SALT TYPHOON: SECURING AMERICA'S TELECOMMUNICATIONS FROM STATE-SPONSORED CYBER ATTACKS

HEARING

BEFORE THE

SUBCOMMITTEE ON MILITARY AND FOREIGN AFFAIRS

OF THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED NINETEENTH CONGRESS

FIRST SESSION

APRIL 2, 2025

Serial No. 119–17

Printed for the use of the Committee on Oversight and Government Reform

Available on: *govinfo.gov*
oversight.house.gov or
docs.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE
60–026 PDF WASHINGTON : 2025

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

JAMES COMER, Kentucky, Chairman

JIM JORDAN, Ohio
MIKE TURNER, Ohio
PAUL GOSAR, Arizona
VIRGINIA FOXX, North Carolina
GLENN GROTHMAN, Wisconsin
MICHAEL CLOUD, Texas
GARY PALMER, Alabama
CLAY HIGGINS, Louisiana
PETE SESSIONS, Texas
ANDY BIGGS, Arizona
NANCY MACE, South Carolina
PAT FALLON, Texas
BYRON DONALDS, Florida
SCOTT PERRY, Pennsylvania
WILLIAM TIMMONS, South Carolina
TIM BURCHETT, Tennessee
MARJORIE TAYLOR GREENE, Georgia
LAUREN BOEBERT, Colorado
ANNA PAULINA LUNA, Florida
NICK LANGWORTHY, New York
ERIC BURLISON, Missouri
ELI CRANE, Arizona
BRIAN JACK, Georgia
JOHN MCGUIRE, Virginia
BRANDON GILL, Texas

GERALD E. CONNOLLY, Virginia, *Ranking Minority Member*
ELEANOR HOLMES NORTON, District of Columbia
STEPHEN F. LYNCH, Massachusetts
RAJA KRISHNAMOORTHI, Illinois
RO KHANNA, California
KWEISI MFUME, Maryland
SHONTEL BROWN, Ohio
MELANIE STANSBURY, New Mexico
ROBERT GARCIA, California
MAXWELL FROST, Florida
SUMMER LEE, Pennsylvania
GREG CASAR, Texas
JASMINE CROCKETT, Texas
EMILY RANDALL, Washington
SUHAS SUBRAMANYAM, Virginia
YASSAMIN ANSARI, Arizona
WESLEY BELL, Missouri
LATEEFAH SIMON, California
DAVE MIN, California
AYANNA PRESSLEY, Massachusetts
RASHIDA TLAIB, Michigan

MARK MARIN, Staff Director
JAMES RUST, Deputy Staff Director
MITCH BENZINE, General Counsel
KAITY WOLFE, Deputy Director for Oversight
GRAYSON WESTMORELAND, Senior Professional Staff Member
MALLORY COGAR, Deputy Director of Operations and Chief Clerk

CONTACT NUMBER: 202-225-5074

JAMIE SMITH, Minority Staff Director
CONTACT NUMBER: 202-225-5051

SUBCOMMITTEE ON MILITARY AND FOREIGN AFFAIRS

WILLIAM TIMMONS, South Carolina, Chairman

MICHAEL TURNER, Ohio
MICHAEL CLOUD, Texas
ANDY BIGGS, Arizona
BYRON DONALDS, Florida
ANNA PAULINA LUNA, Florida
ELI CRANE, Arizona
JOHN MCGUIRE, Virginia

SUHAS SUBRAMANYAM, Virginia *Ranking Member*
STEPHEN LYNCH, Massachusetts
KWEISI MFUME, Maryland
ROBERT GARCIA, California
GREG CASAR, Texas
Vacancy

C O N T E N T S

WITNESSES

Written opening statements and bios are available on the U.S. House of Representatives Document Repository at: docs.house.gov.

INDEX OF DOCUMENTS

Documents are available at: docs.house.gov.

ADDITIONAL DOCUMENTS

These documents were submitted after the hearing, and may be available upon request.

SALT TYPHOON: SECURING AMERICA'S TELECOMMUNICATIONS FROM STATE–SPONSORED CYBER ATTACKS

Wednesday, April 2, 2025

U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
SUBCOMMITTEE ON MILITARY AND FOREIGN AFFAIRS
Washington, D.C.

The Subcommittee met, pursuant to notice, at 10:01 a.m., in room HVC–210, U.S. Capitol Visitor Center, Hon. William Timmons [Chairman of the Subcommittee] presiding.

Present: Representatives Timmons, Cloud, Biggs, Crane, McGuire, Subramanyam, Lynch, and Garcia.

Mr. TIMMONS. This hearing of the Subcommittee on Military and Foreign Affairs will come to order. I want to welcome everyone.

Without objection, the Chair may declare a recess at any time.

I recognize myself for the purpose of making an opening statement.

Good morning. Thank you for joining us today as we confront one of the most pressing national security challenges of our time: cyber espionage by adversaries targeting our critical infrastructure.

I would like to thank our witnesses for being here today and look forward to our conversation.

In recent months, sophisticated cyber-attacks by groups like Salt Typhoon have not only compromised networks used by millions of Americans but have threatened the backbone of our national security. Our Nation's critical infrastructure is under attack at a staggering pace.

Reports indicate that, globally, cyber-attacks against critical infrastructure increased by 30 percent last year, averaging 13 attacks per second. In the United States alone, over 420 million cyber-attacks were recorded in just the last year.

These incidents are not random errors. They are part of a coordinated campaign by a well-funded foreign adversary that exploits vulnerabilities. Salt Typhoon, a Chinese state-sponsored hacking group with direct ties to the CCP's intelligence apparatus, executed an extensive breach that compromised U.S. telecommunication networks.

This campaign targeted essential communication networks, including those operated by industry giants like Verizon and AT&T.

They were able to intercept real-time calls and messaging data from over a million users. Critically, these attacks focused on gathering intelligence from high-value government and political figures.

It is vital to emphasize these telecommunication companies are not at fault. They are on the defensive against an enemy that employs sophisticated tactics using vulnerabilities and sometimes outdated infrastructure and exploiting weak points in network management systems to gain unprecedented access to our critical communications.

This is not a failure of the private sector. It is a clear signal that our Nation must take a more proactive approach. The damage control posture of the previous Administration has left us vulnerable to these state-sponsored cyber-attacks. Instead of merely reacting after breaches occur, we must be forward-thinking and resolute.

National security is paramount, and it is our government's responsibility to safeguard the American people and the critical infrastructure that we rely on every day. Now more than ever, it is imperative for Congress and Federal agencies to join forces with the private sector in establishing a robust, unified cybersecurity strategy.

Legislators have begun proposing measures to require annual cybersecurity certifications for telecom companies, ensuring they adhere to strict security protocols. Yet this is only part of the solution. We must also invest in a more aggressive offensive capability that deters adversaries from exploiting our vulnerabilities, sending a clear message that cyber espionage against American infrastructure will have severe consequences.

Furthermore, the sheer volume of these attacks should serve as a wake-up call for strengthening our critical infrastructure. When our communication systems, integral to our national defense, emergency services, and economic vitality, are compromised, it erodes public trust and jeopardizes our collective safety.

It is our duty to ensure that our government agencies, in collaboration with private industry, take decisive action to upgrade cybersecurity measures and hold foreign state actors accountable.

In closing, let me reiterate: The threat we face is not a result of negligence from our telecom companies but a deliberate, strategic maneuver by sophisticated and hostile state actors intent on undermining our national sovereignty. This is a call to action for every American who values freedom and security.

We must fortify our defenses, invest in advanced cybersecurity technology, and pursue strong, proactive policies that secure our Nation's critical infrastructure against these relentless threats.

The time to act is now, before our adversaries turn these vulnerabilities into tools for even more severe, real-world disruption.

Thank you again to our witnesses for being here today, and I look forward to hearing about your experiences in the cybersecurity field and any recommendations you have regarding our strategic cyber posture.

With that, I yield to Ranking Member Subramanyam for his opening statement.

Mr. SUBRAMANYAM. Thank you, Chairman Timmons. Thank you for holding this hearing.

And I agree with much of what you said. You know, we must protect our telecommunication infrastructure from our adversaries, foreign and domestic.

And the future of warfare is here now, and programs like Salt Typhoon are actively infiltrating our networks and gaining access to sensitive information and credentials.

And I would say Salt Typhoon is one of the worst breaches our country has ever faced in our telecom infrastructure, and we are still uncovering the full breadth and scope of its attacks. And this work to protect our telecom infrastructure is urgent, and it is bipartisan, and it must be a national priority.

And so, it is deeply troubling that, in the midst of this massive cybersecurity espionage effort we are facing, our National Security Advisors are breaking basic protocols that ought to be followed by every person handling sensitive and classified information.

As we saw last week, our National Security Advisor added a journalist to a Signal group chat where top officials shared classified information about an upcoming strike. The Administration has not taken responsibility and tried to deflect, saying that it is not a big deal, and the mission was a success.

But this is a big deal, and the mission is not a success if the whole world now knows how we did it, how we planned these attacks, and where we got the information. We have made it much harder and more dangerous for our troops to carry out these missions in the future.

The Administration also keeps saying that the information discussed was not classified. But, if our war plans right before a strike are not classified, I would like a thorough review of our classification system. But I am pretty sure it was classified. And, either way, it was highly sensitive information that put our troops at risk and the American people at risk.

It also told us who and what we were targeting. So, if you look at these texts here, it says that they identified a target walking into an apartment building. Those texts revealed where we received our intelligence as well. It came from our Israeli allies, who are now furious that this source has been leaked.

And our allies are already hesitant to share information with us and this Administration, and now the Administration has proven that our current national security leaders cannot be trusted to keep sensitive information safe. They will just take our classified information and text it to whomever shows up in their contact list.

The timing of when the planes were taking off, what kinds of planes were being used, and how we generally plan and conduct strikes like this were also shared in the chat. Again, all of this information was sent around using a private, third-party app on private phones that we know are targets of Salt Typhoon and other adversaries.

So, if the objective of this mission was to lose the trust of all of our allies, well, then the mission was a success.

The Administration says that accidents happen, but an accident is when you text gossip to your boss instead of your work bestie. Leaking sensitive military strike information to a journalist is not an accident. This is incompetence that puts our lives in danger.

We need to hold our government leaders to a very high standard. And, just 2 days ago, the White House said, and I quote, "Case closed." But I disagree. And some others on the Senate side, including Republicans, agree with that, that we have to continue to ask questions about this. And I think the American people want answers.

