WEATHERING THE STORM: THE ROLE OF PRIVATE TECH IN THE SOLARWINDS BREACH AND ONGOING CAMPAIGN

JOINT HEARING

BEFORE THE

COMMITTEE ON OVERSIGHT AND REFORM
U.S. HOUSE OF REPRESENTATIVES
[Serial No. 117–5]

AND THE

COMMITTEE ON HOMELAND SECURITY
U.S. HOUSE OF REPRESENTATIVES
[Serial No. 117–4]

ONE HUNDRED SEVENTEENTH CONGRESS
FIRST SESSION

FEBRUARY 26, 2021

Printed for the use of the Committee on Oversight and Reform

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

U.S. GOVERNMENT PUBLISHING OFFICE
43–755 PDF WASHINGTON : 2021

COMMITTEE ON OVERSIGHT AND REFORM

CAROLYN B. MALONEY, New York, *Chairwoman*

ELEANOR HOLMES NORTON, District of Columbia
STEPHEN F. LYNCH, Massachusetts
JIM COOPER, Tennessee
GERALD E. CONNOLLY, Virginia
RAJA KRISHNAMOORTHI, Illinois
JAMIE RASKIN, Maryland
RO KHANNA, California
KWEISI MFUME, Maryland
ALEXANDRIA OCASIO-CORTEZ, New York
RASHIDA TLAIB, Michigan
KATIE PORTER, California
CORI BUSH, Missouri
DANNY K. DAVIS, Illinois
DEBBIE WASSERMAN SCHULTZ, Florida
PETER WELCH, Vermont
HENRY C. "HANK" JOHNSON, JR., Georgia
JOHN P. SARBANES, Maryland
JACKIE SPEIER, California
ROBIN L. KELLY, Illinois
BRENDA L. LAWRENCE, Michigan
MARK DESAULNIER, California
JIMMY GOMEZ, California
AYANNA PRESSLEY, Massachusetts
VACANCY

JAMES COMER, Kentucky, *Ranking Minority Member*
JIM JORDAN, Ohio
PAUL A. GOSAR, Arizona
VIRGINIA FOXX, North Carolina
JODY B. HICE, Georgia
GLENN GROTHMAN, Wisconsin
MICHAEL CLOUD, Texas
BOB GIBBS, Ohio
CLAY HIGGINS, Louisiana
RALPH NORMAN, South Carolina
PETE SESSIONS, Texas
FRED KELLER, Pennsylvania
ANDY BIGGS, Arizona
ANDREW CLYDE, Georgia
NANCY MACE, South Carolina
SCOTT FRANKLIN, Florida
JAKE LATURNER, Kansas
PAT FALLON, Texas
YVETTE HERRELL, New Mexico
BYRON DONALDS, Florida

DAVID RAPALLO, *Staff Director*
PETER KENNY, *Chief Investigative Counsel*
ELISA LANIER, *Chief Clerk*
MARK MARIN, *Minority Staff Director*
CONTACT NUMBER: 202-225-5051

COMMITTEE ON HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
DONALD M. PAYNE, JR., New Jersey
J. LUIS CORREA, California
ELISSA SLOTKIN, Michigan
EMANUEL CLEAVER, Missouri
AL GREEN, Texas
YVETTE D. CLARKE, New York
ERIC SWALWELL, California
DINA TITUS, Nevada
BONNIE WATSON COLEMAN, New Jersey
KATHLEEN M. RICE, New York
VAL BUTLER DEMINGS, Florida
NANETTE DIAZ BARRAGÁN, California
JOSH GOTTHEIMER, New Jersey
ELAINE G. LURIA, Virginia
TOM MALINOWSKI, New Jersey
RITCHIE TORRES, New York

JOHN KATKO, New York *Ranking Minority Member*
MICHAEL T. MCCAUL, Texas
CLAY HIGGINS, Louisiana
MICHAEL GUEST, Mississippi
DAN BISHOP, North Carolina
JEFFERSON VAN DREW, New Jersey
RALPH NORMAN, South Carolina
MARIANNETTE MILLER-MEEKS, Iowa
DIANA HARSHBARGER, Tennessee
ANDREW S. CLYDE, Georgia
CARLOS A. GIMENEZ, Florida
JAKE LATURNER, Kansas
PETER MEIJER, Michigan
KAT CAMMACK, Florida
AUGUST PFLUGER, Texas
ANDREW R. GARBARINO, New York

HOPE GOINS, *Staff Director*
DANIEL KROESE, *Minority Staff Director*
NATALIE NIXON, *Clerk*

C O N T E N T S

INDEX OF DOCUMENTS

WEATHERING THE STORM: THE ROLE OF PRIVATE TECH IN THE SOLARWINDS BREACH AND ONGOING CAMPAIGN

Friday, February 26, 2021

HOUSE OF REPRESENTATIVES,
COMMITTEE ON OVERSIGHT AND REFORM
COMMITTEE ON HOMELAND SECURITY
Washington, D.C.

The committees met, pursuant to notice, at 9:06 a.m., via Webex, Hon. Carolyn Maloney [chairwoman of the Committee on Oversight and Reform] presiding.

Present from Committee on Oversight and Reform: Representatives Present: Representatives Maloney, Norton, Lynch, Cooper, Connolly, Krishnamoorthi, Khanna, Mfume, Porter, Tlaib, Bush, Rice, Wasserman Schultz, Welch, Johnson, Sarbanes, Speier, Kelly, DeSaulnier, Comer, Jordan, Hice, Grothman, Cloud, Keller, Sessions, Biggs, Donalds, Fallon, and Franklin.

Present from Committee on Homeland Security: Representatives Thompson, Langevin, Payne, Correa, Slotkin, Cleaver, Clarke, Swalwell, Watson Coleman, Rice, Demings, Barragán, Gottheimer, Malinowski, Torres, Katko, McCaul, Higgins, Guest, Bishop, Van Drew, Norman, Miller-Meeks, Harshbarger, Clyde, Gimenez, LaTurner, Meijer, Cammack, Pfluger, and Garbarino.

Chairwoman MALONEY. The committee will come to order.

Without objection, the chair is authorized to declare a recess of the committee at any time.

I now recognize myself for an opening statement.

Good morning. I want to welcome everyone to this joint hearing of the Committee on Oversight and Reform and the Committee on Homeland Security. Welcome to Chairman Thompson, Ranking Member Katko, Ranking Member Comer, and all of our members. Today's hearing is the first in the House on the cyberattack uncovered last year that initially targeted the software company, SolarWinds, and its Orion product. The details are truly frightening.

Here is what we know. A sophisticated attacker, reported to be the Russian Government, broke into SolarWinds' system and inserted malicious code into its software which customers then downloaded. The numbers tell how dangerous an attack like this can be. Nearly 18,000 customers downloaded updates containing the malicious code. It is not just the number of potential victims, as staggering as that is, or even the number of known victims of

secondary attacks, but the nature of this attack and the profiles of victims that should give us all grave concern. Among the victims were major technology companies, some of which have the best cybersecurity in the world, as well as critical infrastructure firms, our Nation's law enforcement and government agencies involved in foreign affairs, and national security. It has affected approximately 100 private sector companies and at least nine Federal agencies, including the Department of Homeland Security, Department of Justice, and state, and Treasury, and that is just what we know. There is much more that we still don't know. We still don't know if they are still in the system. In the weeks and months ahead, our committee will continue our joint investigation to examine other aspects of this massive attack.

Today, our focus is on the private sector. The private sector plays a key role in our Nation's cyber defenses, they own critical infrastructure, and they develop essential information, communications, and technology products. They help the government and other companies secure and defend their own networks. It was the private sector that uncovered this attack, not our own government. Specifically, FireEye discovered it, reported its findings, and shared it with the world. Had FireEye not taken that action, the attack could very well be fully up and running today.

At the same time, the private sector was targeted as part of a campaign to gain access to government networks and other entities. All of the companies here today are victims of this attack, and all provide products and services to the government that puts the government at risk. Additionally, it is the private sector to whom the government must turn. In particular, the government has turned to Microsoft to learn whether it was exposed and how badly due to the widespread adoption of Office 365 Cloud.

The private sector must be held accountable for its role. Our committees recently obtained a presentation made by a former employee at SolarWinds named Ian Thornton-Trump. The 23-page presentation, a portion of which I will put up on the screen now, appears to include a proposal from 2017 that stated, and I quote, "The survival of the company depends on an internal commitment to security. The survival of our customers depends on a commitment to build secure solutions." I look forward to hearing from Mr. Thompson about the steps the company took in response.

Cybersecurity demands strong leadership, but, unfortunately, we have suffered under four years of terrible leadership at the very top. On December 18, Secretary of State Mike Pompeo stated during a public interview, and I quote, "This was a very significant effort, and I think it's the case that now we can say pretty clearly that it was the Russians that engaged in this activity." Yet the very next day, President Trump tweeted this, and I quote, "The cyber hack is far greater in the fake news media than in actuality."

So, what can we do now? First, I am pleased the Biden Administration has taken early steps to elevate the importance of cybersecurity and supply chain risk. Our committee plans to focus on Federal procurement. The government pays hundreds of billions of dollars for goods and services each year. We must demand better cybersecurity practices from our suppliers as well as increased information sharing with the private sector as a product of the contract

agreement. Finally, the Oversight Committee plans to closely review agency roles, responsibilities, and strategy under the Federal Information Security Modernization Act, known as FISMA, to meet the complex and dynamic cybersecurity landscape of today. Much work needs to be done. Today and in the weeks and months ahead, we will focus on the facts with an eye toward legislative solutions in how we can improve cyber defenses across both the public and private sectors.

With that, I now recognize the distinguished ranking member, Mr. Comer, for his opening statement.

Mr. COMER [continuing]. Thanking the chairwoman for having this hearing. Last year, our Federal Government was hacked in the largest cyberattack in history. Some of the largest technology companies in the country were also hacked. The cyberattack took months of planning. It took extreme patience to execute. According to all the experts, it was incredibly sophisticated. The attackers covered their steps so they would not be detected, and it was wildly successful. According to one of our witnesses today, over 1,000 people were involved in the attack, and the likely culprit of the attack? Russia.

Three months after the attack was discovered, there is still a lot we don't know, and many government agencies and companies were hacked. We don't know what the extent of the damage is, whether or not the Russians still have access to the systems they hacked, or whether we have been able to successfully kick them out. You may not have heard about this attack because it hasn't affected your daily life. You still go home to a warm house every night, you can still flip on the television at night and watch TV, you can still facetime with your friends and family, but that is only because the attackers chose not to disrupt those activities. As far as we know, this attack was an espionage campaign, an intelligence-gathering operation only, but what the attackers have shown us is none of the software we use in our daily lives is truly safe. The apps we download on our phones, laptops, and tablets, any device, can be sabotaged.

Last week, we all prayed for millions of people in Texas as the power grid failed and they froze in their homes. Now, imagine if an adversary had the ability to take our electric grid offline in the dead of winter or the peak of summer. Now, imagine if this took place during a national crisis. Imagine if an adversary wanted to toy with our financial markets. Imagine if an adversary had the ability to control supply chains and manipulate whatever they wanted. It doesn't take much to realize the horror that would ensue if an adversary were motivated to do any of these things.

The attackers did not take down our electric grid, poison our water, or cause chaos in our financial system, among other necessities or occurrences of our daily lives. At least this time they didn't, but that is not to say they couldn't have. The truth is this attack is still ongoing even today and has not been completely neutralized. This offers the potential for unforeseen additional damage. The fact the attackers did not do these things that received the attention of Americans going about their everyday lives says nothing of their capabilities to do so the next time. This isn't the first-ever attack of this kind, nor will it be the last. For far too long, cyberse-

curity has been addressed as the mere cost of doing business, an add-on, a minor line item to simply check the box. This mindset must end.

No one, including Congress, the Administration, or the private sector can afford to allow this moment pass without ensuring we finally adopt effective solutions. I appreciate this opportunity to review what happened in this massive cyberattack that one of our witnesses referred to as the largest ever, and to play a part in developing a game plan for deterring and responding to any future event. I am convinced, though, that cybersecurity must not be left to the recesses of academic debate or half-hearted compliance, but, instead, it must become a daily focus for all involved in software development, procurement, and operations.

Just contemplate for a moment this particular attack. Companies, which many expect to secure their systems with topnotch cybersecurity, were the very ones who failed to identify the attack before damage had already occurred. Some of those organizations are here today. The same goes for our government agencies who glaringly missed the adversary's nearly year-long presence freely roaming about in our most sensitive network. I believe the time has come to take concrete action to actively defend our Nation from foreign cyberattacks just as forcefully and with the same resources as we would if the instrument of attack were physical or kinetic. We don't sit back when our country is physically breached or our homes and places of business are invaded, and neither should our responses be to roll over following an attack in cyberspace.

It is only a matter of time or chance until we are faced with real disruption and destruction. We must do everything in our power to defend this digital sphere and forecast to our adversaries that we at least are no longer asleep at the wheel. I yield back.

Chairwoman MALONEY. Chairman Thompson. I now recognize Chairman Thompson for his opening statement.

Mr. THOMPSON. Thank you very much. Good morning. I would like to thank Chairwoman Maloney for holding today's joint hearing on the SolarWinds breach and the related malicious cybercampaign. Just over two months ago, we learned that a state actor, likely Russia, had engaged in a large-scale cybercampaign, infiltrating government and private sector networks and burrowing inside them. By the time FireEye voluntarily shared information about the breach of its network, Russian actors had established a presence on victims' network, undetected for nearly a year. That is hardly comforting. While the campaign is notable for its patience, assistance, scope, and scale, the methods and tools used, though sophisticated, are not entirely new.

