACTED] [REDACTED], a Representative in [REDACTED] From [REDACTED], and Ranking Member, [REDACTED] [REDACTED] [REDACTED], and [REDACTED]:

Oral [REDACTED]ment

Prepared [REDACTED]ment

The Honorable [REDACTED], a Representative in [REDACTED] From [REDACTED] [REDACTED], and Chairwoman, [REDACTED] [REDACTED] [REDACTED] and [REDACTED]:

Oral [REDACTED]ment

Prepared [REDACTED]ment

The Honorable [REDACTED] [REDACTED], a Representative in [REDACTED] From the [REDACTED] of [REDACTED], and Ranking Member, [REDACTED] [REDACTED] [REDACTED] and [REDACTED]:

Oral [REDACTED]ment

Prepared [REDACTED]ment

The Honorable [REDACTED] [REDACTED], a Representative in [REDACTED] From [REDACTED], and Chairman, [REDACTED]:

Oral [REDACTED]ment

Prepared [REDACTED]ment

Ms. [REDACTED], Assistant Administrator for [REDACTED], [REDACTED]
[REDACTED]:
Oral [REDACTED] ment
Prepared [REDACTED] ment
Mr. [REDACTED], Executive Assistant Director for [REDACTED], [REDACTED]
[REDACTED] and [REDACTED] [REDACTED], [REDACTED] [REDACTED] [REDACTED]
[REDACTED]:
Oral [REDACTED] ment
Prepared [REDACTED] ment

Question From Honorable [REDACTED] for [REDACTED] [REDACTED]
 Question From Honorable [REDACTED] for [REDACTED] [REDACTED]



their compliance with ██████'s security guidance. This is an important first step, but there is clearly more that needs to be done.

We must resource and empower [REDACTED] and [REDACTED] to act boldly and swiftly to ensure operators of [REDACTED] and all other forms of [REDACTED] harden their systems. Meanwhile, it is similarly important that other agencies in [REDACTED] respect [REDACTED] and [REDACTED]'s experience and expertise on these matters. The [REDACTED] of our critical [REDACTED] is too serious for [REDACTED] to reinvent the wheel by providing duplicative authorities to [REDACTED]. [REDACTED] has the existing statutory authority and technical talent we need to tackle this challenge.

Finally, before I conclude, I must note my disappointment that the [REDACTED] declined an invitation to attend this hearing. It is critical that Members fully understand the [REDACTED]'s role and efforts in countering cyber threats, and I look forward to their participation in future events on these topics.

Mrs. ■■■■■. The Chair now recognizes the Ranking Member of ■■■■■, the gentleman from ■■■■■, for an opening ■■■■■ment.

Mr. [REDACTED]. Thank you, Chairwoman [REDACTED], Chairwoman [REDACTED], and Ranking Member [REDACTED].

I am [REDACTED]ased that the CIPI and [REDACTED] [REDACTED]s are holding this [REDACTED] today on cyber threats to [REDACTED]. As we saw with the recent [REDACTED] attack on [REDACTED], securing our [REDACTED]'s [REDACTED] million miles of [REDACTED] is of utmost importance.

I look forward to hearing today from Mr. [REDACTED] of [REDACTED] and Ms. [REDACTED] of [REDACTED] on how [REDACTED] and [REDACTED] work together to ensure [REDACTED] are secure from cyber threats. I thank the witnesses for their time today.

I am interested to hear from [REDACTED] on the [REDACTED] industry's compliance with the [REDACTED] [REDACTED] that [REDACTED] issued last month. I look forward to Ms. [REDACTED] detailing what plans [REDACTED] has for additional directives in the near future.

I am concerned with the approach to move [REDACTED] oversight from [REDACTED] and into [REDACTED]. I wholeheartedly agree that there is more that [REDACTED] can do in terms of increasing its resources and expertise, but I believe [REDACTED] or [REDACTED] is the appropriate agency to oversee [REDACTED].

█████'s close corroboration with █████ serves to ensure that there is a strong █████ effort in securing all █████ modes against cyber threats. As a committee, we need to continue to strengthen our █████'s █████ 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 discussion today of finding ways to improve security of our [REDACTED]'s [REDACTED] against continued threats of cyber attacks and, frankly, all of our [REDACTED]'s security threats and how we can protect [REDACTED] from cyber threats in the future.