How prevalent is their use of Signal? And will we find out whether other information has been leaked? Are our phones, private phones of these National Security Advisors, being hacked by Russia, Iran, or China? Have any of these devices already been compromised?

It is pretty clear that we got lucky in figuring out that this is happening because of the added journalist, and it is pretty clear that our national security leaders are using Signal all the time for communications like this.

And so, I hope my colleagues on both sides of the aisle today will join me in trying to provide real accountability and oversight over these actions.

We are here to talk about the risk of state-sponsored cyber-attacks. Let us confront this most urgent vulnerability and work together to investigate this massive security leak. This is an issue of national security and the safety of every American.

Thank you. And I yield back.

Mr. TIMMONS. Thank you.

I am pleased to welcome an expert panel of witnesses for today's discussion. I would first like to welcome Mr. Josh Steinman. He is the CEO of Galvanick, a cybersecurity startup that focuses on protecting critical infrastructure.

Mr. Steinman also served as a Senior Director of Cyber Policy and Deputy Assistant to President Trump from 2017 to 2021.

Second, I would like to welcome Dr. Edward Amoroso, who is the CEO of TAG Infosphere and professor at NYU.

Formerly, he was a Senior Vice President and Chief Information Security Officer at AT&T and has decades of experience as a leader in cybersecurity.

Last, I want to welcome Professor Matt Blaze of Georgetown Law, where he focuses on security and privacy in computing and communication systems.

Thank you. I now——

I am going to swear you all in first.

Pursuant to Committee Rule 9(g), the witnesses will please stand and raise their right hand.

Do you solemnly swear or affirm that the testimony that you are about to give is the truth, the whole truth, and nothing but the truth, so help you God?

[Chorus of ayes.]

Mr. TIMMONS. Let the record show that the witnesses answered in the affirmative.

Thank you. Please take your seat.

I now recognize Mr. Steinman for his opening statement.

STATEMENT OF JOSH STEINMAN
CEO
GALVANICK

Mr. STEINMAN. Thank you, Mr. Chairman and the Ranking Member and all Members here for having us here today.

My name is Joshua Steinman. I am the CEO of Galvanick. We are a critical infrastructure cybersecurity company. I previously served in the White House as a senior National Security Council staffer.

I have a simple message today, and that echoes some of the messaging that we have already heard, which is that cyber threats to critical infrastructure are not contained to the telecommunications industry. It is an endemic problem across any number of other critical infrastructure sectors. Those include transportation, water, power, sewer, and the defense industrial base.

Executive branch leaders have, for years, in open testimony here in Congress, talked about the threats from both Russia, China, Iran, North Korea, and others to our critical infrastructure sectors, and now is the time for Congress to take action in concert with the executive branch, in concert with the new Trump Administration to finally get us on a footing to be able to defend these critical aspects of American life against foreign cyber actors.

Thank you both for having me, and all Members. Thank you.

Mr. TIMMONS. Thank you.

I now recognize Dr. Amoroso for his opening statement.

STATEMENT OF EDWARD AMOROSO
CEO, TAG INFOSPHERE, INC.
RESEARCH PROFESSOR, NEW YORK UNIVERSITY

Dr. AMOROSO. Well, thank you. Thanks for the invite, and I am looking forward to our discussion today.

I do a few things. I run a research and advisory company called TAG in New York City. It allows me to kind of keep up on an awful lot of current issues in cyber. I advise enterprise, government, and so on.

I also teach at NYU in the Computer Science and Engineering Department. And I also have the privilege to try to teach cybersecurity to law students, which can be quite a challenge at times, but it is something I enjoy very much.

But I am, perhaps, most known in this industry as someone who has spent 31 years at AT&T. So, I have spent a lifetime protecting critical infrastructure. And, the last 20 years of my career at AT&T, I was in the top job there.

So, a lot of the systems and infrastructure and tools that are likely to be referenced, perhaps in some of your questions today related to Salt Typhoon, I helped to design and build and put teams in place to operate. So, I really do understand how much of this works.

I stepped down from that role several years ago. So, I am happy to, hopefully, provide some insight there.

One of the themes I think you will hear in my comments today, is that we need to be thinking about the next problem. I think a metaphor comes to mind that I often think about when asked about

this topic. It is as if we were driving on a road, hitting a bunch of potholes, and then you ask us to come and talk about the potholes.

We do not want to ignore the potholes, but it is scarier when there are gigantic sinkholes ahead of us. And I think that is the metaphor that makes the most sense here. And those sinkholes will come from an adversary that is increasingly using AI.

And I think, again, you will hear in my comments that, unless we figure out a way to deal with that at a national level, in a coordinated way—and, yes, telecom is a big piece of that, but there is a lot of other pieces—unless we do that, then I think we will look back on Salt Typhoon as, perhaps, child's play.

So, I look forward to our discussion, and I hope my insights today are helpful to you.

Mr. TIMMONS. Thank you for that.

I now recognize Professor Blaze for his opening statement.

STATEMENT OF MATT BLAZE
MCDEVITT CHAIR IN COMPUTER SCIENCE AND LAW
GEORGETOWN UNIVERSITY

Dr. BLAZE. Thank you, Mr. Chairman.

I apologize that I will probably use my 5 minutes fully, unlike my co-witnesses here.

So, although I am in the law school, as well as the Computer Science Department, I am here primarily with my technologist hat on. And I thought I would spend a few minutes just discussing the technical context in which Salt Typhoon was able to happen, and I traced this back to 1994.

In 1994, Congress enacted something called the Communications Assistance for Law Enforcement Act, or CALEA, which mandated that telecommunication service providers incorporate into their infrastructure capabilities to support court-authorized wiretaps, sometimes called lawful access.

CALEA was a response to concerns from law enforcement that newer digital telephony services might not be compatible with existing, at the time, wiretap technology that the government and the police were using.

What CALEA did, was shifted the technical burden for implementing wiretaps from law enforcement, where it had traditionally been for most of the 20th century, into the communications network itself. And what CALEA required was that virtually all switching equipment in the public telephone network must be designed with explicit backdoor capabilities to wiretap traffic.

So, every switch used to serve every consumer would thereafter have to be essentially wiretap ready in case a customer served by that equipment might someday be the subject of a wiretap order.

When CALEA was proposed, many technologists, myself included, raised concerns about the security implications of such a sweeping mandate, that it would expose our infrastructure to attack by malicious actors who would find ways to exploit these new universal wiretap capabilities against ordinary Americans and American companies and government officials.

And, unfortunately, these concerns have over time been proven correct several times and most recently and most spectacularly in

the Salt Typhoon attacks against high-value U.S. targets, including government officials.

While the CALEA mandates introduced vulnerabilities from the beginning, those risks have been greatly amplified in practice over the more than 30 years since the law was passed and are now much more severe than, perhaps, they were at the start.

Telecom infrastructure has changed radically over the last 30 years. In particular, it has become increasingly automated and virtualized. In the previous century, provisioning wiretaps generally required the intervention of a technician with physical access to switching equipment that was serving the targeted customer.

This effectively served as a safeguard against very largescale, unauthorized wiretapping that was not being permitted by court orders because a human being was in the loop and would be expected to notice an inexplicable uptick in surveillance.

Over time, these sort of architectural safeguards, because of the way the phone system worked in the 1990s, have kind of fallen by the wayside as communication infrastructure has evolved. Telecom switches are now more like data centers than they were specialized offices run by humans.

They are designed to be remotely programmed, configured, and managed, often over the internet, and at the same time, the back hall for wiretaps to law enforcement is no longer through dedicated leased lines but, rather, through internet connections that anyone potentially could get access to.

And there are now intermediaries that serve essentially as wiretapping clearinghouses between law enforcement and telecom providers.

Effectively, all of this has expanded the attack surface that has to be defended to prevent tampering with our communications infrastructure and unauthorized surveillance by foreign state actors, especially at scale.

The job of the illegal eavesdropper has actually gotten significantly easier, and, to put it bluntly, something like Salt Typhoon was inevitable and will likely happen again unless significant changes are made to our infrastructure and our approach to protecting it.

Thank you.

Mr. TIMMONS. Thank you for that.

I now recognize myself for 5 minutes for questions.

Mr. Steinman, it is widely reported that U.S. critical infrastructure undergoes thousands of cyber-attacks a day. While many of these attacks are not successful, it is impossible to stop all of them from achieving their goal.

To begin, can you quickly describe the significance of the Salt Typhoon breach last year and its impact on U.S. national security?

Mr. STEINMAN. Yes. Thank you, Mr. Chairman.

I would first want to ask for clarification, which I fear you may not be able to provide, in terms of the language that we use here.

So, this is a challenge that we have faced for many years. I faced it in my last job. I even face it in my current job, which is that, when folks say "attack," I think often they refer to activity such as probing or other things that I think do not bear the same weight that the word "attack" actually does.

This also goes to another challenge in cyber space, which is that, you know, many actors conduct activities that look like both intelligence collection, and then they maintain the capacity to then conduct an operation that may have an impact. That impact may be digital. That impact, especially in this context, may be physical.

Mr. TIMMONS. So, would it be fair to say that, instead of using "attack," you would prefer to use words like "probing," "monitoring," "collecting," "disrupting"?

Mr. STEINMAN. I would defer to my academic colleagues here to choose the specific language. I would just caution against using the word "attack."

Mr. TIMMONS. Sure.

Mr. STEINMAN. Because I will certainly use that word very specifically to mean creating direct impact.

Mr. TIMMONS. Disruptions.

Mr. STEINMAN. Yes, sir.

Mr. TIMMONS. OK. All right. I appreciate that.

Mr. STEINMAN. So, in that case, I think, just to answer your question, we do see critical infrastructure bearing an intense degree of scrutiny, I guess, from foreign actors. Those foreign actors are reported—and, again, you can consult the Director of National Intelligence's Annual Threat Assessment to Congress, which recites these types of frameworks a lot.

But we see foreign threat actors deliberately, repeatedly, regularly in high volume interrogating critical infrastructure facilities across the United States, across the world. The challenge is that many of those critical infrastructure facilities, in fact, are not well defended. We could go into the reason why.

I think, in closing, what I would say, Mr. Chairman, is the internet is a dark and dangerous place. It can be certainly. And our adversaries take advantage of the fact that we have essentially built out America's critical infrastructure from a digital perspective without a sort of wartime footing.