NotPetya, a 2017 destructive supply chain attack with a global impact, involved Russian actors compromising Ukrainian tax preparation software to access victims' network. That same year, security researchers published their findings regarding an attack vector using forged SAML tokens. Nonetheless, the Federal Government and the private sector were caught flat footed. I do not mean to diminish the complexity of the attack or to suggest we could have prevented it, but I want to make a point that our collective failure to make cybersecurity a central component of our national security and invest in it accordingly contributed to the success of the cam-

paign and the difficulty we face in understanding its impact. In short, past warnings of what could come failed to trigger a meaningful shift in our approach to security.

My goal in our joint investigation is to move beyond admiring the complexities of this campaign and the challenges associated with stopping one like it and start charting a path forward. In the 15 years I have served on the Homeland Security Committee, one thing has become clear. We can't become so consumed by preventing the last attack that we are blind to the threats of the future. Instead, we must identify systematic opportunities to improve our ability to prevent, defend against, mitigate, and raise the cost of all malicious cyberactivity. Toward that end, I hope to identify a combination of next-term fixes and longer-term structural solutions that will improve our ability to better understand the adversary, defend our networks, and identify attacks more quickly.

None of the witnesses here today can have a conversation with me or with the Cybersecurity and Infrastructure Security Agency about malicious activity occurring on an agency network because of restrictions agencies add in their contracts. That unnecessarily complicates our oversight work, limits situational awareness, and slows recovery. I believe that is a problem we can fix quickly. In recent days, I have been encouraged to learn of growing interest in enacting a cyber incident reporting log. Former chairman of the Cybersecurity Subcommittee, Cedric Richmond, authored an amendment included in the House-passed National Defense Authorization Act that would have established a cyber incident notification requirement. Unfortunately, we were unable to reach agreement with our Senate counterparts, but we look forward to trying again this year and hope we can enact cyber incident notification legislation in short order.

In the longer term, we must figure out how to make security a value proposition, not only for policymakers, but for investors in the private sector who are focused on earnings. We must address persistent challenges in threat information sharing and find more strategic ways to effectively leverage the unique capabilities of the government and the private sector in our shared goals of better security. In that vein, it may be time to reassess the obligation of large, highly-resourced companies with outsized footprints in our economy, in our government, and evaluate whether more should be expected of them. And we need to find ways to change behavior in the private sector, particularly those in the government supply chain, so executives value security as much as earnings statements and fast product rollout. I look forward to candid conversations about these issues today.

Before I close, I want to thank our witnesses for being here today. Since December, I have been impressed by the degree of transparency in their conversations with us. It is important to have a complete record of what happened, and how, so we can have a candid conversation about what needs to change. With that, I yield back the balance of my time.

Chairwoman MALONEY. I now recognize Ranking Member Katko for his opening statement.

Mr. KATKO. Chairwoman Maloney, and Chairman Thompson, and Ranking Member Comer, and all my other colleagues that are

with us today, this is a very important hearing. It is one of the most important threats facing our country today, cybersecurity, and it is important, I think, that we take a good look at the situation and learn from it.

As everyone in this hearing knows, we are in the midst of arguably the most devastating espionage campaign ever waged against our Nation. With each passing day, we learn more about the tactics, techniques, procedures, and unprecedented sophistication surrounding this campaign. While a number of details remain elusive, the overall picture is slowly coming together, and much of this incremental clarity is due to what we have learned from our private sector partners, so I appreciate their steady engagement in the whole-of-society response. I also recognize that we need more of this private sector sharing. I hope we can spend our time during this hearing evaluating the best paths forward. How can the cybersecurity community do more than just bounce back, but also bounce forward from these events?

From my vantage point, we know enough to identify initial lanes of policy responses that fall into five categories. First, we need to seriously rethink our fragmented approach to dot-gov security by centralizing authority with the Cybersecurity and Infrastructure Security Agency, known as CISA, wherever possible. While CISA's Federal hunt authority from the 2021 NDAA is a welcome step in the right direction, CISA still does not have the proper authorities, resources, or holistic visibility into the Federal networks enterprise to effectively defend and nimbly respond to attacks.

Second, we need to better understand the nature and extent of third-party cyber risks. With no disrespect at all to our witness, Mr. Ramakrishna, relatively few people had even heard of SolarWinds in early December 2020, yet its products are leveraged by most of the Fortune 500's, with a relationship between vendor and customer that inherently enables a high degree of administrative privilege on the host network. In this interconnected web of hardware, software, and services that underpin our way of life, there are concentrated sources of risk that could result in cascading or systemic impact if we assume there is a breach. We need to better illuminate answers to these questions.

Third, once we identify the potentially concentrated sources of cyber risk, we need to ensure that vendor certification processes actually reduce that risk, not create perfunctory compliance exercises. There are a number of vendor certification or risk of judgment regimes in various stages of operationalization right now across the Federal Government with DOD's Cybersecurity Maturity Model Certification, or CMMC, and the Federal Acquisition Security Council, or FASC, garnering the most headlines. Let's work together to ensure these regimes accomplish our common goal of actually reducing the risk.

Fourth, we need to drive better software assurance and development life cycle practices across the entire ecosystem. Whether software flaws are deliberate or not, the software supply chain represents an attack vector that, if exploited, leaves the potential for a digital pandemic of sorts, where the impact of one bad line of code can be felt across the entire country. Last, we must impose real costs on cyber adversaries like Russia, China, Iran, and North

Korea. While there is no silver bullet, deterrence still matters. Naming and shaming, indictments, sanctions, offensive measures where appropriate—these should all be tools in our toolkit and tools that we utilize. From the sophisticated nation-state-led incident to the more routine, such as ransomware, the cost-benefit analysis of cyber aggression still favors adversaries far too often. In short, they are winning the modern-day arms race, and we need to step up. I welcome the recent announcement by the Administration to begin to hold Russia accountable through sanctions. I hope those sanctions are real, I hope they are firm, and I hope they are severe.

I imagine we will hear a constructive dialog today about breach notification and incident reporting. An undeniable gap in our country's cybersecurity posture is the fact that there is not a consistent, overarching incentive for industry to disclose a breach. As a result, our Federal agencies are often operating in the dark instead of having access to the critical aggregate data regarding the tactics, techniques, and procedures of bad actors. As we move forward, we must consider approaches to close this gap. Whether that should be partnership based or compulsory or hybrid is yet to be seen, and I welcome robust private sector feedback on this issue.

These are all necessary and worthy policy conversations for our homeland security, but we must also not lose sight of the immediate needs to put necessary resources toward the Federal dot-gov SolarWinds response. I feel strongly that any executive branch actions related to SolarWinds must build upon and bolster CISA's mission as the lead Federal civilian cybersecurity agency, as I recently stated in a letter to President Biden.

I, again, want to thank our witnesses for testifying today. I look forward to hearing from you all on an issue of great bipartisan interest for the Nation. I yield back.

Chairwoman MALONEY. Now I will introduce our witnesses. Our first witness today is Sudhakar Ramakrishna, who is the current CEO of SolarWinds. Then we will hear from Kevin Thompson, who is the former CEO of SolarWinds. Next, we will hear from Kevin Mandia, who is the CEO of FireEye. Finally, we will hear from Brad Smith, who is the president of Microsoft. The witnesses will be unmuted so we can swear them in. Please raise your right hands.

Do you swear or affirm that the testimony you are about to give is the truth, the whole truth, so help you God?

[Chorus of ayes.]

Chairwoman MALONEY. Let the record show the witnesses answered in the affirmative. Thank you. And without objection, your written statements will be part of the record. With that, Mr. Ramakrishna, you are now recognized for your testimony.

STATEMENT OF SUDHAKAR RAMAKRISHNA, PRESIDENT AND CHIEF EXECUTIVE OFFICER, SOLARWINDS CORPORATION; ACCOMPANIED BY KEVIN B. THOMPSON, FORMER CHIEF EXECUTIVE OFFICER, SOLARWINDS CORPORATION

Mr. RAMAKRISHNA. Chairwoman Maloney, Chairman Thompson, Ranking Member Comer, and Ranking Member Katko, and members of the committee, on behalf of SolarWinds employees, cus-

tomers, and partners in the U.S. and around the world, I would first like to say thank you for inviting us to participate in your hearing today. By way of background, my name is Sudhakar Ramakrishna, and I joined SolarWinds as president and CEO on January 4 of this year. I was previously CEO of Pulse Secure and before that held other executive roles at technology companies. In these roles, I have had the experience of being involved in cyber incidents and seen firsthand the challenges they present as well as the opportunities for learnings and improvements.

Also joining me today is Kevin Thompson, who served as our president and CEO for 10 years until his departure on December 31, 2020, which he had previously announced in August 2020. Mr. Thompson cares very much for our customers and employees, and we appreciate his long service to the company. To aid in our investigation, he has agreed to serve as a special advisor to me and the board. He has had the opportunity to meet the staff of both of your committees to provide early insight into the event. While our products and customers were subject of this unfortunate and reckless attack, we take our obligations seriously to work tirelessly to understand it better, to help our customers, and to be transparent with our learnings.

SolarWinds started in 1999 in Oklahoma as a provider of network tools, and we have remained true to the mission of helping IT professionals solve problems and better manage IT environments, now through more than 90 products. Today, we remain a U.S.-headquartered company, and our 3,000 dedicated employees work hard every day to help customers succeed. When we learned of these attacks, our top priority was to ensure that our customers were safe and protected. Our teams have been working tirelessly to help our many customers first and foremost, while also investigating the what, who, and how of the attack. We acted quickly to disclose the attacks, provide remediations and support to our customers, and share our learnings publicly.

We believe our Orion platform was specifically targeted in this nation-state operation to create a backdoor into IT environments of select customers through versions that we released between March and June 2020. That is a three-month window. SUNBURST has been removed and is not an ongoing threat in Orion. Additionally, after extensive investigations, we have not found SUNBURST in any of our more than 70 non-Orion products. Perhaps the most significant finding of our investigations to date was the discovery of what the threat actor used to inject SUNBURST into the Orion platform. The injected tool, named SUNSPOT, poses a grave risk to automated supply chain attacks through many software development companies since the software build processes, like ours, are very common in the industry.

As part of our commitment to transparency, collaboration, and timely communications, we immediately informed our government partners and published our findings with the intention of helping other companies combat current and future attacks. We understand the gravity of the situation and are applying our learnings from the event and sharing this work more broadly. Internally, we are referring to our work as Secure by Design, and it is premised on zero-trust principles and developing a best-in-class secure soft-

ware development model to ensure our customers can have the utmost confidence in our solutions.

We have published details regarding our efforts, but, in summary, they are focused on three primary areas: first, further securing our internal environments; second, enhancing our product development environments; and third, ensuring the security and integrity of the products we deliver. Given our unique experience, we are committed to not only leading the way with respect to secure software development, but to share our learnings with the industry. While numerous experts have commented on the difficulties that these nation-state operations present for any company, we're embracing our responsibility to be an active participant in helping prevent these types of attacks. Everyone at SolarWinds is committed to doing so, and we value the trust and confidence our customers place in us.

Thank you again for your leadership in this very important topic. We appreciate the opportunity to share our experience and our learnings, and I look forward to addressing your questions. Thank you.

Mr. LYNCH. [Presiding.] Thank you, Mr. Ramakrishna, and because Mr. Thompson and Mr. Ramakrishna submitted joint testimony, Mr. Thompson is not providing oral testimony at this time. Therefore, we are going to move on to Mr. Mandia. Mr. Mandia, you are now recognized for your five minutes of testimony.

STATEMENT OF KEVIN MANDIA, CHIEF EXECUTIVE OFFICER, FIREEYE, INC.

Mr. MANDIA. Thank you. I would like to thank Chairwoman Maloney, Ranking Member Comer, Chairman Thompson, and Ranking Member Katko for this opportunity, and I am excited to share my observations with you, a first-hand account of what took place at FireEye and at many of these other victims. So, I am going to share what happened to most of the victim organizations, and I know Mr. Smith's going next. He's going to talk a lot more about what to do about it, and though I have opinions about who did it and what to do about it, I'll reserve those for the moment when we get questions.

I want to set a little bit of background first about what FireEye does, and it is just to provide context. Responding to breaches is what we do for a living. So, when we ourselves were breached based on having a SolarWinds implant, we put nearly 100 people on the job, and the majority of the folks working it, figuring out what happened and what to do about it, did their proverbial 10,000 hours of computer forensics on intrusions. And as I'm sitting here talking to these committees, we're responding to over 150 security breaches, and in 2020, a tough year for chief information security officers, we responded to nearly 1,000 security breaches globally. So, we're a company that every time we respond, we're the detectives, and we take the trace evidence of every single breach that we have firsthand experience of, and we put in a data base and track it. So, with that, let me talk about the anatomy of this intrusion.

First and foremost, everybody's calling it the SolarWinds hack. In reality, this is an ongoing saga. The group that did the com-

promise that led to 100 different organizations compromised and nine government agencies compromised is not new to the game. These are folks that are special operations. And think of it as, if you're an organization and you've locked your doors and locked your windows, this is the special ops robbing the house, not some average criminal just trying to shake the doorknobs or trying to crack open the windows. So, this was the varsity team on offense, and all the signs, all the digital fingerprints that our company cataloged proves that, that this was a foreign intelligence service.

So, stepping through the anatomy of this intrusion, I look at it in two stages. Stage one, the attacker had to break into SolarWinds, and when they did that, you already heard the details from Mr. Ramakrishna that the attackers did something that's pretty darn hard to detect. At the very end of a build process, they altered the production environment. So, this isn't somebody hacking in and changing source code. They're hacking the build process, and when you go to build your production code, it is altered at the last minute. In this case, to provide the timeline, the attackers that broke into SolarWinds for this stage one of this whole campaign, the first thing they did, they got the implant in, but the implant was innocuous, and there's evidence that in October 2019, the threat actors put the innocuous code in simply to test, "Do we have a way to get into the supply chain?" After the attacker proved that they could get their arbitrary code into production, then they created, by March 2020, an implant that provided surreptitious access to anyone who updated their networks with the next SolarWinds update to the Orion platform.