Madam Chairwoman, I also share your dis[REDACTED] assure that the [REDACTED] did not participate today.

Thank you, Madam Chairwoman. I yield back the balance of my time.

The [REDACTED]ment of Ranking Member [REDACTED] follows:

OF RANKING MEMBER

Thank you, Chairwoman ██████████ ██████████, Chairwoman ██████████, and Ranking Member ██████████. I am ██████████ased that the CIPI and ██████████ ██████████s are holding

this, whether they are by organizations like DarkSide that seek to exploit [REDACTED] weak [REDACTED] for profit or foreign enemies seeking to weaken our [REDACTED]. [REDACTED] must be prepared to fight off attacks and respond to successful security breaches swiftly and effectively.

[REDACTED] is the lead [REDACTED] coordinator for securing critical [REDACTED] from cyber attacks, and [REDACTED] is the designated [REDACTED] agency for [REDACTED]. Yet [REDACTED] failed to properly engage with [REDACTED] in recent months in order to safeguard their [REDACTED] against attacks, and repeatedly rejected technical assistance from [REDACTED] following the [REDACTED] incident.

While I am assured that [REDACTED] has finally agreed to a virtual [REDACTED] assessment from [REDACTED], I am alarmed that they refused to do so until [REDACTED] weeks after an attack that resulted in the full shutdown of their [REDACTED]. Despite authority placed within [REDACTED] [REDACTED] to respond to cyber attacks on [REDACTED], including through [REDACTED]'s authority to issue emergency [REDACTED] [REDACTED]s, [REDACTED] [REDACTED] [REDACTED] was made the lead agency for re [REDACTED] to the [REDACTED].

Additionally, [REDACTED] did not deem the attack a significant cyber incident, as defined by policy, despite its substantial impact. If you don't believe me, ask those folks who were trying to find gasoline all over, everywhere, while this event was going on. It was a significant cyber event.

Cyber incident response plans have been carefully crafted to ensure proper response to incidents, and we must ensure they are followed appropriately. The attacks on [REDACTED] and others provide opportunities to learn and improve the resiliency of the [REDACTED] sector and critical [REDACTED] across [REDACTED].

I was [REDACTED]ased to see [REDACTED] take initial action by issuing the first-ever mandatory [REDACTED] requirements for [REDACTED]. These new requirements went into effect on May [REDACTED] and will be critical to improving coordi[REDACTED] am[REDACTED] the [REDACTED] ind[REDACTED]stry, [REDACTED], and [REDACTED].

More must be done to increase [REDACTED]s for our [REDACTED] and allow [REDACTED] authorities greater ability to assess weak [REDACTED] in critical [REDACTED] [REDACTED]. Unfortunately, cyber criminals are not going anywhere any [REDACTED]e soon. In fact, they are getting smarter, and cyber attacks are likely to become more common. We must ensure [REDACTED] remains at the forefront of protecting our critical [REDACTED] from these threats.

I look forward to our testimony. I yield back, Madam Chair.

[The [REDACTED]ment of Chairman [REDACTED] follows [REDACTED]

█████ works with industry partners to assess and mitigate vulnerabilities, and improve security through collaborative efforts including intelligence briefings, █████, █████, and on-site █████s. Through the Intermodal Security Training and █████, █████ provides █████, trainings, and security planning tools to the █████ community to strengthen company security plans, policies, and procedures. Working with █████ operators' security personnel, █████ conducts █████, █████, which assess the degree to which the █████' physical and █████ measures are integrated into the operator's corporate security plan.

On behalf of [REDACTED], [REDACTED] serves as the co-[REDACTED] [REDACTED] agency al[REDACTED] side [REDACTED] and [REDACTED] for the [REDACTED] [REDACTED] and is responsible for developing, deploying, and promoting [REDACTED] [REDACTED]-foc[REDACTED]ed [REDACTED] initiatives, programs, assessment tools, strategies, and threat and intelligence information sharing products that support the im[REDACTED]plementation of [REDACTED]s [REDACTED]. [REDACTED] is in close alignment with [REDACTED] and coordinates on both a tactical and strategic level to raise the [REDACTED] baseline across the [REDACTED] sector. As noted earlier, [REDACTED] participates in [REDACTED] [REDACTED] and regularly collaborates with [REDACTED] and its [REDACTED] on programmatic issues affecting the [REDACTED] of [REDACTED] systems.