And that means that these types of activities in many cases are purported to have found purchase. And what that means is that we do have foreign adversaries sitting on American critical infrastructure, and that gives them the possibility of being able to, at a time and place of their choosing, conduct an attack.

Mr. TIMMONS. Sure. Thank you for that.

I thought that our—I will call it our 9–11 because that is when we kind of woke up when we were attacked. I thought our 9–11 was going to be the colonial pipeline attack, and we were days away from catastrophe, and we have allowed our critical infrastructure to be basically operated by technology, and that technology has vulnerabilities.

And it is funny because I was in Congress during the colonial pipeline attack, and they had to call all of these 70-and 80-year-old retirees from all over the country to operate the pipeline with wrenches. And these guys knew how to hit it and know what to do next. And, you know, IOT was operating the whole thing.

Luckily, they were able to determine that the administration was actually what was the breach, as opposed to the operational control. So, they were able to turn it back on.

But, you know, Dr. Amoroso, when these types of state-sponsored attacks—and I guess, you know, Salt Typhoon is state-sponsored. The colonial pipeline attack was likely somebody that was just trying to make some money.

But do you believe that the U.S. Government should retaliate against either state-sponsored actors or actors that are operating in countries that are not enforcing the rule of law to show that there is consequences for these kind of behaviors?

And, if so, what kind of response do you believe is justified?

Dr. AMOROSO. Well, it is a good question. It comes up all the time, the last 30 years. Should we say the best defense is a good offense, right? That comes up a lot.

I think the best defense is a good defense. You have got to play defense. I mean, whether we decide to retaliate is sort of a separate issue, but I think it shirks the responsibility we have to do a better job, right.

There is no question that Salt Typhoon—I feel like we are sort of lucky in a sense, right, because we break down problems into two types of things. Ones where they are peeking at your stuff, and that is never good. You know, you do not want anybody surveilling and pulling data. But somehow you feel like you survived that. It is not good.

But, if they are disrupting, if there is kinetic attacks where buildings have to be evacuated and people's lives are maybe taken, I mean, that is a whole other thing.

So, in my opening comment, when I sort of drew the analogy between sort of potholes and sinkholes, sinkholes are consequential attacks where you cannot ignore what is going on, and that is my biggest fear, that I feel like we are headed toward that.

And now is a good time, I think, for our whole country, for everybody to kind of wake up and say, "This is something we should pull together and fix," something where—you know, in America, we are good at that. When we get pissed at something, we do pull together.

And this is a really good opportunity, not just for this Committee but I think for our whole country to do something about it.

Mr. TIMMONS. Thank you for that.

I just want to let my colleagues know that we are not going to be super strict on time, given the fact that some of us have left, and we want to make sure that we get the most out of this. And we will likely be doing a second round of questions at the end.

Thank you for that.

And, with that, I now recognize the gentleman from Virginia, Mr. Subramanyam, for 5 minutes.

Mr. SUBRAMANYAM. Mr. Chair, I want to enter into the record congressional testimony: "Salt Typhoon: Securing America's Telecommunication Information from State-Sponsored Cyber Attacks," April 2, by Corey Simpson, J.D.

Mr. TIMMONS. Without objection, so ordered.

Mr. SUBRAMANYAM. Thank you, Mr. Chair.

So, the Administration has said that discussing attack plans on Signal was not a big deal because Signal is end-to-end encrypted.

But what does that really mean? I just want to explain to people at home exactly how this encryption works and how a phone works,

really. So, end-to-end encryption means that, after I press the send button on my phone, my message gets scrambled if you are using Signal, and that scrambled version travels to its end destination.

Anyone who reads the message in the middle would not know what I said. But what if the hackers are not trying to intercept my message while it is moving? What if they had already hacked the phone itself or hacked my friend's phone who I am sending the message to?

So, let us take a closer look at how a phone works. And you can see here there is a lot of ways a phone can get hacked.

And, Dr. Blaze, this is your area of expertise. Yes or no, is it true that hackers can access information on your phone if you are connected to public Wi-Fi?

Dr. BLAZE. Under many circumstances, yes, with personal devices.

Mr. SUBRAMANYAM. And then can they access your phone and the messages you are sending through a Bluetooth connection or even a USB port, let us say?

Dr. BLAZE. All of those expose the phone to vulnerabilities.

Mr. SUBRAMANYAM. And isn't it true that if I accidently click on, let us say, a malicious ad or link, that could download something on my phone that could also make my messages or what I am doing on my phone vulnerable?

Dr. BLAZE. That is actually a very common way of attacking phones.

Mr. SUBRAMANYAM. So, even if you are using and end-to-end encrypted app like Signal, there are so many ways to hack your phone itself that America's top national security officials should know this, and they are probably the No. 1 target for many of these types of hacks.

And it is actually hard to believe that they would even be using Signal. There is a reason why we do not put secure information and classified information on Signal in the first place.

And, just yesterday, we found out that Mike Waltz' team uses Gmail to communicate as well.

Mr. Blaze, is Gmail vulnerable as well if you are sending information, classified or sensitive information, to and from people? I would say it is probably more vulnerable than Signal, correct?

Dr. BLAZE. That is right.

Well, Gmail is not even end-to-end encrypted. So, it is vulnerable to attacks on both the device and the network itself and Google's infrastructure.

Mr. SUBRAMANYAM. And has Gmail been infiltrated in the past over national security information?

Dr. BLAZE. Yes.

Mr. SUBRAMANYAM. And can you tell me, do you remember any instances of that?

Dr. BLAZE. I mean, there are many, many ways to attack a Gmail user. The most common is to obtain their passwords or other access control, and, you know, essentially login as them with full access. And this happens so often that it is almost impossible to single out a single instance.

But, you know, state actors are notorious for this sort of attack.

Mr. SUBRAMANYAM. And I think it is pretty clear that this should not have been happening. And, if any regular, low-level defense or intelligence staff had been involved in anything like this, they would have been fired immediately, and that is what really is concerning to me.

Now, speaking of firings, we have actually been laying off a lot of our top cybersecurity experts at CISA and across the government. Dr. Blaze, what do you think would be the impact of some of these firings on our ability to defend against hostile cyber-attacks in the future?

Dr. BLAZE. Well, you know, the battle to defend our infrastructure is fundamentally difficult. It is fundamentally a problem that the offense side has an advantage with because computer systems, personal devices, the servers that serve them are all vulnerable to attacks, some of which have not yet been discovered and some of which have not yet even come into existence.

But we do not know how to build secure systems in any top-to-bottom way. So, I would say that, you know, having an active defense to identify and fix vulnerabilities from all sectors, from the private sector, government, and individual end users, is essential.

Mr. SUBRAMANYAM. And, Mr. Chairman, I ask for unanimous consent to enter into the record an article dated March 13, 2025: "People are scared inside CISA as it reels from Trump's purge."

Mr. TIMMONS. Without objection, so ordered.

Mr. SUBRAMANYAM. Thank you.

I think it is pretty clear that this should not have happened. We need to understand how prevalent the use of third-party apps and private phones is when talking about classified or secure or sensitive information. And so, we have sent a letter to the Administration. I hope that we will get some answers.

I yield back.

Mr. TIMMONS. Thank you.

I now recognize the gentleman from Texas, Mr. Cloud, for 5 minutes.

Mr. CLOUD. Thank you, Mr. Chairman. I appreciate you hosting this hearing. I appreciate you witnesses being here.

I actually came to this hearing thinking that we were going to be able to have a bipartisan hearing on this, as we all agree that CCP is a tremendous threat, that our infrastructure needs protected.

It is surprising, again, to come to this and to see the politicization of this hearing. It seems to be that Democrat administrations can use Signal, but Republicans cannot. That when we have successful attacks against the Houthis, they get overlooked, but yet, when the Biden Administration withdrawals from Afghanistan and 13 of our servicemen get killed, that the Dems sit on their hands and do not seem to be concerned about that at all.

We just had another successful attack against the Houthis last night. So, it seems that our Administration is able to proceed unabated, regardless of the Chicken Little Pie in the Sky, the Sky is Falling stories from our Ranking Member.

Thank you all for being here.

Mr. Steinman, could you explain or answer for me, would Signal messages be susceptible to exposure by the Salt Typhoon attack?

Mr. STEINMAN. I would want to defer to my technical colleagues here to the left. Obviously, it is an end-to-end encrypted service. It is going to depend on a wide range of variables including, is the end point compromised? Again, I would defer to the technical experts here.

Mr. CLOUD. Mr. Amoroso?

Dr. AMOROSO. Sure. I am happy to provide guidance.

So, you are asking whether, in a sense, the Chinese——

Mr. CLOUD. Salt Typhoon.

Dr. AMOROSO. Salt Typhoon. So, Salt Typhoon is a broad description of an actor. And one of the things we learned, like take the end-to-end cryptography argument that was made earlier, that the transmission is secure between the end points. That is using a type of cryptography called public-key cryptography. It is a Diffie-Hellman key exchange.

It turns out that is actually something that is susceptible to quantum computers, and it is entirely possible that the PRC could have a bunch of those in the basement.

So, I could imagine that even Signal is vulnerable to nation-state surveillance in real time. What we have learned is, in our own intelligence community, we have always been 10 to 15 years ahead of where we all think cryptography is. So, chances are, it is kind of scary, Russia, China, and so on are probably a lot further along than we think they are in crypto.

That is why I think in general——

Mr. CLOUD. This seems to me to fall into the—I appreciated your opening statements where you talked about kind of the potholes of yesterday to where, you know, since maybe this did not fall into that category but more in the what are the sinkholes for the future——

Dr. AMOROSO. Right.

Mr. CLOUD. I thought that was the whole idea, that, from a security posture, whether it be in our typical DoD stance but certainly in cybersecurity, we need to be skating to where the puck is going.

Dr. AMOROSO. I agree with you. I mean, I know where you are going, and I agree. I think China is a better actor than I think we had ever expected at this point. I mean, just sort of extrapolate back. We kind of used to lampoon, "They do not know that they are doing." And then they got better, and then we kind of see Salt Typhoon, and all of us go, "Whoa, you know, they have gotten pretty good."

So, I think that is a wake-up call. Whether it would be good enough to break Signal, whether Salt Typhoon connects, you know, we can sit and debate that.

But I think, if you push the puck forward on the ice a little bit, it gets pretty scary for things like even Signal. That is kind of my point. Like, where we are going, is even things you might depend on now are probably not going to be things we can depend on soon. So, all of us need to think through how we fix that.