So, how did we find this implant at FireEye? We found it based on literally exhausting every single other investigative lead at FireEye. We had detected some unusual activity on our network, and when we investigated that and started pulling the thread, the earliest evidence of compromise kept going back to a SolarWinds server. And the reason I am sharing this story with you is there is no magic wand on finding an implant. People trust the third-party software that they buy, rely on, and install. In this case, because we do forensics for a living, special operations attacked us. It would take special operations, people that are in the trenches responding to breaches every day, to detect it. We had to reverse over 18,000 files that were in the SolarWinds platform; 3,500 of those files were executables. We de-compiled them into a million lines, and with people that can read assembly language and understand it, they are the ones that found the implant, and that's why this was so hard to detect. So, that's the stage one of this breach.

Stage two I'll cover very quickly because after stage one, the attackers had a menu of over 17,000 companies that had downloaded the implant, but that doesn't mean the attacker stole anything from 17,000 companies. The stage-two victims are where the attacker decided, "I want something," and the attackers manually engaged with about 100 different organizations. In stage two, the attackers did three things: first, steal your keys. They came in through the trap door in the basement that you didn't know about. They took your keys, and with those keys, they accessed your information the same way people and employees do. Second thing they did is they did very specific and focused targeting of documents and

emails. And the third thing these attackers did, I put in the "other" category based on the victim. They stole source code or software, and in the case of FireEye, they stole assessment tools that we use to assess the security of organizations.

So, with that level of detail, I'd like to thank the committee for this opportunity. We stand ready to work with you and work with the companies in the private sector to defend the Nation. Thank you.

Mr. LYNCH. Thank you very much. That is very helpful testimony, Mr. Mandia. We appreciate it. Mr. Smith, you are now recognized for your testimony for five minutes. Thank you.

STATEMENT OF BRAD SMITH, PRESIDENT AND CHIEF LEGAL OFFICER, MICROSOFT CORPORATION

Mr. SMITH. Well, thank you, and I want to thank Chairwoman Maloney, Chairman Thompson, Ranking Member Comer, Ranking Member Katko, and really all the members of the two committees.

I think Sudhakar and Kevin have done an excellent job of describing a lot of what happened, and no doubt we'll get into more of that. I thought I would, as Kevin suggested, build on what the two of them said and talk a little bit about what is it that we can do. What is it that the private sector can do? What is it that all of us can do by working together? I think there are a number of concrete steps, and some of the opening comments, I thought, did an excellent job of identifying, as it was said, many of the lanes down which we need to travel. As Sudhakar said, this was an attack on the software supply chain, and by that, he meant it planted malware into a software update. I think that points to one of the first things we need to focus on securing, more broadly, across the software ecosystem.

The International Data Corporation has estimated that as many as a half a billion software apps will be created in the next three years globally. Well, all of these applications will be distributed. They'll need to be updated. I think we all have work to do. Certainly at Microsoft we look forward to working with others on what we can do to help secure the software supply chain and avoid this kind of risk, this kind of problem, this kind of tampering with software updates. That is a very specific activity.

I think the second thing we need to do is think much more broadly. We need to focus on the modernization of the information technology infrastructure, and we need to apply, more broadly, cybersecurity best practices. We've looked at the customers that use Microsoft software that we were able to identify had been hacked in this incident, and what we have found repeatedly is that they could've better protected themselves simply by applying the many cybersecurity best practices the world has recognized already, that we've encouraged customers to apply already. And I think this is an important day for us to step back and think again about how we better help small businesses, as well as large customers, to apply these best practices.

I think that leads us to a third opportunity for us all to do better. When we ask ourselves why the world is not using all of the cybersecurity best practices that exist today, I think one of the reasons becomes self-evident. It's because in the United States and around

the world, there is a shortage of trained cybersecurity personnel. In the United States today, there's a shortage of more than 300,000 trained cybersecurity personnel, and this is something that we, a tech company like Microsoft, can focus on addressing by helping colleges and universities, high schools, and others develop the people we'll need in the future. But I think there's an important role for government to play as well.

The fourth area where I think we can do better, where we really need to do better, is to share threat intelligence information to ensure that when there is information about this kind of hack or attack, it is being shared first with customers, something that we do immediately when we detect this kind of hack at a Microsoft customer, but something that doesn't happen broadly enough across our industry, and we can share it with the government. It needs to be, I think, better shared across the government and then in appropriate ways back with the private sector itself.

Fifth, I think the time has come to adopt a national law that will impose cyberbreach incident reporting obligations, and there are important questions to be considered. To whom should it apply? When should it apply? How should it be administered? To whom should the information go? How should that information be shared? These are all questions for your two committees and the Congress as a whole, but 2021, I believe, needs to be the year that Congress acts and we use this step to strengthen the security of the Nation.

Finally, I think we need to strengthen the international rules of the road. What happened here is and should be a violation of international norms and international law. It is the kind of act that was reckless. It is the kind of act that needs to have consequences, and those consequences need to be based on global standards. This is a combination of six steps that we can take, steps that I believe will make us stronger. Thank you.

Mr. LYNCH. Thank you, Mr. Smith. Now I would like to recognize my friend, the gentleman from Mississippi, Chairman Thompson, for five minutes for questions.

Mr. THOMPSON. Thank you very much, Mr. Chairman. I thank the witnesses for their very important testimony. This is to Mr. Thompson and Mr. Ramakrishna. A theme emerging this week is that the supply chain compromise that exploited the SolarWinds Orion platform could have happened to anyone, but since December, I have read troubling accounts about the security culture at SolarWinds. One report indicated your server password was "SolarWinds123." Now, according to another report, a former employee raised concerns about the security culture at SolarWinds four years ago. As you know, we have recently obtained testimony from that employee during a presentation. So, Mr. Thompson, did you take any action based on the security recommendation that this employee, Mr. Trump, made to the company?

Mr. THOMPSON. So, I believe that we have, over the history of time at SolarWinds, taken security seriously, security of our internal systems and the secure development of our products. Mr. Trump arrived in the company April 2017. Shortly after that, we actually hired Tim Brown, who is a 30-year veteran from Dell who was a fellow at Dell, which is one of their highest-ranking engineers, to be in charge of not only the internal security of

SolarWinds, but also product security at SolarWinds. We also actually did hire Mr. Trump back in September 2017 as part of some of the initiatives that we were working on. So, I believe we have taken security seriously in 2017, and really beginning in 2016, we enhanced our security posture.

We hired a CTO in 2016 who had been a CIO at a large global Fortune 500 company. We hired a very experienced CIO in 2017. As I said, we hired Tim Brown in the middle of 2017, who is a very experienced VP of security. We also implemented a——

Mr. THOMPSON. Thank you. Thank you. Thank you very much. So, your testimony is that, based on that recommendation, you did do things. So, Mr. Smith, you talked about the challenges facing companies, like all of the cyber companies that we have talked about. One you talked about, the challenge of a work force. You know, our committees are constantly being requested by many of the companies on the screen to expand the visa programs so that we can import labor supply because we don't have it here. So, tell me what a company like Microsoft is doing with historically black colleges and minority-serving institutions to help that labor force be developed right here in this country.

Mr. SMITH. Well, thank you, Chairman Thompson. I think it is a very important question. You know, so far, just this year, Microsoft has spent more than $2 million to provide grants to faculty members at HBCUs to add cybersecurity and other information technology curriculum to, you know, the courses that are offered at these institutions. We are going to be increasing that amount to $3.2 million per year. We are going to be spending that each of the next three years.

But it is not just, I think, investing in these institutions so that they can train the next generation of professionals. We are very focused on hiring individuals at HBCUs. Our recruiting season is still unfolding this year, but already we have had recruiters at 27 HBCUs. We are excited that already 136 students at these institutions have accepted jobs to work at Microsoft, 73 full time, 63 to be with us as interns this coming summer. I do believe that the HBCUs are growing and powerful engines for the protection of cybersecurity. We can collectively, I think, as an industry add to their strength, and we will be the beneficiary of the students that they will graduate.

Mr. THOMPSON. Thank you very much. This notion of a cyber breach info office, I take from your testimony, as you know, we tried to get it passed last year, and it was taken out in the Senate. So, your testimony to both committees is that that would be an important instrument for us to have to get in-time notification of breaches.

Mr. SMITH. Yes, that's correct. I think we do need to take that type of step. There will be important details that need to be discussed, but this is the time to take that kind of action.

Mr. THOMPSON. Thank you very much. I yield back, Mr. Chairman.

Mr. LYNCH. The gentleman yields back. The chair now recognizes the gentleman from New York, Ranking Member Mr. Katko. You are now recognized for five minutes.

Mr. KATKO. Thank you, Mr. Chairman, and I want to thank all the witnesses for their very thoughtful and engaging testimony. I am really heartened that your comments are consistent with and supportive of the five categories of response that I laid out in my opening statement, and I want to explore those a little bit more if I can.

First of all, with Mr. Mandia, earlier this week, you outlined, Mr. Mandia, some of the enormous time and costs that go into the threat-hunting and intrusion-remediation services. Can you describe briefly for me, just briefly, the magnitude of the resources that go into these threat-hunting teams and penetration-testing services, how much they cost, the man hours, woman hours that go into it, things like that briefly?

Mr. MANDIA. You know, sir—thank you for the question—I don't think it takes a lot of people to test your networks on how secure they are, and I do believe that is the best way to get unvarnished truth in security. Kind of like you do crash test dummies to test the safety of a vehicle, shoot real bullets at a bulletproof vest to determine how effective it is, in cybersecurity you need to test your security, and that is a couple folks. There is a great asymmetry between offense and defense. To have somebody perpetrate what would be perceived as offense, not a lot of resources.

The problem is the 52-card pickup you play on the other side because of that asymmetry. One attacker can create work for hundreds of thousands of defenders. It is a bad asymmetry in cyberspace I think other nations have picked up on where they can't beat us with tanks, won't beat us with planes, but in the cyber domain, if they train folks, the A-team can create work for potentially millions of defenders. So, the bottom line, that asymmetry is the problem. It is hard to answer your question without cataloging the offense, very few people. Defense, you have to pitch a perfect game every day and put a lot more people on it.

Mr. KATKO. Got it. Thank you for that. And to followup on that, as you know, CISA was granted authority in the Fiscal Year 2021 NDAA to conduct threat hunting on Federal agency networks——

Mr. MANDIA. Mm-hmm.

Mr. KATKO [continuing]. With or without consent, which is, I think, a very positive step forward. Do you have recommendations on how CISA can most effectively implement this new authority?

Mr. MANDIA. Well, I am convinced this will work with the private sector on that. We all have threat-hunting teams. My company does it every single day all the time for thousands of customers. Microsoft has a team that does it. There are a lot of security folks that do threat hunting, and the reason we have to do threat hunting is not every product stops everything, period. There is no such thing as perfect security, so you have to have the catcher's mitt behind your products. And CISA's folks that do threat hunting will be able to tap the private sector and be driven by the private sector, so I think it is exactly the right thing to do.

Mr. KATKO. Mr. Smith, I am going to followup on something Chairman Thompson said, and I am in complete agreement with him that the information sharing is such a critical component. But the problem with the information sharing is if a company is hacked into and they share the information, are they buying themselves

more problems and more public scrutiny and perhaps more liability if they do the right thing and share that information with CISA? So, what role do you see CISA as a hub for a Federal focal point to help aggregate all this national risk picture across the sectors, right, No. 1? And No. 2, how do you do so in a way that protects the industry and incentivizes the industry to share this information instead of just not sharing it because they are afraid of opening Pandora's box and problems for them?

Mr. SMITH. Well, first of all, I think you make a really important point. The White House said a week ago that more than 100 companies, or roughly 100 companies, in the United States had suffered this kind of attack or hack. You have three companies here today, and that is because we have chosen to speak up, and what you get is an invitation to appear as a witness under oath at a House hearing. And so I think a lot of companies choose to say as little as possible, and often that is nothing.

But silence is not going to make this country stronger, and so I think we have to encourage and, I think, even mandate that certain companies do this kind of reporting. I think we do need to identify the right place where the report should go. CISA is a very strong candidate, and it deserves serious consideration, and we need to think about the process and the type of information that should be shared and when it should be shared. And we need to be very careful that we don't, in effect, tell firefighters to stop fighting the fire so they can fill out forms and, you know, meet with government officials instead. So, we need to balance all of the work that needs to be done, but Kevin really captured well the asymmetry, and we can only be effective if we can connect the dots in everything that we see. That can only be done with this kind of effective information sharing.

Mr. KATKO. Well, it is not often that you hear the private sector saying they need more government mandates, so that, I think, highlights the importance and the magnitude of this problem. And I think Chairman Thompson, and I, and the others are going to work very hard to try and make this a reality because information sharing is what made us a much safer nation after 9/11 with the Joint Terrorism Task Forces. We need to do the same thing in the cyber area, and anything we can do to turbocharge that process, we have to do going forward. I have so many more questions, but I am out of time and I yield back. Thank you.

Mr. LYNCH. The gentleman yields back. The chair now recognizes the gentlewoman from the District of Columbia. Ms. Norton, you are now recognized for five minutes.

Ms. NORTON. I thank the gentleman for yielding. This is an important hearing, and we have heard of breaches of both the private and the governmental sectors. It is kind of a two-fisted breach. My first question is for Mr. Mandia of FireEye. Our most recent information from the current White House, I do believe these breaches occurred in the last Administration, but it is clear that it could occur and may be occurring right now. So, let me ask about the breaches or the impact on government agencies in particular.