█████ supports █████'s ██████ efforts in alignment with the █████ ██████-█████ 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. █████ works closely with the ██████ ind-█████ try to identify and reduce ██████ vul-█████ abilities, including facilitating classified briefings to increase ind-█████ try's awareness of cyber threats.

In response to the recent [REDACTED] cyber intrusion, [REDACTED] is using its statutory authority to strengthen the [REDACTED] and resilience of [REDACTED] owners and operators. The first [REDACTED] issued following the recent incident requires [REDACTED] owners and operators of critical hazardous liquid and natural gas pipelines or a liquefied natural gas facility designate a [REDACTED] coordinator; report [REDACTED] incidents to [REDACTED]; and assess their current [REDACTED] posture against a specific set of measures within [REDACTED]. As part of this assessment, the owners/operators must identify any gaps, develop a remediation plan if necessary, and report the results to [REDACTED].

All information reported to █████ pursuant to this directive is shared with █████ and other █████ agencies as appropriate. Similarly, all information provided to █████ is shared with █████. By requiring the reporting of █████ incidents, █████ is better positioned to understand the changing threat of cyber events and the current and evolving risks to █████. The design █████ of █████ coordinators will give █████ a known and consistent point of contact with critical █████ ow █████ and operators, allowing █████ to easily share security information and intelligence. The █████ will assist the ow █████ and operators and █████ to better understand the current █████ of █████ practices in individual companies and across the industry. In addition, █████, in close coordination with the █████ and █████, is also exploring ways in which immediate threats, such as █████, can be mitigated through additional █████ measures to ensure

██████████, and the broader ██████████, has acted urgently to catalyze ██████████ action around this risk. In January ██████████, ██████████ unveiled the Reduce ██████████ ██████████ ██████████ to raise awareness and combat this ongoing and evolving threat. The campaign is a focused, coordinated, and sustained effort to encourage public and private-sector organizations to implement best practices, tools, and resources that mitigate ██████████ risk. Additionally, in coordination with ██████████ ██████████ ██████████ ██████████ ██████████ (ISAC), ██████████ released a joint ██████████ ██████████ that details industry best practices and a reusable checklist that can serve as a ██████████-specific addendum to ██████████ and local ██████████'s cyber incident response plans.

In February, during his first remarks dedicated to [REDACTED], Secretary [REDACTED] issued a call for action to tackle [REDACTED] more effectively. To further drive a call to action, Secretary [REDACTED] initiated a [REDACTED] in April [REDACTED] that has included a series of high-profile [REDACTED] events intended to ensure that leaders across all sectors of the economy understand the criticality of this risk and take urgent action to re[REDACTED].

██████████ is a critical challenge and the risks posed to our ██████████'s critical ██████████ are severe. But the challenge is not insurmountable. ██████████ intrusions generally do not ███ zero-day vulnerabilities or exquisite tradecraft, but rather exploit known security weaknesses or a failure to adopt generally accepted best practices. By investing in improved ██████████ as recommended in ██████████ guidance, organizations can reduce the risk of a ██████████ intrusion and limit the potential impacts.

AN EXAMINATION OF A BROADER RISK: INTRUSION

The [REDACTED] that impacted [REDACTED] was one of the first cyber intrusions in our [REDACTED] to have a direct effect on many [REDACTED]s' daily lives. But the intrusion itself was not unique: The Darkside [REDACTED]-as-a-service group has been associated with hundreds of intrusions in recent months and [REDACTED] intrusions have impacted essential services on a smaller scale, from elementary schools to hospitals. Upon learning of the intrusion, [REDACTED] immediately began to collaborate with [REDACTED] ([REDACTED]) and other interagency partners [REDACTED] to gather information that could be [REDACTED] to help protect other potential victims. Within [REDACTED] days of the intrusion, [REDACTED] and the [REDACTED] published a [REDACTED] advisory on the incident, which included detailed information on how to reduce risk across critical [REDACTED]. This advisory contained specific mitigation measures to reduce the likelihood of a [REDACTED] intrusion and, critically, steps to reduce the consequences. This latter element cannot be over[REDACTED]: All critical [REDACTED]-[REDACTED] organizations should assume that they can be compromised by a [REDACTED] intrusion and take steps to reduce impacts, including by ensuring that their essential functions can remain operable even if their primary business network is unavailable. [REDACTED] and the [REDACTED] subsequently enriched this advisory with specific indicators of compromise associated with the Darkside [REDACTED] group and [REDACTED]-[REDACTED] intrusion.