Mr. CLOUD. A couple of my big concerns—and I may run out of time to get both of them, but, you know, it has been said, if you find yourself in a hole, stop digging. So, while we need to talk about what we can do going forward to kind of build and harden

our infrastructure and those kind of things, I am also concerned about what we might be doing already that is allowing access.

You know, I wonder—we do not know the actors or the group within Salt Typhoon. I think only one has been kind of outed. The rest we do not know. So, we do not know where they are getting their training, but I do wonder how many of them were trained here in the United States at our universities. I wonder about the infrastructure that we get that is—you know, even most of our phones are made in China, for example.

Could you speak to that and what we could do to kind of harden our infrastructure where it is right now, and then we can talk about where we need to go?

Dr. AMOROSO. Great analogy. You do want to stop digging when you are in a hole.

I think one of the things that I hear all the time, like in the context of telecom, Salt Typhoon, and even the broader issues is we need to find the gaps. Go find the three, five, seven gaps, and close them. I think that that is a fool's errand. Like looking for the gaps and fixing them is not the way we get out of this.

I think we need to design brand new infrastructure and start finding a way to eventually transition. Like, in our world, we would call that next-generation infrastructure, and I think that is something we have to do. It may sound like a big lift, but I do not see any other way.

Mr. CLOUD. I guess my concern is, OK, if China is still building the next-gen hardware and then importing it into the United States, do we still have that issue? I guess that is the kind of question I am asking.

You know, and if we are still training—you know, we come up with the latest best practices, and then we continue to train their cybersecurity experts and send them back home to do damages.

Dr. AMOROSO. No, I am against that.

On the hardware thing with Huawei——

Mr. CLOUD. That is kind of, I guess, my concern. I do not know.

Dr. AMOROSO. It is sensible, to your point, that, for things like Huawei, that we stay away from that equipment. I think that is wise, and I think we all probably agree with that.

What is interesting is, in Salt Typhoon, they did not use any Huawei backdoors. While I was at AT&T, I do not think they have since gone and bought any Huawei equipment. So, that was not either the front, side, or even one of the components of the attack. So, we sort of learned that they do not need that.

Now, I am not saying we should be buying that. I am against that. But it was not part of the attack factor, which, for a lot of us, is kind of——

Mr. TIMMONS. Thank you. We are going to have time for a second round of questions.

I now recognize——

Mr. SUBRAMANYAM. Mr. Chair, I wanted to enter something into the record.

Mr. TIMMONS. Sure.

Mr. SUBRAMANYAM. I would ask for unanimous consent to enter into the record an article, dated March 27, 2025, titled "Previous

administrations were wary of the messaging app Signal. Trumpworld has embraced it."

Mr. TIMMONS. Thank you for that.

Without objection, so ordered.

I now recognize the gentleman from Massachusetts, Mr. Lynch, for 5 minutes.

Mr. LYNCH. Thank you, Mr. Chairman, and thank you for holding this hearing.

This is a serious issue. This is a serious issue. What bothers me is that, you know, raising the issue of national security when our top national security and defense officials go on an insecure app, and they talk about—they offer actionable intelligence in advance of a military operation in which our sons and daughters are at risk. And then, if we raise it in the Oversight Committee on a hearing, it is politicization?

It is one thing—you know, I know a lot of my Republican colleagues. Over 25 years, I have worked hand in hand with a lot of them on issues of national security. And, you know, Senator Lankford, when he was over here, very serious on that issue. Worked with him on a bunch of different things.

It is one thing—look, I can understand if Republican Members do not want to say anything about what the Trump Administration did on this and what they continue to do. But to call it politicization and also to give the blessing on what they did and call it a success scares the hell out of me.

If you think that was a success, going on an insecure line in advance of a military operation and discuss openly on an insecure app the operational details of the forthcoming strikes on Yemen, including information about targets——

Mr. CLOUD. Will the gentleman yield?

Mr. LYNCH. and weapon systems and attack sequencing, that is OK?

Mr. CLOUD. Will the gentleman yield?

Mr. LYNCH. No, I am not going to yield.

I am offended. I am offended that Members would say that is politicization when we are trying to protect our sons and daughters in uniform and use this forum. Are you kidding me? Are you kidding me?

That was a colossal failure. We cannot encourage that. We cannot encourage that type of activity.

On this Committee, classified briefings, we are informed not to use Signal. We were informed that there are certain protocols that you have to take up.

Mr. TIMMONS. Will the gentleman yield?

Mr. LYNCH. I am not yielding, no.

And my colleague got an extra minute on top of what——

Mr. TIMMONS. I will give you 2.

Mr. LYNCH. A minute and 40. So, maybe I will have time at the end to yield.

Here is what gets me. It is pointless for us to sit in this Committee and try to grapple with the real issue of Salt Typhoon and other threats to our communication systems if the people at the top do not take it seriously. We can talk about all of the protocols and

debate and devise the best methods and insist upon up-to-date technology and take all of those steps.

But, if the Vice President, J.D. Vance; and National Secretary of Defense Pete Hegseth; and Secretary of State Marco Rubio; and Mike Waltz, our National Security Advisor; and Director of National Intelligence Tulsi Gabbard go on an insecure line and talk about operational intelligence on an insecure line, then everything we do here is pointless. That is what I am getting at.

So, we ought to be able to talk in a meaningful way and point that out. That is relevant. That is important. And they need to know that.

And telling them, "You were great, and that was a success and look how great you did,"—that is not good. That is not good. That is not helpful to our national security.

They made a mistake. Now, you do not have to say that publicly, but, dear god, do not tell them, "Way to go, nice job, great success." That is insane. That is insane for anybody who takes national security seriously. That is what I am getting at.

And so, our work here cannot be just, you know—it cannot be just, you know, advice to Democrats when they are in office. It has to be guidance as well to others, you know. It shows that we are taking our job seriously, and it is not just for show.

This is not politicization. This is national security. This is the real stuff. And there have been—and I am happy to hear—there have been Republican colleagues who are very worried about this, and they have said that. And they try to be as respectful as they can to their Republican colleagues, and I understand that. I get that part.

But that is a far cry from saying, "Way to go, do it again, that was successful." You know, it is just—it does not bode well for our future and for the work of this Committee.

Let me just ask a quick question, Mr. Blaze. On top of all this, the Trump Administration has just laid off 130 folks at CISA, and these are some of the very best.

So, the private sector is covetous of, you know, getting some of our really smart cybersecurity people to work for them. So, when you lay off 130 CISA personnel, does that help our national security? And what problems does that present?

Dr. BLAZE. Well, I mean, I can tell you that CISA, in both the first Trump Administration and the Biden Administration, was an invaluable resource in protecting critical infrastructure. It is a small agency. You know, arguably, it has been understaffed from the beginning.

But it is, essentially, the only clearinghouse for threat intelligence across government and the private sector. And any diminishment of that capability will harm us.

Mr. LYNCH. All right. Thank you, Mr. Blaze.

Mr. Chairman, if I have any extra time, I would yield to you, Mr. Chairman.

Thank you.

Mr. TIMMONS. We will have an additional round of questions if you would like to ask additional questions.

I now recognize the gentleman from Arizona, Mr. Biggs, for 5 minutes.

Mr. BIGGS. Thank you, Mr. Chairman. This is an important hearing. I appreciate you holding it.

I appreciate the witnesses being here. And you have been able to witness already the politicization of this hearing. So, it is a crying shame.

And, Mr. Steinman, what I will tell you is I am a layman, and so I will use the term "cyber-attack," and I may mean probe; I may mean disruption. But I am talking about a malignant actor, a malign actor who is trying to do something that is detrimental to some secure system that we have. That is what I am referring to.

And so, according to the Internet Security Alliance, thousands of daily attacks, cyber-attacks, put the operational continuity of critical infrastructure at risk and have led to trillions of dollars in economic losses to date, meaning that cyber-attacks threaten both our national and economic security.

Estimates indicate that 40 to 70 percent of our private and public sector cybersecurity work force and resources are spent on navigating a patchwork of overlapping, contradictory, and duplicative regulatory regimes. These contradictory schemes are promulgated not only at the international, local, and Federal level but often between Federal agencies themselves.

Every minute spent navigating the bureaucratic morass of conflicting rules is time actually spent focused away from cyber threats.

So, my question for you, and I will go with you, Mr. Amoroso, what steps should Congress and the Trump Administration take to harmonize Federal cybersecurity regulations to ensure that cybersecurity resources and the cyber work force are focused on protecting the American citizens in our critical infrastructure?

Dr. AMOROSO. Thank you for the question.

And, on behalf of every CISO on the planet, we would sure like to see fewer frameworks and regulations.

The NIST cybersecurity framework, which is in version two, is really good, and it is almost like an umbrella standard to most of the other standards that are imposed on an enterprise security team.

So, I think if you add 50 heads of security across the whole critical infrastructure, even midsize and small companies, they would all agree that simplifying that to one or two frameworks would be a really good idea.

Now, we use these tools called GRC tools—governance, risk, and compliance tools. So, we have been able to automate away a lot of the complexity. So, we have dealt with it. But it would be quite welcome if there was some simplification there.

Mr. BIGGS. Do you have any thoughts of how tools like artificial intelligence could be deployed to assist in reviewing and constructing a framework?

Dr. AMOROSO. They would be great. I mean, everyone in the room here has used ChatGPT where you ask it a complex question. You feed this complex thing and say, "Explain this to me." Well, think about complex regs and asking how it might apply to an industry. AI is really good at that.

So, we have gotten pretty good at dealing with—you would use some words like "complex," which is absolutely accurate. We have

dealt with that using technology. But still, it would be nice to simplify that. I think it would cleanup a lot of the security infrastructure we have in place.

Mr. BIGGS. Mr. Blaze, Professor Blaze, your written testimony outlined a concern that I share, that lawful access mandates present risk to Americans, both that tools may be abused or that those lawful access mandates may be exploited by malign actors.

And you talked about encryption. Indeed, encryption is not a silver bullet, but it is, as you discussed, an important countermeasure.

Despite years of advocacy that Congress impose wiretap-ready mandates on end-to-end encrypted communication tools—which, by the way, I really appreciate you raising that in your piece—in response to the Salt Typhoon attack, Federal law enforcement agencies issued a series of public reports and statements recommending that Americans utilize encrypted voice and text communication methods.