For example, the information I have been given is that the breaches included the Department of Energy, including a component responsible for managing the Nation's nuclear weapons. You

can see the issue there, Mr. Mandia. Another agency was the Department of Justice, of course, which enforces our laws, but breached also, but also has to do with countering foreign intelligence on the United States. Also breached, of course, was the Department of Treasury. Now, that Department maintains the Nation's financial infrastructure and imposes financial sanctions on our adversaries. You can see, Mr. Mandia, what this leaves us open to. Would you agree that compromising any one of these agencies would be considered a victory for an adversary?

Mr. MANDIA. Well, I think the first comment I would say is this is an ongoing intrusion set. The SolarWinds backdoor was just part of a very long saga. I first started responding to breaches for the U.S. Government in the 1990's. This group was active then. They are going to be active tomorrow. There is going to be ongoing targeting of those agencies. This intrusion set using the SolarWinds backdoor happened to be successful at least for surreptitious access and staying surreptitious and clandestine on the networks for a certain period of time. You know, we will respond to it, and it will take those agencies time, months, to get their arms around the scale and scope of what happened. And I think we are in that window where they don't know yet, and we got to wait on the final investigation.

Ms. NORTON. Well, we certainly need the investigation to be finalized because we are still in the window and they are still being breached. That raises continuing problems for us. And continuing with you, Mr. Mandia, in 2015, a foreign actor or groups compromised the systems of the Office of Personnel Management. They accessed clearance information on 21 million people. Now, that was only one agency. Mr. Mandia, would the OPM compromise be considered a serious breach?

Mr. MANDIA. I think you have to consider it a serious breach. When you look at these breaches, what generally happens is there is a successful breach. We find out about it. We take steps and do sprints within the Federal Government to try to escalate our security programs. The bottom line, there are threat actors out there that attack the U.S. Government on a daily basis, and they are feeling no risk or repercussions to doing it. So, we are just sitting here playing defense every day against an A-team that is going to have successes.

Ms. NORTON. Yes. This time around, these actors were able to compromise up to 3 percent of Microsoft Office email accounts at the Department of Justice. Again, that sounds like a small number until you put it in perspective. Three percent of email accounts at the Department of Justice translates into roughly 3,500 accounts. Mr. Mandia, if you were writing up a damage assessment for a customer and they had 3,500 accounts compromised for months, how would you categorize that? Would it be sincere even what seems to be a small number? How would you categorize that?

Mr. MANDIA. Well, this is obviously a group that compromised with collection requirements, so the damage assessment is going to be based on the content of the emails, period. And how that information is intended to be used, we don't know. That is the problem. We have to get our arms around all the content and all the potential use and misuse of all that content. So, the bottom line, we may

never know the full range and extent of damage, and we may never know the full range and extent as to how the stolen information is benefiting an adversary.

Ms. NORTON. Well, we better get our arms around the full impact of these breaches, but we know that it has very serious implications for both the government—that is why I focused on Federal agencies—as well as the bottom sector. You have given us a mandate in this committee to get to the bottom of how this breach occurred, every entity that was affected, and how to protect against this type of incident in the future, and it looks like we have a lot of work to do. I yield back.

Mr. LYNCH. The gentlelady yields back. The chair now recognizes the gentleman from Georgia, Mr. Hice, for five minutes.

Mr. HICE. Thank you very much, Mr. Chairman. I appreciate it and appreciate this hearing. As ranking member of Gov Ops, it has been honor working with Chairman Connolly on these issues over and over in the past trying to improve our government-wide information security. And, of course, we both know, and I am sure everyone on both of these committees, in fact, everyone involved in this hearing right now is keenly aware of the importance of cybersecurity, the vital nature that it provides for our government, and to make sure, frankly, that our government continues to run efficiently and effectively, and, most importantly, in this context, securely. I am certainly looking forward, in that light, to the upcoming FITARA hearing on the FITARA scorecard that Chairman Connolly is going to be bringing up, and hopefully we will be able to discover the level of preparedness of various agencies within our government.

But in light of the massive attack, the cyberattack that brings us to this hearing today, these efforts around Federal information security are obviously extremely important and all the more prescient for us. And I understand, I get it, and I think it is probably good that our witnesses today are from the private sector. They certainly are able to bring some valuable insight to us today as to what and how we can best secure our IT assets in Federal Government.

So, Mr. Mandia, let me begin with you. Beginning with your company's focus on cybersecurity services, I am wondering your opinion in regard to cloud migration, and, in particular, what I am talking about, or what at least I have in mind, is Chairman Connolly's bill, FEDRAMP, which both myself and Ranking Member Comer have both co-sponsored. But how do you view that in terms of is it a step in the right direction for improving cybersecurity?

Mr. MANDIA. Sir, first off, the migration cloud is going to happen whether we want it or not. It is rare in history where something costs less and is better. Cloud is actually costing less and is better. For example, if I wanted a server set up at FireEye, I could ask an IT staff to do it, or I can go to an infrastructure as a service provider and get it in five seconds. So, the cloud is coming. And then you add the pandemic to it and the work from home. All the major enterprises, all the major organizations are going to the cloud.

The upside is it cuts both ways, but you should get better visibility and better controls in the cloud, and the reason why is you

are putting all your decentralized IP and value into one place. It is easier to monitor it, easier to safeguard it. You don't have distributed security controls at that point. I think we are in the middle of the cloud migration, but over time, what we will see is organizations recognizing at least the infrastructure portion of the cloud will be more secure because these companies have to secure it, meaning the providers have to secure it.

Mr. HICE. OK. OK. So, when you say, "Whether we like it or not, it is going to happen," I get that.

Mr. MANDIA. It is going to happen.

Mr. HICE. And you are exactly right. But with it happening whether we like it or not, do you feel good that that is indeed a safe method? Is that good for us to go there that way?

Mr. MANDIA. Sir, after 30 years in IT security, I believe it will be easier to secure the cloud than the last 30 years of us trying to secure everybody's home offices and secure inside four different walls all over the place. Yes, it is a good move.

Mr. HICE. OK. Mr. Chairman, for whatever reason, the clock is not showing up on my screen, so I really don't know where I am on time, but if there is time, if I could have a brief answer from each of our——

Mr. LYNCH. The gentleman has 45 seconds.

Mr. HICE. OK. Well, each of the witnesses real briefly, what needs to be done? What does the private sector have that we could use? If you can just give a 10-second answer, each of you, or whatever, just very briefly. I will start with Mr. Smith.

Mr. SMITH [continuing]. The cloud, but then implement the cybersecurity best practices that are needed to use it effectively. As a cloud services provider, we can enable all of the tools, but ultimately, it is our customers that will have to decide how to use them.

Mr. HICE. Thank you.

Mr. RAMAKRISHNA. Congressman Hice, my recommendation would be to share information as fast as possible in as timely a manner as possible because speed and agility are key to addressing these issues.

Mr. HICE. Thank you, sir.

Mr. MANDIA. And, sir, in the last 12 seconds, I will get to what Congressman Katko was referring to. I believe we need to separate disclosure of a breach to sharing of threat intelligence. If you can share threat intelligence from the private sector to the government, or government to the private sector confidentially, you can do it quickly without worrying about all the liabilities that come with public disclosure of a breach. So, we got to think of threat intel sharing and disclosure of a breach as two separate things, and threat intelligence sharing will defend the Nation.

Mr. HICE. Very good. Thanks to each of you, and thank you, Mr. Chairman. I yield back.

Mr. LYNCH. The gentleman yields back. The chair now takes great pleasure to recognize someone who has done yeoman's work in this area for a long time. The gentleman from Rhode Island, Mr. Langevin, is now recognized for five minutes.

Mr. LANGEVIN. Thank you, Mr. Chairman, and I thank you for your leadership on cyber.

Mr. LYNCH. I believe the gentleman may have muted himself.

Mr. LANGEVIN. Yes, I think——

Mr. LYNCH. OK. Go ahead.

Mr. LANGEVIN. Thank you, Mr. Chairman. Again, I was saying I appreciate your leadership on cyber and data, the chairs of the two committees that are holding this joint hearing today and the ranking members. It is obviously a very important topic, and I want to thank our witnesses for being here this morning.

Let me start with Mr. Smith, if I could. Mr. Smith, you have testified that Microsoft is aware of 60 victim organizations; that is to say, organizations where at least one Office 365 email account hosted in Microsoft's Cloud was accessed by the adversary. But how many accounts has Microsoft confirmed were accessed?

Mr. SMITH. I would have to get you the precise number of accounts. I will say, in general, the pattern that we saw was typically a relatively small or very small number of accounts per customer. I think that was indicative of the stealthy practices that this actor tends to deploy, namely, to take great care to be very discreet. And so I think——

Mr. LANGEVIN. OK. Yes, if I could just stop you. Let me just say my time is limited. In conversations with staff yesterday, Microsoft indicated that about 77 accounts had been confirmed to have been accessed. Does that sound about right?

Mr. SMITH. It certainly sounds like it is in the right range. Again, I would want to go check the specifics, but it sounds like it is in the right range.

Mr. LANGEVIN. All right. That sounds like a just incredibly small number to me. All right. If I could, just in CISA's alert detecting post-compromised threat activity in Microsoft cloud environments, they note that the amount of security log data in cloud environments is often significantly less than in on-premises environments, which can hamper threat hunting. In fact, the same alert notes that in order to detect certain accounts that have been compromised, a special, more expensive Office 365 account or G5 or E5 license is required. Do you believe that security should be an add-on or up charge or baked into cloud accounts from the get-go?

Mr. SMITH. Well, the particular offer that you described, what we call as E5, you know, is the service that we offer that includes security and other advanced features. We offer a range of choices to our customers. E5 is absolutely what we hope and expect and recommend that our customers purchase. Some people don't want to buy it, and we honor that, but it is absolutely what we encourage.

Mr. LANGEVIN. All right. Just so that I understand and the committee understands, is this a profit center for Microsoft for this, or are the services being provided at cost that you are charging the customers?

Mr. SMITH. Well, you know, we are a for-profit company. Everything that we do is designed to generate a return other than our philanthropic work.

Mr. LANGEVIN. OK. Thank you, Mr. Smith. Mr. Ramakrishna, if I could turn to you. Can you shed some light on how the adversary initially accessed SolarWinds' network? On Tuesday, you testified before the Senate Intelligence Committee that your partners had

narrowed the number of possible vectors to three. What are those vectors?

Mr. RAMAKRISHNA. Congressman Langevin, thank you for the question. Our investigation was segmented as to what exactly happened, how did it happen, and who may have done it. As it relates to the what, we have made a lot of progress and have discovered the specific injector tool that I described could affect any supply chain, and we have been able to publish it such that other companies can evaluate their security postures and supply chains and possibly get help from our efforts.

As it relates to your question, we have narrowed it from several hypotheses. At one time, we had 15 different threads that we were pulling, so to speak, and we have battled it since to about three at this point. One is what I call a classic password spring type approach that we are investigating. Two is some form of credential theft. That can happen through various methods. And three is a potential vulnerability in a third-party software that we have deployed on premises. Just like other companies on this witness stand, we use a lot of third-party software as well, and we are looking at it in those three dimensions at this point. We are evaluating several terabytes of data to be able to sift through this in the hopes that we can pinpoint patient zero in this context.

Mr. LANGEVIN. OK. Thank you, Mr. Ramakrishna and Mr. Smith, to our witnesses. I just wanted to note for the record, Mr. Chairman, I know my time has expired, but I want to thank Mr. Ramakrishna for briefing me about a week ago, and I appreciate how they have been very forthcoming in helping us to get our arms around this. And to Mr. Smith, your team had briefed me a couple days ago, and I appreciate them taking some detailed questions there, too. So, thank our witnesses, and, Mr. Chairman, I yield back.

Mr. LYNCH. The gentleman yields back. The chair now recognizes the gentleman from Texas, Mr. McCaul, for five minutes.

Mr. MCCAUL. Well, thank you, Mr. Chairman. You know, I have worked on cybersecurity for very many years along with Mr. Langevin. And back when I was chairman of the Homeland Security Committee, we authorized, stood up into law CISA to be the lead civilian agency to protect our networks, and then we had the cyber incident response teams that were authorized into law. You know, 80 percent of this critical infrastructure is done in the private sector as is most of the threat information, and that is why these private/public partnerships, I believe, are so important.

I have had the opportunity to visit with Mr. Ramakrishna. SolarWinds is actually in my district in Austin, and also with Mr. Smith from Microsoft, but I want to just get a couple of just factual details on the event itself. And, Mr. Ramakrishna, I also want to thank you for being so forthcoming and transparent with the Federal Government, but do you think the initial intrusion began around, say, March of last year?

Mr. RAMAKRISHNA. Congressman McCaul, thank you for the question. March of last year is when we first shipped, so to speak, the code with the malware injected in it, so three releases between March 2020 and June 2020 is when the malware was impacting the Orion platform.

Mr. MCCAUL. So, between March and June you have the intrusion. It is detected in December 2020. Is that correct?

Mr. RAMAKRISHNA. Yes.

Mr. MCCAUL. So, this is very sophisticated malware that can, as I understand, can go in and out of your system through the in-door and through the backdoor without detection. Is that correct?

Mr. RAMAKRISHNA. So, that threat actor I would describe, Congressman McCaul, as hiding in plain sight.

Mr. MCCAUL. Mm-hmm.

Mr. RAMAKRISHNA. They were very, very careful about covering their tracks, cleaning up after themselves, and the patience with which they worked was not similar to the run-of-the-mill virus whose job is to spread as fast as possible and create as much damage as possible. This was very sophisticated. And, as you heard from Mr. Smith and Mr. Mandia, being in the security business, it still took them a long time, and in talking to Mr. Mandia, they looked at this as almost a last resort in their investigation.