In order to further amplify the importance of these mitigation steps, [REDACTED] convened a broad stakeholder call with over [REDACTED] attendees from across [REDACTED] critical [REDACTED] to provide an overview of the incident, threat actor, and impact. [REDACTED] also convened a meeting under its Critical [REDACTED] Part [REDACTED] Partnership Advisory Council with leadership from the [REDACTED] critical [REDACTED] sectors to discuss potential operational impacts for critical [REDACTED] due to the [REDACTED] intrusion. This contributed to [REDACTED]'s ability to assess potential impact to the [REDACTED] [REDACTED] [REDACTED] from a sustained shutdown, and anticipate cross-sectoral impacts, including from [REDACTED] slow-downs and impacts to chemical facilities. Finally, [REDACTED] leveraged our regional personnel deployed across the country, and particularly in areas impacted by [REDACTED] [REDACTED] outage, to provide focused guidance to other critical [REDACTED] organizations and provide [REDACTED] [REDACTED] with detailed information on cascading impacts across sectors.

MANAGING A BROADER RISK: [REDACTED]'S ROLE IN [REDACTED]

Well before ██████████ intrusion, ██████████ was addressing ██████████ risks to ██████████. Over the past several years, ██████████ and the ██████████ ██████████ (██████████), in conjunction with ██████████, ██████████ Laboratories, and private industry, have been focused on addressing ██████████ risks to the ██████████'s 1.1 million miles of ██████████ through ██████████ ██████████ (██████████). The ██████████ was formed in response to increasing dependence on automation within the oil and natural gas (██████████) ██████████ industry and the growing attack surfaces of assets ██████████ connected technology.

██████████, somebody ██████'s sabotage, et cetera. Those are things that we need to protect, and ██████ needs to do that.

But in terms of ████████████████████, is there really a difference between the control systems for the computer network, the thing that is going to be hacked, for a ██████████ and, say, an airport or a bank or any such thing? Isn't ████████████████████ really attacking the computer systems themselves and it really ██████'s not matter what industry that computer system is controlling?

Mr. ██████████. Sir, thank you for that question. I think there are █ ways to answer 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, ██████████, hospitality, across the board—which is why ██████ has been so focused on promulgating these cross-cutting best practices and guidance, including our advisory promulgated after the ██████████ intrusion, that is equally applicable to any organization because, as you imply, these sorts of ████████████████████ best practices are generalizable across sectors.

Now, it is also the case that different sectors may have different specific technologies. They may have different network architectures or different ways to have devices 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 using multifactor authentication, leveraging off-line backups—those are practices that are generalizable 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 ██████████, you 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 ████████████████████?

Mr. ██████████. So, in general, ██████ puts out guidance and best practices, and in the case of ██████████ agencies, directives that are generally applicable. Occasionally, we will put out guidance that is specific to control systems, or certainly if we know about a given threat or incident that is affecting a particular sector, we may produce a targeted alert or warning focused 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, generally regulators, including ██████, may seek ██████'s expert advice and consultation on 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 generally 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 ██████ is 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 electricity, the ██████████, banks, is coming out of the computer, and the computers are being hacked, and that is where vulnerability lies.

5

Mrs. ██████. Thank you. We will now recognize Representative ██████ for 1 minutes. Thank you.

So the recent [REDACTED] [REDACTED] [REDACTED] attack was, obviously, not the first we have seen against critical [REDACTED], but 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 example, the Hampton Road Sanitation district suffered a [REDACTED] attack last November that disrupted billing across the service region for several weeks.

So I wanted to ask the question of our witness today. With regards to our critical [REDACTED] owners and operators, such as those that operate [REDACTED], what evidence do you and other agencies have that the organizations you oversee actually understand the extent of their [REDACTED] risk?

We also work with our [REDACTED] and operators to conduct [REDACTED], so 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

An[REDACTED]. Re[REDACTED] was not received at the [REDACTED] of publication.

An [REDACTED]. Re [REDACTED] was not received at the [REDACTED] of publication.