I ask for unanimous consent, Mr. Chairman, that one of those, the Cybersecurity and Infrastructure Security Agency's mobile communications best practices, be entered into the record.

Mr. TIMMONS. Without objection, so ordered.

Mr. BIGGS. Thank you.

And, back to you, Mr. Blaze.

Would imposing such a mandate expose those communication methods to the same risk present without encryption?

Dr. BLAZE. I mean, end-to-end encryption makes the communication strictly more secure—it is not perfect. It is not a panacea. It still leaves us vulnerable to attacks against the end point.

But what effective end-to-end encryption does is essentially removes attacks against the infrastructure, such as we saw in the Salt Typhoon attacks that have been made public so far, from the equation.

Essentially, Signal's encryption, you know, we do not know that it is perfect. We do not know that there are not hidden——

Mr. BIGGS. I am not talking specifically about Signal. I will save that for another round of questions.

Dr. BLAZE. Sure.

But, for example, Signal, we do not know if any of this encryption is perfect. We do not know if there is some attack that will be discovered in the future, but it is probably safe to say that the easiest way to attack an end-to-end encrypted communication is by attacking the end point.

It essentially becomes a waste of time to attack it through the infrastructure, and that is a significant gain.

Mr. BIGGS. So, while we are here, Mr. Chairman, if you will indulge me just real quickly, it has been publicly reported that the U.K. has been putting pressure on Apple to build a lawful access backdoor into encrypted iCloud backups, not unlike what you talked about in the 1990s.

Senator Ron Wyden and I have raised concerns about this approach with the Trump Administration, specifically asking the Administration to put pressure on the U.K. to back down or face consequences.

And I ask unanimous consent that our February 13, 2025, letter be entered into the record.

Mr. TIMMONS. Without objection, so ordered.

Mr. BIGGS. And so, here is the question, Professor Blaze. What tools are at the Administration's disposal to ensure that our own allies are not taking steps that jeopardize Americans' privacy?

Dr. BLAZE. Well, you know, again, we should encourage the use of end-to-end encryption because we use the internet and communications for essentially everything about our economy, everything about our national security. Everything about our personal privacy depends on the security of our communications infrastructure.

And, you know, so, we need to promote the use of end-to-end encryption enthusiastically and vigorously. And anything, regulations that mandate things like cryptographic backdoors, are a step backward from doing that and will make us less safe.

Mr. BIGGS. Thank you.

I yield back, Mr. Chairman. Thank you for indulging me.

Mr. TIMMONS. Thank you.

I now recognize the gentleman from California, Mr. Garcia, for 5 minutes.

Mr. GARCIA. Thank you, Mr. Chairman.

Thank you to our witnesses for being here.

And, obviously, I think we can all agree that the Salt Typhoon hacks were very serious. It deserves a full response. Clearly China is targeting our networks, and we need to step up to prevent them and, of course, prevent worse things from happening.

But, of course, I strongly disagree with the comment that we should not be discussing other serious national security concerns. Members of Congress have the absolute right in hearings to ask questions that are of grave national security concern, and the fact that we, as the House Minority, Democrats, are focused on the serious national security breaches that have happened because of Secretary Hegseth and others on the Signal fiasco I think is the right response from us.

The American people demand accountability for the Signal disclosures, and, as a reminder, we had not only Defense Secretary Pete Hegseth; we have National Security Advisor Mike Waltz; the Vice President; the CIA Director; our Secretary of State, Marco Rubio; Treasury Secretary; and the Director of National Intelligence all debating foreign policy, arguing about national strategy, and sharing what is clearly war plans, even though they would like to say that they were not, on a Signal chain.

So, this is of absolute importance to this Subcommittee and important for us to discuss it.

Of course, they are doing all this while chatting with a reporter. We can all agree, hopefully our Republican colleagues included, that that is totally insane and a level of incompetence and recklessness that should never be in our government.

Now, Dr. Blaze, we have seen this many times. This is, of course, one of the updates from Secretary Hegseth. Dr. Blaze, here we have the Defense Secretary laying out exactly when and which planes we are going to fly and when our pilots would be in danger.

Now, Dr. Blaze, I understand that Signal is a good commercial option to communicate. A lot of folks use it. But to communicate

exact times, directives, war plans is absolutely unacceptable. Would you—I know you have said it before, but do you agree that this, from a national security perspective, should not be on this type of unsecured chat.

Dr. BLAZE. I have no idea at what level that would be classified, but it is certainly sensitive national security information intuitively.

Mr. GARCIA. And do we agree that Secretary Hegseth or anyone at DoD should know this, correct?

Dr. BLAZE. Yes. Anybody with access to classified information would also be briefed and have access to the authorized tools for handling that.

Mr. GARCIA. And so, here we have Secretary Hegseth sharing information, which exposes our soldiers to danger, even though he should know that information could actually get to our adversaries.

And, remember, the best cybersecurity practices in the world actually do not matter if you are also careless enough to send all of this classified information, which I believe it is classified, straight to an actual reporter.

So, Dr. Blaze, can you remind us what would happen to an enlisted person or an officer who had leaked similar information?

Dr. BLAZE. Well, I think, you know, it is safe to say that if I did something like that, my access to classified information would be immediately revoked. I would probably be terminated immediately and be facing a criminal investigation.

Mr. GARCIA. Right. So, if you are a rank-and-file member of the military, you certainly would receive severe punishment, a variety of different options. Yet the Secretary of Defense is still in his position, having committed a major offense, clearly a breach on national security protocols, and put American lives in danger.

Many of us have said it before. We will repeat it again. He should resign, or he should be fired.

In addition to that, Hegseth, of course, we all know has had numerous other issues in his past, been accused of numerous other things, was never qualified to actually do the job, and continues, in my opinion, to not live up to this enormous mistake that he, of course, and others made.

Now, I want to also just point out the bombings actually did not solve anything. Attacks from Yemen still continue. And the whole episode revealed breathtaking incompetence. We got lucky this time that no Americans were killed, but unless things change, we are sitting on a ticking time bomb.

And I just also want to note, because I think it is important, that the CIA Director and DNI Director, Tulsi Gabbard, who were active participants in the chat, have told Congress under oath that they do not remember basic facts about the conversations they actually had and were involved with, of course, to avoid any sort of responsibility.

Personally, I think they lied to Congress and should be held accountable.

Now, we also know this is not the only time these people have used Signal to discuss classified information or other systems, and I just want to remind us that the *Wall Street Journal* just reported that Waltz, quote, "created and hosted multiple other sensitive na-

tional security conversations on Signal with Cabinet Members." And, of course, now we are also learning that he is sending information through his personal Gmail account.

So, this is an enormous amount to investigate. We absolutely have a right to bring it up in this Committee, and we need additional accountability.

And, with that, I yield back.

Mr. TIMMONS. Thank you. I now recognize the gentleman from Arizona, Mr. Crane, for 5 minutes.

Mr. CRANE. Thank you, Mr. Chairman, for holding this important hearing today.

Thank you, guys, for coming. You guys are probably starting to see why it is tough for us to get anything done up in Washington, D.C.

I do want to defend my colleague, Mr. Cloud. I do not believe he ever said that, you know, the Signal Chat episode was a success. I believe he was talking about the strikes against the Houthis.

I also find it rich that my colleagues on the other side, who now claim to be the accountability and transparency police, said absolutely nothing, you know, when we pulled out of Afghanistan and 13 Marines were killed, amongst other issues.

So, moving on to this hearing, I think it was great, Dr. Amoroso, that you talked about potholes and sinkholes. You are looking at many of these hacks that we have experienced in the past as potholes. But you seem more focused on the bigger attacks that will come in the future, and you are referring to those as sinkholes. Is that correct?

Dr. AMOROSO. That is correct.

Mr. CRANE. Sir, would you look at some of the individuals that have hacked into our energy grid as a possible sinkhole scenario?

Dr. AMOROSO. Yes.

Mr. CRANE. Can you tell us what your major concerns are when it comes to infrastructure like that?

Dr. AMOROSO. Disruption.

Mr. CRANE. Yes. Isn't it true that the former FBI Director Wray even talked about that himself?

Dr. AMOROSO. You know, I am not sure. That is a common point though, certainly.

Mr. CRANE. Mr. Steinman, do you remember that?

Mr. STEINMAN. I believe I do, sir.

Mr. CRANE. Yes. What do you think would happen if the CCP or one of our adversaries were to take down our energy grid?

Mr. STEINMAN. I think it would sow incredible chaos. I think it would be damaging to almost every American in the first and in the second order, given the food supply chains that we use to eat every day, the energy required to purify water, to process sewage, et cetera. And, respectfully, sir, I would just offer that there have been numerous unclassified statements by executive branch senior executives to say that we do have foreign adversaries on that energy grid.

Mr. CRANE. Right. Absolutely. One of the things that you guys brought up is whoever controls AI and does the best at implementing it into our cybersecurity, you know, will obviously be in the best position. Can you guys talk to how the U.S. Government

is doing in implementing, developing AI, and using it within cybersecurity?

Dr. AMOROSO. I can offer a couple of points. I have spent a lot of time on that. First, I think everyone should recognize, again, another analogy: If you are a human being playing a well-programmed computer in chess, you realize you lose every time, right? I think everyone gets that.

So, just, do you think we can beat a computer at cyber? You kind of can. And, as your adversary starts to really move in that direction, you have to do that too.

Now, when we think AI—in fact, for any of you, if you are thinking AI, the first word that should come to mind is "data." You have to have data to train systems to learn. Just like with children, they have to be exposed to experiences to learn. AI has to be exposed to data and, to some sense, experience. That is the first thing we need to do as a Nation.

So, we have a lot of privacy concerns and a lot of issues of intellectual property and ownership and competition. And you have seen some of it in the hearing. You hear some of the squabbles that we have in our country. We have to fix that. If we cannot fix that, then we will never be able to build—like I have heard the President talk about this big global shield. Well, I think that is a perfectly good metaphor for AI. We need to do something that allows us to protect against AI offense. So, the only way to do that is we have to architect something that makes sense. We need to have the right access to data. We have to have the national labs involved, and large critical infrastructure has to be involved. Academia has to be involved, and our government leaders need to be working together to help us coordinate something along those lines.

Mr. CRANE. Mr. Steinman, do you want to take that one?