Mr. MCCAUL. I am sorry, but my time is limited. So, when it was detected in December, within two days Microsoft developed and created the kill switch. Is that correct?

Mr. RAMAKRISHNA. That is true, and within a matter of 72 hours, our teams fixed the malware and delivered remediated code. And since then, we have pretty much had a 7 by 24 operation——

Mr. MCCAUL [continuing]. Report it to CISA and the Federal Government? At what time?

Mr. RAMAKRISHNA. We reported it as soon as we knew on December 12 to CISA and the Federal Government, and we continue to do so.

Mr. MCCAUL. We believe that this originated out of Russia. Would you agree with that assessment?

Mr. RAMAKRISHNA. Congressman, we do not have the internal expertise to create attribution, but based on our investigation partners, it appears to be true.

Mr. MCCAUL. So, this is for both you and Brad Smith. What is the extent of the damage, to your knowledge, and if it came from Russia, which I believe it did, by looking at what they stole, it didn't seem to be a destructive virus, but more of a theft and espionage type of malware. What was their motivation and intent here?

Mr. SMITH. Well, I would say that, based on every indication so far, there were probably two or three. One is espionage, obviously to obtain information, especially, say, from the U.S. Government and other agencies. Second, to learn more about technology because obviously technology is the plane on which this organization's activities take place. That is why 50 percent of the victims that we identified are communications and technology companies. Third, I think there is an aspect of this that you would almost put in the context of counterintelligence. They focus on red team tools so that they know how to withstand attacks. They look for whether a company like Microsoft may be knowing about them so that they are able to try to circumvent what we are doing in the future. That is true for other tech companies as well.

Mr. MCCAUL. Now, I applaud you for transparency, the kill switch, and the notification, but not all companies do this. And Mr. Langevin and I are working on a mandatory notifications breach of

any cyber intrusions. This can be done by taking sources and methods and company names out to protect them as you have a duty to shareholders. It would just simply send the threat information itself to CISA so they could provide both industry-wide, and Federal-governmentwide, and state the threat information that they would need to address it on a larger scale. Is that something you think would be a good solution?

Mr. SMITH. I think that would be an important step. I think the time has come to recognize that it is probably an essential step, and I think the precise tailoring, something along the lines of what you just described, is exactly the kind of conversation we need to have.

Mr. MCCAUL. Well, I appreciate that, and I thank you for testifying here today. And with that, Mr. Chairman, I yield back.

Mr. LYNCH. The gentleman yields back. The chair now recognizes himself for five minutes.

You know, one of the weaknesses in our system is the endemic need for us to share information in order for it to be applied, and that includes classified information. One of the things, Mr. Mandia and Mr. Smith, that I have come across during 20 years of these investigations is that the worst is always denied. So, in this case, we are being reassured by some that that no classified systems were compromised. That is what we are being told. But if the previous patterns are followed here like they have in other breaches and other investigations that we have done, later on down the line we find out that, yes, in fact, classified systems were compromised.

So, can you, Mr. Mandia and Mr. Smith, can you reassure me? I mean, are you willing to guarantee me that no classified systems were compromised? These people had at least nine months, and it seems to be the general consensus here that these were highly professional people. This was a special ops deal, and they cleaned up after themselves. They clearly intended, with the patience that they exerted, and we are talking about thousands of people working on this hack, you know. Can you assure me that our classified systems were not compromised?

Mr. SMITH. Well, I would say, first, I think we are probably the wrong people to try to answer that question. You know, the classified systems are obviously, you know, maintained by the government, and, you know, it is the government's——

Mr. LYNCH. That is what worries me.

Mr. SMITH. But I would say this. I mean, first, there are two things that one should think about, and they cut in opposite directions. The SolarWinds hack was one vector of attack by an agency that, in all probability, is engaged in many vectors of attack every single day of the year on a broad international basis. So, what we have seen here is one slice of activity that is always ongoing, and we should, I think as your question suggests, always assume that there are things that we don't know, and even assume that there are things that are worse than what we do know. That is, I think, a cause for concern.

Now, I will say, on the other hand, what this actor did in many instances, really in all instances, is once they were in a network, they were able to take advantage of lapses in basic cybersecurity practices. The reason they got into, say, a particular number of

DOJ email accounts, in all probability, was because they were able to steal the password of someone or some individuals who had access to those accounts. And by definition, I think we can count on the government to have higher levels of cybersecurity precautions in place for secret and top-secret workloads.

You know, as a cloud services provider, Microsoft, you know, stands up secret and top-secret workloads for the U.S. Government, and, you know, what we consistently find is what you would expect. You know, the people in government agencies who are working in this space are, by definition, going to be more rigorous, so, you know, we should assume that there are more vigorous attacks or hacks. We should also count on stronger protection for those kinds of workloads.

Mr. LYNCH. Mr. Mandia?

Mr. MANDIA. Yes, I think, again, we are not in the purview to know the answer to that question. I can tell you this is an intruder that has collection requirements, sensitive data lost definitely. I did do my stint in the military. I would say it is unlikely that classified information was probably accessed, meaning classified systems, but I can't answer the question. I am not in a position to do so.

Mr. LYNCH. Yes. Well, thank you for your service. I appreciate that. Obviously, it would be valuable to us to know right now in designing our response. It is a whole different dynamic and the level of urgency if our classified systems have been compromised, not only, you know, for the purpose of plugging those holes, but also protecting, you know, sources and methods and other aspects of that as well, so it would be very, very important for us to know that as soon as possible.

With that, I see my time has expired, and I will now recognize the gentleman from Wisconsin, my colleague and ranking member, Mr. Grothman. You are now recognized for five minutes.

Mr. GROTHMAN. Can you hear me? Can you hear me?

Mr. LYNCH. Yes, we can hear you. Go ahead.

Mr. GROTHMAN. OK. I think Mr. Mandia mentioned that there was a problem in that we don't have enough people going into this field. Maybe it was him, maybe it was Mr. Ramakrishna. For either one of you, first of all, what type of compensation do people, say, right out college make if they go into this sort of field? Could you give me an idea? I guess it is maybe an unfair question.

Mr. MANDIA. Yes, I think it was Mr. Smith that commented on that, but I would comment. I think everybody is seeking to hire more cybersecurity professionals. This is something that you don't just walk out of college great at this and proficient at this. You do come out of college with some background in it, but generally you have to do some on-the-job training as well, but right now there is a lot of colleges offering programs. There is a lot of infusion of talent into those programs, and I know the military is actively recruiting people into the cybersecurity space. So, it is something where the ranks are starting to grow, but right now the biggest challenge is the 1-A enterprises are getting the talent because they can afford it and they have the resources for it. And I think there is a bigger concern for smaller agencies in the government or for small to medium businesses that may not have the mission or the money to get the talent.

Mr. GROTHMAN. OK. I realize people probably pay all over the map and that sort of thing, but give me a general idea, and two questions. First of all, a general idea of the compensation people make, and second, what type of background you look at. I think like a lot of jobs, you are telling me you get hired by somebody and then they train you, but if that is the case, what type of background do you get out of college? Do you want to be a communications major? Do you want to be a physics major? What type of thing are you looking for when you hire somebody out of college as well?

Mr. MANDIA. For me and then, you know, I would be fascinated with the other witnesses' answers, it is a computer science background or just an unbelievable passion and desire to be in cybersecurity. It has got to be a fit of desire.

Mr. SMITH. Yes, I would offer a few thoughts. I mean, No. 1, if somebody wants to go get trained in cybersecurity, they are likely to have a good job for the rest of their life. This is an area that is going to continue to grow in importance. Second, I would just say, you know, if you look at technology jobs, if you certainly look at companies like ours, you know, even entry-level positions, you know, have compensation at or north of $100,000 per year, and, you know, people make more money over time.

Third, I do think that there is another important aspect of this, which is really thinking about the pipeline even more broadly than, say, computer science graduates from four-year colleges. At one level, I think there is a huge amount that community colleges can do to help accelerate the development of the cybersecurity work force. People who might have gotten their training in something else, if they want to go back, if they want to want to spend, say, a year taking a set of cybersecurity-related courses in community colleges, they can put themselves on a path to quickly enter this field. And then finally, I would say we need to keep investing even before we get kids to college.

Mr. GROTHMAN. Right.

Mr. SMITH. I grew up in the district next to yours. I grew up in Appleton. You know, as a company, we in Microsoft, you know, do work to provide computer science in high schools. We do it in, say, the two Oshkosh high schools in your district, and what we are finding is that there are young people everywhere who want to learn this field. They just don't have the opportunity that they need and deserve today. So, I think with the right kind of action from the Federal Government, state governments, private sector, philanthropy, we can move so much faster to create more opportunities for people.

Mr. RAMAKRISHNA. And, Congressman Grothman, if I may add, I agree with both my colleagues here on all the points that they made. There are a lot of free online courses and resources that students and kids can essentially access and start becoming savvy in these fields. The criticality there is that the internet is not accessible to everyone in the country. And to the degree that we can do that to ensure that, for instance, inner-city kids, economically disadvantaged children have access to the internet and we give visibility to them for these courses, we will have a larger, more effective, more diverse work force. And to your question about what can

they get paid, I would say with a high school degree and some experience learning online and putting it to use, depending on where you are in the country because cost of living changes, you can make anywhere from $70,000 to $120,000 to begin with.

Mr. GROTHMAN. OK. Thank you. Next general question. Well, I will switch to another question here. This is for Mr. Mandia.

Mr. LYNCH. The gentleman's time has expired. I am sorry. The chair now recognizes the gentleman from New Jersey, Mr. Payne, for five minutes.

Mr. PAYNE. Thank you, Mr. Chairman, and I would like to thank the chairs of the whole committees, Chairwoman Maloney and Chairman Thompson, for holding this hearing today. Just to the point my colleague just before me, to all the witnesses, that information that you are talking about, the opportunities to enter that field and have people learn online and what have you, I think if you could take the time to publicize that more somehow across your companies, that would be very helpful because there are a lot of times where inner-city youth don't know that. But if you were able to publicize it more, they would be able to find those opportunities, so I just wanted to mention that.

The Russian Government has backed, either directly or indirectly, election meddling and other malicious cyberactivity against our interests for quite some time. During his term, former President Trump was reluctant to confront Russia for these attacks and failed to publicly condemn multiple instances of cyber aggression. It is clear that the former President's appeasement of Russian cyberattacks emboldened our adversaries and is partly to blame for the SolarWinds breach. The question is for all the witnesses. Why is it important that our leaders present a strong, united front in containing cyberattacks?

Mr. SMITH. Well, I will say I think this is like any type of offense that the world wants to stop. People will only stop if they are held accountable for the violations in which they engage. You have got to have clear rules. You have got to have clear standards. You have to have clear lines so that it is apparent to everybody when somebody steps over the line. And then you have to have people, especially people in government, who are prepared to speak up and hold others accountable. I think the best type of attribution takes place when it is not just one government, but even by multiple governments together when that is what the situation warrants.

We did see that twice in 2017. I think it is right to acknowledge that. You know, the White House, together with other governments, did that vis-&-vis North Korea in the wake of the WannaCry attack. It did it again with Russia in the NotPetya attack. But we need this on a consistent basis, and I am very hopeful that with leadership that Anne Neuberger is bringing to the White House as deputy national security advisor, with her press conference last week, with the steps she's talking about taking, you will see the kind of leadership we need.

Mr. PAYNE. OK. Thank you. Next?

Mr. RAMAKRISHNA. I agree with Mr. Smith's comments about accountability and rules of engagement. It is important to recognize that we do not accept attacks without some form of reciprocation, so to speak, and holding people to account.

Mr. PAYNE. Thank you. Next?

Mr. MANDIA. Yes, and I would just agree with the other witnesses. It is about risks and repercussions. It is about understanding the rules of the road.

Mr. PAYNE. Thank you. And I guess, Mr. Chair, my time is dwindling, so I will yield back.

Mr. LYNCH. The gentleman yields back. The chair now recognizes the gentleman from Texas, Mr. Cloud, for five minutes.

Mr. CLOUD. Thank you, Chairman, and thank you to the witnesses for being here. I really appreciate you taking the time. I want to especially thank Mr. Ramakrishna for being here in light of the context of what we are dealing with. Your transparency and involvement in this process, we are very grateful for that. I want to ask you, have you provided a list of your clients to the committee?

Mr. RAMAKRISHNA. Mr. Cloud, thanks for the information. Thanks for the question. As it relates to providing names of clients, we have not.

Mr. CLOUD. I serve as ranking member, along with Chair Raja Krishnamoorthi, on the Economic and Consumer Policy Subcommittee of Oversight. Could you provide a list to our committee?

Mr. RAMAKRISHNA. Congressman Cloud, I will take that for the record and consult with my team to see what is possible to disclose at this point in time.

Mr. RAMAKRISHNA. As you can understand, we take the privacy of our customers very seriously, but I will go back and work with my team on it.

Mr. CLOUD. OK. Thank you. Mr. Mandia, you said December of last year that this all began as a dry run in October 2019. You also indicated in December of last year and in Tuesday's Senate hearing that government agencies sensed something wrong in their systems but couldn't really connect the dots until they were notified by FireEye of the breach. What would have enabled us to connect those dots sooner, and would any of these proposals of a centralized agency have assisted with that?

Mr. MANDIA. You don't know. The bottom line, sir, I just felt, as soon as we detected our breach, we were in dialog with our government customers, period, first, to tell them about it. Regardless of laws and legal liabilities, we told our government customers about what we were dealing with. My reaction was that I didn't see surprise. Like, people were shuffling, thinking, and I think that there are a lot of folks who have various products that they had little blips on the radar, and we had to connect dots for many different vectors. This attack, because of the way it was conducted, is just harder to piece together. If you centralize the intel, it can only improve the speed at which that picture and vision will come together.