Mr. STEINMAN. Yes, sir. I would also offer that it might be worth the Committee's time to look into some of the barriers to information sharing that private sector executives and companies face. I believe it was mentioned previously around DHS' role as acting as an information clearinghouse. But there are a number of barriers around liability protection that I believe in order to adequately address will require congressional action. So, I would just offer that up as a possible place where you all can do some work.

Mr. CRANE. Thank you.

I yield back.

Mr. TIMMONS. Thank you. I request unanimous consent that the Subcommittee shall have a second round of questions for the members.

Without objection, so ordered.

I now recognize myself for 5 minutes of questions.

So, I was hoping to talk about Salt Typhoon more. I just want to clarify some things about the Signal chat issue. So, there is really three components of it. There is the app Signal. There is the individuals', that are on that are communicating on the app, cell phones. And then there is the content and the people that had access to the content.

So, let us talk about Signal first. Mr. Blaze, the Salt Typhoon attack, would Signal messages have been susceptible to the Salt Typhoon attack?

Dr. BLAZE. So, from what we know from the Salt Typhoon attack, so far, it has been limited to the infrastructure itself.

Mr. TIMMONS. The unsecured communication on the infrastructure.

Dr. BLAZE. On the infrastructure.

Mr. TIMMONS. They were basically collecting data that was going through the infrastructure, and because—if it was unsecured, they would be able to access and see what it says. But, if it was secured, they would just throw it away because it is ones and zeroes and does not make any sense.

Dr. BLAZE. That is right. What Signal effectively does, is means attacks against the infrastructure cannot reveal content.

Mr. TIMMONS. Thank you. That is exactly what I wanted you to say.

So, Signal has actually been encouraged to be used by the Department of Homeland Security, Cybersecurity Infrastructure Security Agency, CISA, and it was actually recommended under the Biden Administration for potentially highly targeted individuals to use it. So, not only is it best practice to use end-to-end encrypted; it is encouraged to the point where, when the CI Director took his post, they were like, "You need to use Signal; you cannot use anything else."

So, I guess, No. 1, Signal is secure unless—unless—the cell phone is compromised. So, my question, Mr. Blaze, does it matter what app you are using if the cell phone is compromised?

Dr. BLAZE. Well, no, but let me just add a bit of nuance to what you said. Signal is secure in that it protects the information in transit. But one of the reasons it is not authorized for classified national security purposes is it lacks features designed to protect classified information, such as ensuring that the recipient has a clearance and is authorized to receive it.

Mr. TIMMONS. Correct. But, again, Signal is secure end-to-end encryption. But, again, it has to go to the right person.

Dr. BLAZE. It has to go to the right person. So, it would be—the classified tools would make it impossible, for example, to inadvertently add a reporter.

Mr. TIMMONS. But, again, if the cell phone is compromised, it does not matter what app you are using because the cell phone is compromised. And, in this case, our national security actors are not—have had their cell phones checked; their cell phones were not compromised. Obviously, the issue now becomes the content, which was not classified. Was it best practice for a reporter to be included? No. Had that reporter told the Houthis what was going to happen, would that be really bad? Yes. It did not happen. I can promise you that this will not happen again.

National Security Advisor Waltz has indicated that this was an error. And, I mean, listen, it is an error that will not be repeated. He is an incredible asset to our national security team. So, again, there is just a lot of confusion around this.

Signal is a secure end-to-end encrypted app. The cell phones were not compromised. A person was added in error, and it did not have any impact on the outcome of the operation, which was a success.

So, I mean, I think the biggest thing here is that I feel like my colleagues across the aisle are talking out both sides of their mouths when they are concerned about this Signal chat that had no adverse impact to national security and did not involve classified information—and I can promise you it will not happen again—when we did not have any hearings on Joe Biden having classified information that he actually had no right to have in his garage from his time in the Senate. Hillary Clinton's, I mean, classified email private server for days. And Joe Biden used a fake email account to correspond with his son's business associates.

So, I guess all of these things. I mean, we are here to talk about Salt Typhoon and what we can do to, as Dr. Amoroso pointed out, avoid the sinkhole. We have got potholes for days. The sinkhole is coming, and we need to be working to make sure that we are ready. And I would say that we certainly are not right now.

So, I look forward to working with my colleagues across the aisle to make sure that our country's critical infrastructure is secure, and we have got a lot of work to do.

With that, I yield back.

And I now recognize the gentleman from Virginia, Mr. Subramanyam for 5 minutes.

Mr. SUBRAMANYAM. Can I get unanimous consent first to enter into the record a couple of articles? One, "Chinese hackers are said to have targeted phones used by Trump and Vance." This was October 25 of 2024. I believe that is the *New York Times*.

Mr. TIMMONS. Without objection, so ordered.

Mr. SUBRAMANYAM. And then the second one: "Pentagon Warned Staffers Against Using Signal before White House Chat Leak." I believe this was the *Washington Post*, on Tuesday, March 25, 2025.

Mr. TIMMONS. Without objection, so ordered.

Mr. SUBRAMANYAM. Thank you, Mr. Chairman.

So, Mr. Blaze, have you seen any evidence that the personal devices of the people who were using Signal were compromised or not compromised?

Dr. BLAZE. I have seen no evidence one way or the other.

Mr. SUBRAMANYAM. Yes, so we do not actually know if their phones were compromised or not. But we do know from the article I just entered into the record that, certainly, the Vice President was already a target. And, certainly, if I were looking to target someone, I would look at our National Security Advisors.

And I just have to say, that I have not heard from the Administration much about this being an error, but I am glad I am hearing it from some. But, you know, what I really want to hear from the Administration is that they made a mistake, that they are going to fix it, and here are the steps they are going to take to make corrective actions in fixing what was a serious, serious blunder and a serious leak of national security intelligence.

And that is my problem with this is that, even if you say that a mistake happened, there are no steps right now in fixing this as far as I know. And there is no one admitting that they made a mistake. And there is nobody telling us what corrective actions are actually being taken, how prevalent this issue was.

I entered into the record earlier about how previous administrations were hesitant to use Signal for this very reason that our wit-

nesses are telling us today. One witness said that Signal could actually be hacked, even though it is encrypted, end-to-end, because we now have quantum computing. That is a really good point.

And then, Mr. Blaze, Dr. Blaze has also mentioned that these systems are vulnerable, even setting aside Signal itself. And we have 13,000 secure facilities across the country, and we have staff for every one of these national security experts who are there for the very purpose of making sure that they can communicate, anywhere and anytime around the world, troop movement and other sensitive classified information. And so, it is not like we have not given the Administration the resources to communicate securely. It is just that they decided not to. And, in doing so, I think they have broken at least six laws in regards to security as well as transparency. And I think this is a big problem that the Administration has broken these laws and not admitted any sort of faults or mistake.

And the response has been to just toss this aside as just ho-hum or Chicken Little, I think, was said earlier. I think there needs to be more attention paid to what happened, how prevalent it is, and what the Administration is actually going to do about it.

And so, this is relevant because, you know, today's hearing is about compromising our telecommunications infrastructure. But, you know, if you did a poll—I think we have a study of all of the chief information security officers—I think 80 percent said that human risk was the No. 1 problem in securing cybersecurity and telecom information.

And then I would actually ask you, Mr. Blaze, would you agree with that characterization that human error might be the No. 1 concern when it comes to telecom risks?

Dr. BLAZE. That is probably true, although I quibble a little bit with how we define human error. A lot of human error is inevitable because of poor design choices for the systems that we use.

Mr. SUBRAMANYAM. Sure. But I guess what I would really like, is to just have an investigation into what happened. And one of the things I would like to share with my colleagues is that we have actually asked for an investigation. I think there are only Democrats on the letter to the Administration right now, but I know some Senators on the Republican side have actually openly asked for some sort of investigation. But at least we can get to the bottom of what happened, how prevalent this is, and what we can do to fix it so that it never happens again. I hear that that is a shared goal, and I would like to see us work together in doing that.

And so, instead of trying to sort of brush this aside as something that is not a big deal, let us admit that it was a big deal, and let us try to take steps to fix it and not just try to cover this up.

Thank you, and I yield.

Mr. TIMMONS. Thank you.

I now recognize the gentleman from Virginia, Mr. McGuire, for 5 minutes.

Mr. MCGUIRE. Thank you, Mr. Chairman.

And thank you to the witnesses for coming here today.

During the attack, Salt Typhoon maintained undetected access for up to 18 months. This incident is described as one of the most severe telecom hacks in U.S. history. Despite existing public-pri-

vate partnerships to prevent cyber-attacks, it seems as though there are still significant information sharing gaps.

Mr. Steinman, are there any Federal laws or regulatory red tape that prevents or hampers the information sharing about hacks between government agencies and the telecommunications industry?

Mr. STEINMAN. Thank you, Congressman. I would, of course, defer to Dr. Amoroso's experience, being the former Chief of Information Security officer of AT&T, around specific granular challenges with information sharing. But I would like to emphasize the point that you made, which is that whether it is questions of liability at the corporate or individual level, questions of insurance, insurance policies—we saw that in the NotPetya cyber-attack and in the Colonial Pipeline attack, where we had issues of who would pick up the tab when there was a business interruption process as a result of a cyber-attack, but it really is a deep-nested issue.

Mr. MCGUIRE. The next question is for Dr. Amoroso. The 2023 National Cybersecurity Strategy emphasizes preventing the abuse of U.S.-based infrastructure, but it largely omits deterrence.

Dr. Amoroso, in your view, why was deterrence overlooked? And how critical do you think it is to incorporate it into the strategy?

Dr. AMOROSO. You know, it had come up earlier, this question of deterrence. I mean, certainly, it helps. I mean, I am an operator. So, I would not be the person doing the deterrence. But, if someone is doing it, it is going to help.

Your point about information sharing is an important one. You know, back in 1996, I remember sitting in this building when we first started talking about it; it was PDD 63. It was the first sort of ISAC stuff. We were very hopeful that information sharing would solve a lot of problems. It kind of has not. I wish it had, and I wish I could tell you that just improving the communications will make things better, but I have kind of given up on that.

I think it is time now to build a new barn. You know what I mean? Like, I think the one we have has been patched so many times, and it is so rickety that you and I are standing looking at it going, "You know what, time to build a new barn."

Mr. MCGUIRE. Well, we all know the definition of insanity. And, you know, China believes that everything can be used as a weapon, and it should be used as a weapon.

So, how would you propose, Dr. Amoroso, that the U.S. increase the cost on China to deter their cyber operations, especially when they seem to act with impunity under the current framework?

Dr. AMOROSO. Yes, I understand. Obviously, deterrence can be done in any number of ways. It is not really my area of specialization. You can do it with diplomacy. You can do it with non-cyber. But I think the best deterrence of all is to have best defense on the planet. You know, if they cannot break in, then there is no discussion.

Mr. MCGUIRE. Yes, it seems like we are in a reactive position rather than a proactive position on that.

Dr. AMOROSO. I would agree. I think that is where we are now. I think you and I would agree on that. But I would like to get around that. I think there is active defense; that is different than deterrence. You know what I mean?

Mr. MCGUIRE. Sure. Congress and President Trump established the Cybersecurity Infrastructure Agency in 2018 to protect critical infrastructure and guard against cybersecurity threats. Under the Biden Administration, CISA diverted resources to collude with social media companies to surveil and censor American citizens. Would you agree with that?

Dr. AMOROSO. I do not know anything about that. The others might know something. But I do not know.

Mr. MCGUIRE. Mr. Steinman?

Mr. STEINMAN. Yes, that is my understanding, sir.

Mr. MCGUIRE. And how about, Mr. Blaze, would you agree with that statement?

Dr. BLAZE. I have no idea how the resources were allocated.

Mr. MCGUIRE. Sure. Well, thank God we have President Trump back in the White House to fix the broken agency and restore it to its congressionally directed mission.

But I would ask you, if you wanted to become a subject-matter expert in cybersecurity for the purposes of helping the Trump Administration—and I guess I will start with Mr. Steinman, where would you go? What would you do to become a subject-matter expert so you can better help make decisions in Congress to help President Trump's America First Agenda and protect us from China and other adversaries?

Mr. STEINMAN. There is great resources available at the Sands Institute. It is a place where I point a lot of aspiring young cybersecurity professionals. There are classes taught by my two fellow panelists at Georgetown and NYU. I am sure they would love to have you as well. Thank you.

Mr. MCGUIRE. Dr. Amoroso?

Dr. AMOROSO. Ditto. There is a lot of good resources.

Mr. MCGUIRE. Mr. Blaze?

Dr. BLAZE. Absolutely. And I will point out many of my students are here in the gallery.

Mr. MCGUIRE. Awesome. And tell me where they are students?

Dr. BLAZE. Georgetown.

Mr. MCGUIRE. With that, I yield back. Thank you.

Mr. TIMMONS. Thank you.

I now recognize the gentleman from Texas, Mr. Cloud, for 5 minutes.

Mr. CLOUD. Thank you, again, Chairman.

And one of the big concerns I have is, of course, we need to secure ourselves against China, harden our infrastructure, you know, do everything we can to stand against what they're trying to. But we are a free society as well. So, I am always mindful that keeping the American people safe is one of our top priorities, but keeping them free is actually our top priority as Members of Congress and of the government.

And so—and then we are in the context of, as we move to AI, as you pointed out, Mr. Amoroso, the challenges are going to get monumental when it comes to cybersecurity, and then AI is dependent and developed on big datasets, which the CCP has no qualms about stealing, hacking, invading personal privacy of their own people and our people in order to create these huge datasets.

And so, as we put together solution sets, I am curious about how to keep that balance, as we move forward, of protecting the American people. Mr. Blaze, you even talked about the back doors in some of—that have been required in some of our telecom infrastructure, which is of a concern to me as well. I wanted to throw that out there and just see what your thoughts were. I guess we will start with you, Mr. Amoroso, if you want to follow up.

Dr. AMOROSO. Sure. I will give you an example. So, everyone in the room here uses Microsoft or Google for email, right, pretty much. And I am guessing everybody in the room here would say that doing emails is the worst 1 hour or 2 hours or 3 hours of your day, right? So, if you had a piece of AI that did your email for you and you trusted it and it worked and it gave you a little list at the end of the day the things that it needed to check in with you, then phishing goes away, like the phishing risk. There is other attacks that emerge; you know, malware in your AI agent. But the point is that, as we upgrade our infrastructure and we do it intelligently, we can make some of these attacks go away. It is one example. There are a lot of things like that, but to do that would require a concerted sort of coordinated effort with the email providers, with privacy groups, with government, and so on and so forth. That is kind of what I am talking about. But you can diminish the intensity of these attacks by using technology intelligently.

Mr. CLOUD. Mr. Blaze, do you want to speak to the issue of back doors and——

Dr. BLAZE. Certainly, so, more broadly, we are, you know, right now, fighting a battle in which the attacker for the offense side has the advantage because the systems that we have to defend are incredibly complex. New vulnerabilities are found, you know, every week. And the implications of attacks are so far-reaching we cannot even analyze what the consequences of some of these threats will be fully. And we will probably be at a disadvantage on defense for a while. It is one of the fundamental problems of computer science that we do not know how to build bug-free software. And, as complexity increases, the number of bugs and vulnerabilities also increases along with that. And that is a problem.

Mr. CLOUD. A bug is different than a mandated backdoor.

Dr. BLAZE. That is right. And so, adding mandated backdoors into the equation essentially, you know, preloads the bugs. We do not even have to find them; we know they are there already.

So, you know, we will never be able to make our defenses perfect with the way we are doing things now. It is a problem I would love to solve. But we can absolutely do better than we are currently doing.

Mr. CLOUD. Mr. Steinman, I wanted to ask you, you talked about us not being on a wartime footing when it came to our cyber infrastructure development. One of the disadvantages—you know, when we point to our history, for example, with the Soviet Union versus the CCP. I would say at least the Soviet Union was honest with us. The CCP has pretended to be our friend while they have planned for world domination and certainly our demise and used every avenue, including cyber, to be on war footing against us while, you know, we, especially in the previous Administration

would refuse to acknowledge that as a Nation. What does that look like using your experience and knowledge base?

Mr. STEINMAN. Yes, Congressman, I think that is right. I think Chinese Communist Party and their military intelligence apparatus are already, you know, in a footing that we would describe as a wartime footing. They believe that that is the posture that they should have 24/7. And they use language to try and communicate to us that they are not in that footing, and they use that language deliberately to deceive us and to make us think, oh, everything is OK; we can just sort of be friends.

They do this while hacking us blatantly while then denying when they get confronted. And so, I believe that it is time for us to take a much more aggressive posture. That is what we did when I was in the White House during the last Trump Administration, and I believe that it is the smart thing to do now.

Mr. CLOUD. Thank you.

My time is up. I yield back.

Mr. TIMMONS. I now recognize Mr. Biggs for 5 minutes.

Mr. BIGGS. Thank you, Mr. Chairman.

And thank you, again, to the witnesses for being here.

I just have a couple of specific questions and then a comment or two and then back to questions.

So, the first question is, do we know the—there were more than a million people essentially victimized in the cyber-attack that has consumed us today—well, should have consumed us today.

Do we know if each one of those victims, because I would say they are all victims, were each and every one notified that they were a victim? Do we know? Mr. Steinman, do we know?

Mr. STEINMAN. I do not know, Congressman. I think it is a great question.

Mr. BIGGS. Dr. Amoroso or Mr. Blaze?

Dr. AMOROSO. I have spent a lifetime with these kinds of large-scale attacks, and almost always the answer to that question would be no.

Dr. BLAZE. OK. I agree with Dr. Amoroso.

Mr. BIGGS. Yes, I always wonder with my own paranoia, you know, if I am in that group. But, in any event, and that leads me to some specific questions with regards to states and working with the Feds. So, you have all kind of alluded to this. There needs to be cooperation. There needs to be communications. There needs to be some kind of mutual communication about what needs to be done.

How have the states themselves responded, or how are they being treated in this? Well, let me back up. Is there any kind of working collaboration that really exists today?

Mr. Steinman?

Mr. STEINMAN. Thank you, Congressman. I would point to some of the bright spots in America's cybersecurity apparatus as the National Guard elements that do cybersecurity, and they have done a lot of activity both at home and abroad where they will train with victims of some of the most latest attacks.

Mr. BIGGS. Is this a broad—what I am trying to find out, is there a broad coalition or a collaboration that is going on? I mean, or is it a pocket here, pocket here, siloed here, siloed here?

Mr. STEINMAN. I have seen it state by state with the state partnership program of National Guard cyber elements.

Mr. BIGGS. OK.

Mr. STEINMAN. I do believe that is coordinated to some degree at the Pentagon, but you would have to dig into that.

Mr. BIGGS. Any other comments from Dr. Amoroso?

Dr. AMOROSO. I coach a lot of the security leads at the state level, and it is a full range. You know, there is multistate, different groups, multistate ISACs, and someone coordinating this and that, councils, groups. But they also compete. You know, they want to be the top state, you know, to do cyber. But the one thing they all say in common is, "We have no resources; we need more people." I think I have never met a state that says, "Gosh, we are good." So, they do need more resources.

Mr. BIGGS. Yes.

Dr. BLAZE. Oh, I would just point out that the resources of states are very much at a disadvantage compared with national resources that we have of the Federal Government. You know, effectively, we never ask—we do not ask the state police to repel foreign military invasions. And, you know, in a lot of cybersecurity issues, that is exactly what we are doing.

Mr. BIGGS. Yes, you know, I am thinking of places like Arizona, which has one of the largest nuclear facilities in the country, in Palo Verde. I am really interested. I have talked to them, and they are actively trying to, you know, protect that structure, the state is. But I am not sure how—whether the resources are there, whether the personnel is adequately there.

And now I am just going to make a quick comment here. And then I have to do this, and I am sorry because I wanted to get to some very specific issues, but this comment has to be made.

When you keep 30,000 classified emails on a private server in a private home, you might have a bit of a security problem. And that is what happened with Hilary Clinton, and bupkis, silence, quietude from the left.

And, Dr. Blaze, I am not trying to put you on the spot, but I am going to put you on the spot because they asked you a question; I am going to ask you a question to follow up, sir. It is not meant to be an attack at all. But, with regard to CISA and the individuals who have been RIF'd at CISA, I assume you do not have any personal knowledge of any of those persons, any of their qualifications, any of their performance capacity, any of their skills, their training, et cetera? Is that fair to say?

Dr. BLAZE. That is fair.

Mr. BIGGS. Yes. So, that is what we mean when we say this gets politicized. What they do not know, we do not know. But what we really wanted to find out today is what happened, how do we prevent it, how do we work together to stop it? And I feel like we have been derailed just a little bit here today, and that is unfortunate because both sides profess and want to get to the bottom of this because it is a national security issue and will, in fact, impact us, actually, for generations to come. So, we have got to get ahead of it like right now.