Mr. CLOUD. OK. One of the questions that I have is, you know, I wholeheartedly agree we need to invest more in making sure that we have the capability to defend and also to build in some attack capabilities certainly to respond to situations like this, the workflow issue being one of the primary indicators, so, you know, making sure students have an interest in engagement. But we also know from past experience that our universities have been a place

where, especially notable actors like China, which I realize this is attributed to Russia, at least to our understanding at the moment. But how do we ensure, of course without creating some sort of discriminatory environment, that we won't be training our adversaries in this regard, you know, especially for something so critical to our national security?

Mr. SMITH. I guess I would suggest here a few things. I mean, one, obviously there is always a role for background checks in a wide variety of different situations. Two, I think the best way for us as a country to ensure that the people that we are training at our universities really support our country is to bring to the country people that we want to have stay here and to make it easier for them to stay here. Right now, unfortunately, it is easy to come study, but it is hard to then stay afterwards. So we are, almost by definition, focusing on training people that we expect to go back to their home country, and I don't think that is the right way to conceive of the talent strategy for the country. The last thing I would say is, if you want to pinpoint the greatest risks, I probably myself would not look to universities.

Mr. CLOUD. Right. Right.

Mr. SMITH. You know, most of what happens in universities gets published anyway.

Mr. CLOUD. OK. Well, yes, I appreciate that. Those are some good thoughts. One final thing, and you probably would be the best to comment on this. In Tuesday's Senate hearing, there was a discussion about the difference between compliance and excellence, especially in critical areas of our government cyber structure, to create some standards that ensure that we have a high standard of protection. But doing so in such a way, a lot of times when government imposes a regulation or mandates, it becomes a check box as opposed to continuing to foster this innovative spirit. How do we get that balance right?

Mr. RAMAKRISHNA. Congressman Cloud, I think I was the one that mentioned that distinction. There are a couple of ways we can do that. One is, CISA has been mentioned a few times in this conversation. We are dedicating resources from our team to work directly with CISA on sharing information. So, it is not just about threat intelligence, but it is also human resource, and human intelligence, and actual experience of building software that needs to be shared, such that standards bodies, like NIST and CMMC, can actually have examples of correct behavior that will put us all on a path of excellence versus simply checking boxes on have you done this, have you done that kind of question and answer. So, that is really where I was coming from where real examples from companies, such as the ones here today, can be contributed to those standards bodies to enrich them.

Mr. LYNCH. OK. The gentleman's time has expired.

Mr. CLOUD. Thank you all.

Mr. LYNCH. I just want to inform the members that there are series of five votes on, so after I recognize the next speaker, I will turn the gavel over to the gentlelady from District of Columbia, Ms. Norton, to preside while I vote. I now recognize the gentleman from Tennessee, Mr. Cooper, for five minutes.

Mr. COOPER. Thank you, Mr. Chairman. Can you hear me?

Mr. LYNCH. I can, yes.

Mr. COOPER. The testimony so far strikes me as at least fatalistic, if not defeatist, because here we have a number of prominent tech companies, and they are really not proposing tech solutions. They are proposing human re-engineering. So, it is as if they are telling us they really can't sell products that are completely safe, so we have to have a rule instead of "let the buyer beware." And I think that tech companies should continue to pursue tech solutions to make us all safer.

But another interesting thing in the testimony that has been completely unmentioned so far is the fact that there is already a hidden, private-sector regulator of cyber intrusion, and perhaps it is hidden because it is private sector, and here I am thinking of insurance companies that sell errors and omissions policies. On page 25 of the stock offering that SolarWinds engaged in in 2018, they talk about how they have incurred and expect to incur significant expenses to prevent security breaches. Then they go on to say, "Our errors and omissions insurance coverage, covering certain security and privacy damages and claim expenses, may not be sufficient to compensate for all liabilities we incur."

So, I would like to find out from each of the companies what claims you have already made to your errors and omissions insurance companies, how much they have paid. Have your premiums increased or do you expect them to increase, because this is the primary way insurance companies regulate behavior, by increasing their premiums for riskier companies. And what percent of the industry do you think has this sort of coverage to essentially inoculate yourselves, but not your customers, against these errors and omissions, and what are the names of these prominent errors and omissions insurance companies? And wouldn't you want to suggest to those companies that they perhaps have a more polite name for the coverage, because "errors and omissions" seems kind of disrespectful to their customers. So, perhaps we can start with SolarWinds and go to FireEye and then to Microsoft.

Mr. RAMAKRISHNA. Congressman Cooper, thank you for the question. Since my coming on board, we have really focused on the investigation and addressing the safety and security of our customers through remediation. And to your point about the private sector taking on more responsibility for tech-based solutions, I could not agree more with you, and that is the reason why we came up with the notion of Secure by Design, which is completely a technical-based approach to enhancing and ensuring the safety and security of our supply chain and that of our customers.

Now, specific to your question, I do recognize that we have insurance. However, I would like to take that question on record to give you the specifics, which I don't have handy at this point in time.

Mr. COOPER. Mr. Mandia?

Mr. MANDIA. Sir, same answer. I would like to take that question on record because I am not prepared to speak to it at this point.

Mr. COOPER. Mr. Smith?

Mr. SMITH. I would say two things. First, I don't know about the specifics here, but generally as a company, Microsoft self-insures. We don't rely on policies from insurance companies. But second, more broadly, if we have left you with the impression that we are

defeatist, then that is the error and omission that we should be talking about. We are the opposite of defeatist. We are looking at this as an enormously challenging and important problem the country needs to address. These are major nation-states, but technology is moving forward. It is getting better. We are offering technology solutions to our customers, not just as a company, but as an industry. You are right that ultimately, just like an automobile, it takes the driver to choose to put on the safety belt, but we are making it easier every year. And I think we should be embracing this with an enormous amount of self-confidence.

Mr. COOPER. Well, instead of two-factor authentication, do we need three-factor? What is it going to be? Are we stuck with passwords? There has got to be a better way to do this, to interface with humans.

Mr. SMITH. Oh, I completely agree, but it is really a combination of steps, and I think that is what your question points to. You know, it is really some things as simple as putting your authentication into the cloud. You know, a lot of what happened here was with customers who did not have it there. They hadn't secured their devices with a service like Intune that we offer. They were not necessarily using what is called "least privileged access" so that when one person's password was stolen, you know, they were able to access more accounts than they should have been able to. A lot of the steps, when you really understand them, do rely on common sense and vigilance. And I do think it is up to us to continue to make that easier for our customers in this country and around the world.

Ms. NORTON. [Presiding.] The gentleman's time has expired. Next is Mr. Higgins of Louisiana.

Mr. HIGGINS. Thank you, Madam Chairwoman. It is our understanding that Russia is responsible for this cyber espionage. They utilized some of our own publicly available hosting services to orchestrate these illegal actions. In my opinion, all server hosting companies, large and small, share a responsibility in vetting their clients, and then also play a part in preventing foreign interference in their operations. There is no daylight between private operations and government operations in the cyber realm. We have to work together to secure our systems for the citizens we serve. This was a direct attack on our Nation's technology infrastructure on a scale never seen before. Eighteen thousand SolarWinds customers compromised and many more thousands of systems breached in the private and government sectors. Russian cyber espionage gained full access across thousands of systems for a number of months. I think it is important to note that this is not the first time that the U.S. Government and private American cyber systems have been subject to major cyber espionage from Russia.

Many years ago, two Administrations ago, the Kaspersky systems were approved on the GSA catalog. That security system was brought into Federal cyberinfrastructure. In 2015, it was identified as being used to steal NSA tools. In 2017, it was finally banned and removed from the GSA list. There are reports as recent as 2019 that Kaspersky software lingers in the government system, and beyond that, Kaspersky had a deal with Best Buy to preload on every computer they sold. Thus, they infiltrated the private sys-

tems at the same time. So, I have been listening to the testimony and the questions from my colleagues. None of us should be surprised about this, and I believe we should be more prepared than we are right now.

Mr. Thompson, I have a question for you, sir. Is it true that you received a 23-page PowerPoint presentation from a former SolarWinds security advisor that listed potential SolarWinds breach vulnerabilities and suggested improvements needed to bolster security? Did you receive that briefing in 2017? And if you did receive that briefing, what did you do about that, good sir?

Mr. THOMPSON. Yes. I believe that we have really taken the security of our customers and our products seriously over the history of the company. We have got a unique relationship with our customers where we are very engaged with the individual users of our products. And so this——

Mr. HIGGINS. Pardon me, Mr. Thompson, but that sounds like an answer prepared by attorneys. It is a simple question, respectfully. Did you receive this major briefing in 2017 that I am referring to? Did they recommend changes, and did you enact those changes?

Mr. THOMPSON. So, it is my understanding, based on our investigation, that there was a briefing provided to some of my IT leadership team, and that that briefing was about security posture in general and about what the company could do to make sure that its security posture was enhanced and to make it a leader in security. And, yes, not as a result of that presentation, but beginning even before that, we began to invest in security and enhancing the posture of our security environment. In fact, we spent more than the average technology company of our size over the last four years on security. So, we have taken security very seriously, but not really as a reaction to that presentation because we knew security was important before that, and we were focused on it.

Mr. HIGGINS. I appreciate your response. My time is winding down. Mr. Smith, can you quickly address the cloud hosting systems? It has been reported that threat actors in this breach leveraged servers from Amazon Web Services. Can you talk about what we can do to protect our cloud systems from further espionage efforts?

Mr. SMITH. Well, I am obviously not in a position to speak on behalf of Amazon or AWS. I do think we should take more steps. We certainly are always taking more steps in Microsoft to ensure that our cloud services, to the extent possible, cannot be used by a foreign adversary. I actually think it should start with transparency. I am here today. I am answering all your questions. Microsoft has published 32 blogs since this came to light. Amazon has yet to publish its first. So, I think we will all benefit if we create a culture where tech companies are sharing more information.

Mr. COOPER.[Inaudible] for that point, Mr. Smith. Madam Chair, my time has expired. I yield.

Ms. NORTON. Yes, the gentleman's time has expired. I recognize Ms. Clarke of New York. Go ahead, Ms. Clarke.

Ms. CLARKE. Yes. Thank you very much, Madam Chair. I just wanted to, first of all, thank our panelists today for appearing before us. I currently serve as the chairwoman of the Cybersecurity Subcommittee, and I want to be perfectly clear that as a Nation,

we cannot let this happen again. SolarWinds was but the latest malicious cyber campaign against our country, and it will not be the last. We certainly must hold the perpetrators of these attacks responsible, but we also must bolster our defenses so that they can't succeed in the future. So, my question is for Mr. Smith and Mr. Ramakrishna.

Earlier this week, you both expressed your support for requiring critical infrastructure owners and operators to report cybersecurity incidents. Again, as the chairwoman of the Cybersecurity Subcommittee, this is something my subcommittee has been working on for some time. In fact, the House-passed version of the Fiscal Year 2021 NDAA included language that would require critical infrastructure entities to report cyber incidents to CISA. Unfortunately, that language fell out during the conference, but I intend to take a close look at this issue again, and I am heartened to see that there is so much momentum behind this.

As anyone that has been working on this issue for a while knows, the devil is in the details. We need to figure out who would be subject to reporting requirements and what kind of incidents would trigger the requirement report. We also need to determine who they are reporting incidents to, whether that is CISA, a new agency modeled after the NTSB, or someone else. And finally, we need to decide what our ultimate goal is, holding companies accountable or are we just trying to get a better understanding of why our security controls fail. So, to the two gentlemen, can you elaborate on the reasons you believe we need a cyber incident reporting requirement and some of the benefits you expect to flow from such reporting?

Mr. SMITH. Well, I would say we really appreciate the leadership that you have been bringing to this, and I think you provided a checklist of some of the most important questions that need to be answered. But to address the one that you posed at the end, which perhaps is the most important of all, what are we trying to accomplish, I think our top priority is to make the country more secure. And the reason that we should want companies in the private sector, companies that, as you mentioned, are in the area of critical infrastructure, it is to provide information about threats so that one entity is in a position to scan the entire horizon and connect the dots between all of the attacks or hacks that are taking place.

I think Kevin Mandia who described it really well earlier—you know, you really cannot oftentimes determine exactly what is going on until you connect all of those dots, and today, this information is in separate silos. So, I would say let's solve the problem that needs to be solved, which is the cybersecurity protection for the country.

Ms. NORTON. Mr. Ramakrishna?

Mr. RAMAKRISHNA. Congresswoman Clarke, thank you again for your leadership and for your question. Having a single entity to which all of us can refer to will serve the fundamental purpose of building speed and agility in this process. Too much time is wasted in communicating across agencies where information is very fragmented, and oftentimes the dots are not connected because they are separate. That is the fundamental reason why I think having a singular agency to which all of us can communicate to and have

two-way communication with them is fundamental to improving our speed and agility around these topics.

Ms. CLARKE. We have a few seconds left, but I would be interested in your thoughts on how Congress should scope this new reporting requirement. Who should it be subject to, who should be required to report, and who within the Federal Government is best positioned to receive and make use of such reports?

Mr. RAMAKRISHNA. Congresswoman Clarke, you mentioned CISA a few times. We have been engaged with CISA and other government agencies. We are also offering our human resources to work with CISA as well. That could be an initial starting point, and obviously you are more qualified to decide if that is the established entity to take this on and going public. So, our belief is all private enterprises should be instructed with reporting requirements and be made part of this community vision where public and private sectors can work together to tackle this issue.

Ms. NORTON. The gentlewoman's time has expired.

Ms. CLARKE. Very well. I have run out of time. I yield back. I look forward to our conversation as we continue to address this issue. Madam Chairwoman, I yield back.

Ms. NORTON. I thank the gentlelady from New York, and I call on Mr. Norman of South Carolina.

Mr. NORMAN. Thank you. Two of the most, I guess, disturbing things that I have heard this morning during this testimony is, one, that it took nine months, that the Russians or whoever was involved had access to our most valuable intelligence. And I agree with Congressman Lynch: our next hearing ought to be with those that can answer the questions, what has been compromised, because national security is at risk. The other thing that really has shocked me is, Mr. Smith, your testimony that, really, we are at a shortage of cyber experts to connect the dots. I guess my question, we can't wait to train somebody out of high school, college, junior college. What group can we go to? Is it those that have been successful at breaking the system and are incarcerated, that are street smart, I guess, to know how to get to making sure this doesn't happen again? Your thoughts.

Mr. SMITH. Well, I think it is a key question, and I would point to two things that I think we can do to move faster as a country. No. 1, really harness the power of our community colleges. We don't need to send somebody back for four years of education. You know, there is a set of eight or ten courses that an individual can take over, say, a year or a bit more if they want to go full time, or they can, you know, take some courses while they are holding a full-time job. And I think that is probably the fastest way for us to expand the cybersecurity work force.

I think the second thing is really for us in the tech sector ourselves. You know, we are doing more, we are investing more, but I think we can and should do more, and, you know, that is a good point of learning for somebody like me and for a company like Microsoft. You know, we have LinkedIn. That is part of Microsoft. And so, you know, it is an opportunity for us to harness the power of, say, LinkedIn Learning and the connections not just with community colleges, but with employers. We are also focused on, you know, how we can add cybersecurity curriculum to, you know, the

training programs of employers of all sizes so that if there is somebody who needs to learn, you know, six extra things, they don't need to go back to school. They don't even need to take a course to do it. We can take the training to where they are, and we can build it into their workflow on the job. That is something that we are using our own technology to do.

So, I think this is a lot like anything. Once you understand the importance of the problem, you can really harness all of the available resources to address it. And I think it is right that we make this one of the priorities that comes out of this.

Mr. NORMAN. So, as a Member of Congress, what should we do to get the Amazons on board? You know, you are one company. You are a big company in Microsoft. But what can we do to get private sector, the other large companies that, you know, basically have monopolies, how do we get them activated, or what is your advice to us?

Mr. SMITH. Well, look, I am not the best person to give you advice on how to get Amazon to do something. There will be others who will be more insightful than me. What I would say is if I were in your shoes and I really wanted to have the broadest impact as quickly as possible, you know, I would look at opportunities to provide, you know, incentives for individuals who want to go study at community colleges so they can do so. And I would look at, say, tax credits for smaller businesses so that if they want to invest in the training of their people, they can do that as well, so that you would target, you know, the limited budget, the limited taxpayer dollars to the places where they would have the greatest impact in the shortest possible time.

Mr. NORMAN. Well, that is just what we need to hear, and a lot of times in politics, we don't know what we don't know. We are going to have to depend on y'all to give us a roadmap on how we can do it. We simply cannot take another nine months to let countries that don't have our best interests at heart damage us, and I would be interested in anybody else, any other comments any of the other panelists have, I would be interested in.

Mr. RAMAKRISHNA. Congressman Norman, if I may suggest one area where the Congress may be able to help us also is by encouraging us and incentivizing us to come forward with more of these intelligence aspects and share them more broadly. In addition to litigation risk, some of us may be worried about reputational risk that it causes where the victim is victimized for coming forward, and those should stop so that we can all come together and really build our efforts to thwart these major issues going forward.

Ms. NORTON. The gentleman's time has expired. I will call on Mr. Connolly of Virginia next.

[No response.]

Ms. NORTON. Is Mr. Connolly there?

[No response.]

Ms. NORTON. If Mr. Connolly isn't there, I am looking for the next Democrat. Please give me the name of the next Democrat. I think you are the next Democrat, sir.

Mr. KRISHNAMOORTHI. Were you talking to me, Chairwoman?

Ms. NORTON. Yes. Yes.

Mr. KRISHNAMOORTHI. OK.

Ms. NORTON. I am moving to you, yes.

Mr. KRISHNAMOORTHI. OK. OK. Very good. Thank you so much for all of you testifying today, and thank you for your transparency and for giving us some very insightful information. So, my first question is to Mr. Smith. Mr. Smith, you gave an interview with "60 Minutes" recently, and in that interview, you said that essentially the supply chain tech attack was ongoing currently. One question I have right out of the box is, are you aware of whether that malware and that attack is potentially present on computers in the U.S. House of Representatives?

Mr. SMITH. We are not aware of this being focused on the U.S. House of Representatives, so no. The answer is, no, I am not aware of that.

Mr. KRISHNAMOORTHI. How about the U.S. Senate?

Mr. SMITH. I am not aware of any use of this tactic on the U.S. Senate either. We have seen cyberattacks, you know, in the past on members of the House and members of the Senate, and whenever we have detected them, we have let either the Sergeant-at-Arms or the Speaker or members know.

Mr. KRISHNAMOORTHI. Sorry. My time is limited, Mr. Smith, so I am just to ask you to respond briefly.

Mr. SMITH. OK.

Mr. KRISHNAMOORTHI. How about the Office of the President?

Mr. SMITH. I am not aware of any attack using this vector on the Office of the President.

Mr. KRISHNAMOORTHI. Now, in that "60 Minutes" interview, you also mentioned that perhaps the only way—because you have to understand this. The way I kind of picture this is that it is almost like the burglar is in the home while we are all here. And one of the things that you said that really struck me in your "60 Minutes" interview is that you said that perhaps the only way to make sure that we get rid of this attack or this intruder is to "rip and replace every single piece of network equipment and computer that may have been affected." Do you still stand by that quote that you gave to "60 Minutes"?

Mr. SMITH. Yes, I don't believe that I am the one who said that. If I did, I referred to the thought that some have that that may need to be done. I don't——

Mr. KRISHNAMOORTHI. OK. Let me stop you there for a second. Have you done an assessment of what that might require? Because, at the end of the day, we need a foolproof way to eject the intruder from our homes. We cannot be in a situation where the intruder has carte blanche espionage capability on us. So, talk to me a little bit about that. What type of, you know, effort would be required if we were to undertake that?

Mr. SMITH. Well, we have not been asked to do it. To the best of my knowledge, we have not undertaken an analysis of what it would take to rip and replace all of the, say, technology infrastructure of a particular agency or part of government. It is actually not what I believe needs to be done. I think that efforts are better focused on other approaches.

Mr. KRISHNAMOORTHI. Well, here's my concern, which is, what is the foolproof way to get rid of the intruder from our collective home at this point, because we are tired of hearing that the intruder is

here. We have no idea what that person, that intruder is doing, but we should just kind of move on to the next subject. We need to eject the intruder from our computers right now, whether it is in the private sector or in the public sector. So, what is the foolproof way that would come short of ripping and replacing all this network infrastructure?

Mr. SMITH. Well, I would say two things. No. 1, one always needs to identify how someone got in or is getting in in order to get them back out. So, you know, that is in the realm of the kind of cybersecurity sort of forensic investigation that, you know, a company like Microsoft can help with, a company like FireEye does, you know, every day. You know, among the best, we are the best in the world. That is one part. The second thing is, there are five really straightforward cybersecurity steps that we believe, put together, will strengthen protection across the board: move authentication into the cloud, secure each of your devices, ensure that you are using anti-malware software across the board, use multi-factor authentication, apply privileged access. If you do those five things following a review by a company like FireEye, you should be in a much, much stronger position.

Mr. KRISHNAMOORTHI. I guess my final question is to Mr. Ramakrishna. You know, you are the new CEO and you are coming into a pretty bad situation. The NSA is not allowed to surveil private networks. It is only allowed to surveil foreign networks. Is the FBI and current agencies capable of doing what is necessary to surveil private sector networks in the U.S.?

Mr. RAMAKRISHNA. Congressman Krishnamoorthi, I wish I were an expert in being able to give you a yes or no answer on that, but I am not particularly qualified to address that. Does some level of surveillance and sharing of information between private and public sector need to happen at a level that is not happening today? My belief is absolutely yes, but with regards to surveillance, I am not the expert to address it.

Mr. KRISHNAMOORTHI. Fair enough. Thank you.

Ms. NORTON. I thank the gentleman for his questions. His time has expired, and I call on Mr. Biggs of Arizona next.

Ms. BIGGS. Thank you, Madam Chair. Because of the scope of this attack, I am concerned. It looks like it may take years before we fully understand its impact. Mr. Smith, my first question is for you. How likely is it that these attacks are continued, and, if so, how can we best determine who is still being attacked?

Mr. SMITH. Well, the first thing I would say is this agency's attacks or hacks did not start with the use of SolarWinds software, and it did not and will not end there. I think we should assume that this is an agency, and this is one of a relatively small number of very well-resourced governments that are focused on these kinds of threats against the country every single day, and they will be for the rest of our lives. And so I think what we need to do is just continue to strengthen the cybersecurity defense of the country, and we need, in part, to couple that with the better sharing of threat intelligence so that we are better able to spot the attacks or hacks as early as possible after they begin.

Ms. BIGGS. So, one of the concerns I have is that Congress is going to say, well, let's just create another layer of bureaucracy in

there and then call it good. We will have done something until the next time we have an episode like this that we need to deal with. And I am wondering, and I will just turn to all the panelists, real briefly if you would. Would you tell us whether you see the solutions to prevent future attacks coming from government, or are they going to come from the private sector? So, let's start with Mr. Smith and then just move on down the panel.

Mr. SMITH. Well, I think we each need to play our role and do it well. I think that the public sector, the government has a unique role to play in establishing rules of the road, strong laws and holding foreign governments accountable. I think the government has a unique role to play, both in and securing the government's own infrastructure and in collecting threat intelligence in a centralized way and putting it to good use. I think those of us in the private sector have an enormous role as well. We need to continue to strengthen the technology. We need to continue to make it easier for people to use the technology. We need to share the information we have, something that is not yet happening nearly to the extent that it needs to happen across the tech sector.

Ms. BIGGS. Thank you. Mr. Ramakrishna, if you would go next please.

Mr. RAMAKRISHNA. Congressman Biggs, I agree with my colleague, Brad Smith's, comments here and the work that he, and Kevin Mandia, and our colleagues at CrowdStrike and others are doing. As it relates to your question, the picture I would like to paint is, we are dealing with intruders, not an intruder, in this case. They behave like Transformer toys in many ways where they are constantly morphing and changing their tactics and procedures on us. So, to that end, we have to be nimble as well in working between the private and public sectors, and shaping our policies and shaping our information practices to adapt to this changing set of intruders and go on the offensive.

Ms. BIGGS. Thank you. Mr. Mandia?

Mr. MANDIA. Yes, I agree with both witnesses, both Sudhakar and Brad, on this one. It comes down to the government exists to have a proportional response and deterrence. The private sector will most likely be building the technology to safeguard in cyberspace working with the government, and you meet in the middle with the threat intelligence sharing.

Ms. BIGGS. So, all of you at one point, either in answering this question or other times today, have talked about information sharing. I just want to know, are there any legal or regulatory barriers to information sharing that you see that currently exists? Back to you, Mr. Smith.

Mr. SMITH. Well, I would say there are two barriers today. The first is, it is not always entirely clear to whom we should be sharing the information or sharing it with. But then second is, the one thing that we have noticed that we have mentioned publicly that is a legal barrier, is today, it is a fairly standard aspect of Federal contracting practices that agencies restrict a company, like Microsoft, from sharing with others in the Federal Government when a particular agency has been hacked in this way. So, one of the specific things that we had to do in December was go to each agency, tell them that we had identified that they were a victim of this.

And then we had to say, you need to go over to this person in this other part of the government to let them know. Please do that. We cannot do that for you. And the good news is that people did that. They did it quickly. But I think it is a barrier that is an impediment.

Ms. BIGGS. In what little time I have left, I would urge the chairs of these two committees to take us into a classified hearing because I think there are some things, like, I would like to know, how do we know it was Russia. I would like to know what China's involvement was. A classified hearing would allow us to get more of that information, and I would look forward to that. And I thank all the panelists, I thank the chair, and I yield back.

Ms. NORTON. Well, that, I think, is certainly an idea. The gentleman's time has now expired, and I call on Mrs. Watson Coleman of New Jersey now. Mrs. Watson Coleman, you are recognized for five minutes.

[No response.]

Ms. NORTON. Mrs. Watson Coleman appears to have stepped out. Mrs. Demings of Florida, you are recognized for five minutes.

Mrs. DEMINGS. Thank you so much, Madam Chair, and thank you so much to those who are with us today. It has been a very good discussion. As I listened to the line of questioning from Mr. McCaul from Texas, those were particularly some areas that I certainly was interested in. I believe during that line of questioning, there was an indication that the malware was hiding in plain sight, and I've also heard that in order to keep up, that we have to constantly change and adapt and improve, I guess, our capabilities. What I am particularly interested in is a better understanding of how the transition to iCloud services, like Microsoft, affects a customer's visibility related to network activity. Although the cloud environment was not the initial entry point for malicious actors in this campaign, it is where they were able to access data and proliferate through iCloud assets undetected for the better part of the year.

So, Mr. Smith, have any of Microsoft's cloud customers informed Microsoft that their cloud environment was accessed as part of this campaign, or has Microsoft had to inform its customers?

Mr. SMITH. Yes, it is an excellent question. The first thing I would say is the right way to think about what happened here is that each and every one of these attacks, hacks, that we have seen happened on premise, meaning it was on a server, say, that was in the server room or onsite. Now, once the attacker was in the network, one of the things it did was it looked for the keys or the passwords to get into cloud services, like email or documents, or other things. Once they did that, then they were able to go up into the cloud and access those kinds of cloud services.