And, with that, Mr. Chairman, I yield back.

Mr. TIMMONS. Thank you.

I will now recognize the gentleman from Arizona, Mr. Crane, for 5 minutes.

Mr. CRANE. Thank you, Mr. Chairman.

Since my colleagues came in here and politicized this event today, I want to ask the Chairman: Chairman, did you forget to invite the Democrats to this event today?

Mr. TIMMONS. I did not. No, sir.

Mr. CRANE. Ah, that is interesting because, as I look down, I see a bunch of empty seats. And, for those that came in here and talked today, you will note that they asked very few questions about cybersecurity, how to prevent and stop it. They spent most of their time talking about a Signal chat.

And, after their comments, I hope y'all noticed that they got up and left. They did not really care what you had to say. Did you guys notice that? OK. Good. I am glad you did.

Now, back to the hearing. Because a lot of us are laymen on this topic, a lot of us wonder how hard is it once you identify a cyber threat that has embedded itself within your infrastructure or systems to either block them, kick them out, et cetera?

Dr. Amoroso?

Dr. AMOROSO. Yes, you know, someone that Matt Blaze and I remember, Ken Thompson, wrote a paper in 1983 where he taught all of us basically how you do what you just said and make it essentially disappear. I think it is not completely gone, but it is mostly gone. And we all kind of freaked out at the time. And here we are 40 years later, and we are talking about it. But you should kind of accept that, if somebody is really good at dropping malware into your infrastructure, you are probably not going to find it.

Mr. CRANE. Really?

Dr. AMOROSO. Yes.

Mr. CRANE. Do you think AI will really help us with that?

Dr. AMOROSO. I think you have to change the game. It is a terrible analogy, and I apologize. But, if I could drive a truck bomb into your home and blow the whole place up, how do you stop that? You do not put a fence. What you do, is you break your home up into a lot of different pieces. Suppose your home was a thousand concrete blocks; what do you blow up? And you say, "Well, I can't live in a house like that," and that is true. But computing works that way. We call it virtualization and cloud and so on.

So, it is we have to change the game, not sort of solve that older problem because you are not going to solve that problem.

Mr. CRANE. When you guys—you spent a lot time talking about the CCP and China today because they do have a very robust cybersecurity offensive capability. But, obviously, there is our countries out there as well that are hacking into U.S. infrastructure, like Iran, North Korea, Russia, et cetera.

When you guys look at the amount of resources that those countries throw into cyber attacking, and then you look at what we are spending on that as well, how does that measure out? Mr. Steinman?

Mr. STEINMAN. I think it is a great question, Congressman, and it is one that I would encourage a significant amount of attention from the Committee on, which is, you know, what are we paying for? Billions of dollars have flowed to the various cyber elements

of the Department of Defense and elsewhere, and what is that producing?

I will say it does produce a lot of good people that are very talented. But, when we think about capability, I just think there is probably a lot of room for investigation there. And thinking about, how can we use those dollars effectively and efficiently? I would also just like to touch on something that you seem to raise, which is that—and the panelists have raised—which is that we have lots of attackers coming at our critical infrastructure.

And what I would say is, by taking a more aggressive posture to go back at those attackers, we throw sand in their gears. We force them to spend time and effort to defend against our counter attacks. And those could be ones that are managed at the national level, or they could be the prickly landing point inside the company that those cyber actors are going after.

And so, I would just offer that there is a lot of opportunity to interrupt and delay and deny and obfuscate when we think about offense.

Mr. CRANE. I want to talk real quick, Dr. Amoroso, I know you come from the corporate world, the private sector. When you look at the amount of resources that the corporate and private sector is throwing at countering cybersecurity attacks as opposed to the Federal Government, can you give us some sort of comparison and understanding the differences between what the corporate and private America is doing and what the Federal Government is doing?

Dr. AMOROSO. There is a difference between size and quality, right? I mean, you can throw a bunch of resources. If you are doing it wrong, then you can double that, and it will not make any difference. So, I think, both in corporate and in government, we need to improve both. We need to optimize—like, in some cases, we do not spend enough time.

Take cryptocurrency; that is a place where we should be spending more time. I think, like, North Korea, I think they like fund the whole country by stealing cryptocurrency. So, there is an area where we have done a very poor job globally protecting ourselves. But in other areas we referenced earlier, like compliance, I mean, we have so many resources chasing framework after framework after framework that, when you count those resources, to your question, you could double it; it would have no impact. So, we have to rethink the size and quality. It is an optimization question as opposed to, do we have enough? Does that make sense?

Mr. CRANE. Yes. Thank you, guys.

I yield back.

Mr. TIMMONS. Thank you.

In closing, I want to thank our witnesses once again for their testimony today. Salt Typhoon is an important thing for us to learn from, and I guess we got to talk about Signal a bunch too. But, luckily, Signal chats are immune to Salt Typhoon, as Mr. Blaze pointed out.

With that, I now yield to Ranking Member Subramanyam for closing remarks.

Mr. SUBRAMANYAM. Thank you, Mr. Chairman.

Just before I go to my closing, I want to address a couple of things. One, someone mentioned that they did not know who the

CISA employees were, what their qualifications were. Actually, many of them live in my district, and so I can tell you from hearing from a few of them, they are actually—many of them were fired because they are probationary employees and who are actually very highly qualified in the work they are doing. They actually had very good performance records. And we had actually, in the past two administrations, including the first Trump Administration, been begging tech talent to come to CISA and come to the Federal Government, and then we fired them all. And so, we are actually—a judge actually said that that was illegal. And so, they are currently on administrative leave. But it is a big risk to our country when we are chasing away tech talent in our Federal Government. And so that is what really concerns me.

And, second, I still think we need to have an investigation into what happened with these Signal chats. If we want to fix the errors, if we want to make sure that this mistake does not happen again, we need to know, first, what happened? Second, what corrective actions are taken? Third, if this was not classified information, we should actually be able to have a secure briefing where we can get the communications from CENTCOM to the SecDef on exactly what they were saying or whether that was classified or not and what he shared, whether that was classified or not. We can do that in a secure briefing room.

But, either case, we need to get to the bottom of what happened, and that does not need to be partisan. But somehow it has become partisan, and that is disappointing.

I want to end by just sharing, again, constituent stories about this Signal incident because this really does hit home for many of the veterans and military families that live in my district.

One constituent said that they have worked in national security for 18 years: "I have held the highest security clearance for 18 years. And, for 18 years, I have lived a life most people will never understand. My promise to defend this Nation does not stop when I clock out, it permeates every single aspect of my life. It affects my marriage, who I live with, who I date, who I am friends with, who I speak to. I would be sitting in jail right now if I had done something as brazen and thoughtless and dangerous as what J.D. Vance, Pete Hegseth, John Ratcliffe, and Mike Waltz, amongst others, did today."

A second, whose son is the military said that, "That our Nation's top defense officials shared sensitive troop movements over a commercial social media platform without verifying who was on the other end is not only reckless; it is terrifying. Our servicemembers and their families deserve leaders who treat their safety with the gravity it demands. This breach not only endangers lives but erodes the trust of those who served and support our military. My son has sworn to defend this country. I expect the same level of responsibility, integrity, from those in charge."

I yield back.

Mr. TIMMONS. Thank you.

I guess we are going to start with Signal. I think it is important to realize that President Trump said Waltz messed up. So, accountability has been acknowledged, and a mistake was made. Waltz has, again, said it was an error himself.

I think what is important is that no harm resulted from this mistake. And I can promise you that it will not happen again.

So, I appreciate that my colleagues across the aisle will continue talking about Signal, but I think what is important is that our Administration is leading in the global community and is holding our adversaries accountable and keeping us safe.

As to the CISA employees that have lost their jobs, we have $36 trillion in debt. We are running a $1.8 trillion deficit. We have to right-size the fiscal ship in order to address any of the challenges that lie ahead.

And, while it is unfortunate that all of the probationary employees across all of the government were let go, we cannot continue forward on the trajectory we are. We just cannot afford it. We cannot afford it. So, we are having to make these decisions in order to make sure that we have the American Dream for generations to come.

Last, but certainly not least, Salt Typhoon—why we are here. So, we have had a good conversation about the exposure. Obviously, the Chinese were able to use outdated infrastructure to gather enormous amounts of unsecured data, and they focused it largely on Washington, D.C., because it is our seat of government and because they are able to learn what we're planning, learn from the communications between our government officials.

And I realize that my colleague from Arizona was asking the question of, was his data collected? If he is communicating on the phone or through unsecured text, I guarantee it was. So, you know, and they probably were able to figure out that he was a Member of Congress. And we need to use Signal, which is funny. We need to use Signal because it is more secure.

I also want to talk about what I think—Dr. Amoroso mentioned that we got to have a good defense. And I agree with him. I think that we need to do a much better job, and we can do that; we got to invest.

I think the bigger thing—I actually—on liberation day, as President Trump talks about tariffs for, you know, right-sizing our competitiveness in the global economy, I think that we have the opportunity to use tariffs in cybersecurity by holding our adversaries accountable. If you breach critical infrastructure, if a foreign adversary or even a foreign actor that is in a country that is not enforcing the rule of law, if they breach a business in the United States, if they breach the U.S. Government, if they breach critical infrastructure, we can say, "All right, this is why we believe it is the Chinese; this is the attribution. We are going to hold you accountable by using tariffs to extract revenge of some kind, to create a deterrent threat to make sure that this does not happen again."

Again, in the case of the Colonial Pipeline attack, we could give the resources to whatever country is struggling to enforce the rule of law. In the case of 9/11, harboring al-Qaida was enough for us to physically invade.

So, it is not unreasonable, if a terrorist or a foreign state is going to cause immense damage and threaten our national security, that we just use tariffs to hold them accountable to extract economic pain.

These are the conversations we are going to be having going forward. And I think that we need to both invest in a good defense and also go on offense to make sure that we are able to use every tool in our toolbox to hold both nation-state actors and nonstate actors accountable. That is the future.

And, again, I just really want to thank the witnesses for being here today. This was a very productive conversation.

And, with that, I will close.

Without objection, all Members have 5 legislative days within which to submit materials and additional written questions for the witnesses, which will be forwarded to the witnesses.

If there is no further business, without objection, the Subcommittee stands adjourned. Thank you.

[Whereupon, at 11:44 a.m., the Subcommittee was adjourned.]