Once they did that, we were able to see them because we scan the services that we run every day with a specific eye toward some particular threats. We have a Threat Intelligence Center that does that. So, in each of the 60 instances where there were Microsoft customers that were victims, we identified that they were the victim and we notified them. We have a team called the Detection and Response Team, DART. It is their mission to every day take this kind of information and let customers know if they are being vic-

timized in this way. And, yes, it is one thing that we do. I think it is something that the tech sector more broadly needs to do.

Mrs. DEMINGS. OK. Thank you so very much for that. And for my kind of breaking it down as a former law enforcement officer, I kind of liken what you just said as to a burglar going around trying the doors. You are looking for that unlocked door or the key, and then they are able to access, as you just indicated. Can a cloud customer identify unauthorized access to their Office 365 accounts with their own logs? Can they do it themselves, the customers?

Mr. SMITH. I think the short answer is, yes, they can do it in a variety of ways. They can do it either by themselves or, you know, some customers may want to rely on the help of a third-party service provider, a cloud service provider and the like, you know, that is working with them. So, yes, they don't need to rely exclusively on the infrastructure or, you know, a company like Microsoft to do that, but it is an added service that we do provide both in terms of detection and letting people know.

And then I will also say we also try to offer advice. In some ways, what happened here was, you know, for example, it is like leaving your keys on the kitchen table, and when you do that, somebody can go steal your car, you know. The cloud may be, in this case, you know, your email that they access.

Mrs. DEMINGS. Right. And, you know, Mr. Smith, what bothers me so much about that is we are talking about nine governmental agencies, right?

Mr. SMITH. Well, that is why we say don't leave your keys on the kitchen table.

Mrs. DEMINGS. Yes. Yes. Yes.

Mr. SMITH. We give people advice and secure ways to store their keys.

Mrs. DEMINGS. What steps have been taken, finally? I have 14 seconds. What steps have been taken or discussions that have taken place to really review the cloud environment logs and prepare for the next breach?

Mr. SMITH. Well, I think that work is ongoing. Any time something like this happens, it should cause all of us to step back and say what have we learned and how can we get better because we continually must. We are definitely working through an effort like that here at Microsoft, and, yes, I would hope it is taking place at other companies in the cloud services business as well.

Mrs. DEMINGS. Mr. Smith, and to all of our witnesses——

Ms. NORTON. The gentlelady's time has expired. The gentlelady's time has expired. I call on for five minutes Mr. Van Drew of New Jersey.

Mr. Van Drew. Thank you, and I want to thank the chairs and ranking members for doing this. This is good work. You know, America is under constant attack from adversaries looking to damage our businesses, our hospitals, our municipalities, and critical infrastructure using cyber warfare. Like the witnesses have already stated, we face serious threats from Iran, China, Russia, North Korea, and other bad actors in the global landscape. The SolarWinds campaign was a devastating attack that showed how vulnerable we are to those types of attacks. The integrity of our critical infrastructure is not as robust as we thought it was.

The Federal Government needs to do better and so does the tech industry. With close to 80 percent of Fortune 500 companies utilizing SolarWinds technology, there needs to be collaboration obviously between public and private entities to protect America. We owe it to our constituents, our municipalities, and our country to ensure that we are adequately prepared for these harmful actions.

In my district, two years ago, the Atlantic County Utilities Authority, located in Egg Harbor Township, New Jersey, was the victim of a cyberattack. The Utilities Authority reported an incident in which perpetrators gained unauthorized access to sensitive data of customers. Additionally, operational information was withheld as the criminals demanded ransom. Fortunately, the overall function of the Authority was minimally impacted, but the fallout could have been far, far worse. I applaud the previous Administration's efforts to increase our Nation's cyber defenses and improve gaps in our framework, and I implore the Biden Administration to take this issue seriously and prioritize the safety and well-being of Americans.

For Mr. Smith, in your written testimony, you discuss Microsoft's relationship with other technology companies and their role in Microsoft's response to the attacks. How is Microsoft's relationship with the Cybersecurity and Infrastructure Security Agency, CISA, and do you feel we are safe from future cyberattacks of this nature?

Mr. SMITH. Well, I think it is an excellent question. We feel very good about the progress that CISA has been making. It is a young agency. It has moved far, and it has moved fast. It is going to need, I think, to move farther and faster in the future, and that will require additional resources as we continue to build the role of CISA in protecting the country. I also think it is just worth noting, your examples, I thought, were so important because so often we see two things. We see the most sophisticated cyberattacks begin with nation-states, and then we see their tactics copied by cybercriminal organizations, and then they go to the weakest point. And the kind of ransomware attacks that you have experienced in your district, they were experienced in Baltimore, in New Orleans, by hospitals across the country.

And if there is one thing I consistently find today, it is that many of the public sector computers and information systems software, especially at the state and local level, are not as modern as they should be. Just to give you one example, one department of health at the state level that we are working with on the distribution of vaccines, we went to help them strengthen their work. And when our consultants looked at the manual for the software program they were using, it was for a company that Microsoft acquired more than 20 years ago, so the software was more than two decades old. So, part of what I think we need to do is strengthen CISA, but I think part of what we need to do is really, across the country at the state and local level, embrace the modernization of our IT infrastructure, and, in so doing, embrace the modernization of our cybersecurity protection.

Mr. VAN DREW. So, thank you for a very good answer. Do you know what they are doing with localities? Are they specifically working? Like, I know, for example, in our utility, there was ransom, the ransom was paid, it went through insurance, and then

they still didn't have a key to get them out. They actually had to figure it out on their own.

Mr. SMITH. Yes. No, that is often a problem. We oftentimes work with hospitals and municipalities that have been the victims of these kinds of ransomware attacks. There are times when consultants like ours can go in and solve the problem, and there are times when it is not possible because of the effectiveness of the attack. I do think CISA does an important job in providing advice, but this also comes down to really state and local government budgeting for modernization, and, I would say, decisionmaking so that you integrate the decisions of the IT team with the needs of, say, in vaccines, the epidemiologist, for example, that need the technology to help them do their jobs. You know, we need to just think anew about how we manage technology across the public sector.

Mr. VAN DREW. Real quick. Are we going in the right direction?

Mr. SMITH. We are going in the right direction. We need to move much faster.

Mr. KRISHNAMOORTHI.[Presiding.] Thank you, Mr. Van Drew. I would like to now recognize the distinguished gentleman from Virginia, Mr. Gerry Connolly.

Mr. CONNOLLY. Thank you, Mr. Chairman. Can I be heard?

Mr. KRISHNAMOORTHI. Yes.

Mr. CONNOLLY. Thank you. I want to talk about threat hunting and cyberdefense, and I am going to ask all the witnesses when I pose a question to be as succinct as you can because I have a lot of them. Last month, Mr. Ramakrishna announced SolarWinds intends to increase threat hunting capabilities to bolster the company's security. Mr. Thompson, did SolarWinds routinely employ threat hunting before the discovery of the attack in December?

Mr. THOMPSON. We had a number of security defenses at the company before the discovery of the SUNBURST malicious code. So, we leveraged a lot of the technologies that other companies leverage, and I think that we were doing more than the average software company to protect our environment.

Mr. CONNOLLY. The question was threat hunting capabilities specifically.

Mr. THOMPSON. And I don't recall whether we were doing threat hunting specifically.

Mr. CONNOLLY. Mr. Smith, Microsoft provides threat hunting as part of its cybersecurity services. Why did Microsoft's threat hunters fail to discover the SolarWinds compromise?

Mr. SMITH. We do have a large number of threat hunters. I would say we did not detect this intrusion as quickly as we might because, first, it was very limited on Microsoft's own network, and second, until we heard from someone else, like FireEye, you know, we didn't have the specific threat to hunt for. You know, it is definitely a capability that we are continuing to invest in to expand at Microsoft.

Mr. CONNOLLY. Has Microsoft learned any lessons from its investigation of the compromise that could improve hunting for this type of threat in the future?

Mr. SMITH. Absolutely. I mean, I think whenever something like this happens, we need to learn a lot, and you need to take a little bit of time and let the dust settle. You know, there is the kind of

threat hunting that needs to take place every day, and that includes the work of our Threat Intelligence Center to scan the horizon. I think one of the things that we learned is when you have an adversary that is this focused, this determined, and this well-resourced, there will be major cyber incidents that require you to expand overnight the number of individuals who are engaged on response or threat hunting.

We did that in this instance. We expanded to more than 500 engineers who were pretty much on this 24 by 7, but we are asking ourselves how we build the capability in the future to grow to even a larger number if that is what we need to do.

Mr. CONNOLLY. OK. I am sorry. I am going to run out of time, but let me ask one more question in this series. How can the government support private companies that have been engaged to threat hunt on Federal networks?

Mr. SMITH. Well, I think the single most important thing the government can do is create a centralized point of intake so the threat intelligence, the information that is found from threat hunting, can go to a central place, but there is a second step that is needed as well. The government then needs to decide when and how to share information it is finding back with companies, like FireEye or Microsoft, so that we can act using that information in an appropriate way.

Mr. CONNOLLY. The National Defense Authorization Act provided cybersecurity agencies with increased authorities to do threat hunting across the Federal civilian networks. Do you believe those provisions in the National Defense Authorization Act would do what you just suggested?

Mr. SMITH. I think the NDAA that was just passed goes far in adding additional tools and layers of protection. I think there is more that we need to do to add to what was passed last year. In this area of, you know, information about threat intelligence, I think, you know, this is a specific topic that it is good we are talking about here. I think it is an area where additional legislation would be helpful.

Mr. CONNOLLY. Mr. Ramakrishna, you indicated, in response to Mr. Langevin, three theories you have about the attack, but the third one intrigued me, that you were a victim of supply chain attack. What is the evidence to support that?

Mr. RAMAKRISHNA. Congressman Connolly, my point on the third hypothesis that we laid out was a potential vulnerability in a third-party software that we are deploying at our company. So, I wasn't referring to necessarily a supply chain attack on a third party as much as a vulnerability that we are yet to discover.

Mr. CONNOLLY. And my final question is to Mr. Mandia. Based on your experience in the Air Force and the Pentagon, what are the limitations from your perspective about threat hunting when used by the Federal Government, and then I will yield back, Mr. Chairman.

Mr. MANDIA. First, I think threat hunting is something that is probably a decade old. Not every company does it. We are talking about an attack that impacted 17,000-plus organizations, and nobody detected it until we reversed the whole thing. So, you are going to see threat hunting gain in popularity, but it is a high-skill-

set thing. Government agencies that we have worked with are well trained, can conduct threat hunting, and I think it is all about authority. Do they have the authority to do it or not?

Mr. CONNOLLY. Does the NDAA give broader authority?

Mr. MANDIA. I am not prepared today to speak to that. I haven't read the whole document.

Mr. CONNOLLY. Maybe you could get back to us with that for the record.

Mr. KRISHNAMOORTHI. The gentleman's time has expired.

Mr. CONNOLLY. Thank you, Mr. Chairman. I yield back.

Mr. KRISHNAMOORTHI. Thank you, Mr. Connolly. Now I would like to recognize Mr. LaTurner from Kansas. Mr. LaTurner, you are on the clock.

Mr. LATURNER. Thank you. My question is for Mr. Smith, and I would like to discuss cyber deterrence as it relates to the private sector. This is a discussion that you had some on Tuesday, but I want to talk about the frustration that does or does not exist in the private sector that the U.S. Government just isn't doing enough to deter these attacks. Could you speak to that?

Mr. SMITH. I think that there is a need for additional deterrence or accountability measures, and I think it probably needs to fall into three categories. First, in certain areas, there is an opportunity to strengthen the rules of the road and, in particular, with respect to three issues: something that puts this kind of software supply chain or hardware supply chain disruption off limits, especially for these kinds of disproportionate and indiscriminate attacks; second, something should put attacks on hospitals and the public health service off limits; and third, it should put attacks on the electoral system off limits. That is step one.

Step two, I think we then need a consistent government policy that says that when these lines are crossed, the government, whenever it finds sufficient information, is going to have public attribution, and that public attribution, where possible, should be with our allies as well so it has multinational effect. And third, the government needs a set of tools so that there are consequences for when these lines are crossed.

Attribution is the first step, but there may be instances where there are sanctions. There may be instances where there are other steps. I think this is fundamentally a question for the government itself, but it is like anything. If you catch somebody who is engaged in an offense, you need to hold them accountable, and you need a variety of ways to do that.

Mr. LATURNER. I appreciate that, and I want to talk about information sharing and how that can enhance the ability to address some of these threats. And specifically, does Microsoft contracts prevent you from sharing threat intelligence with the government? What kind of restrictions does that put on you?

Mr. SMITH. Well, the government's contracts impose restrictions on Microsoft and other government contractors in this kind of situation. So, that was the specific limitation that we encountered when we wanted to notify different parts of the U.S. Government of what we were seeing. And we found that we could only inform the agency that was the victim itself, and we had to ask them to go talk to another person, or individual, or part of the government,

which they did. But it struck us as a barrier that is not serving the government itself very well.

Mr. LATURNER. But no issues with private sector contracts. Is that what you are saying?

Mr. SMITH. No. I mean, it is very interesting to me how varied the practice is across the tech sector. At Microsoft, when we see one of our customers that are attacked, I think it is our first responsibility to let the customer know. We have done this more than 13,000 times in the last two-and-a-half years with nation-state attacks, and yet there are other companies that, to the best of my knowledge, have not even alerted their customers or others that they were a victim of the SolarWinds-based attack. These are companies where their own infrastructure was used to launch the attack, and somehow they don't think it is part of their responsibility to let these victims know that they are victims. And that needs to change, and it needs to start in the tech sector. I think we need to come to terms with this.

Mr. LATURNER. Thank you for your testimony today. Mr. Chairman, I yield back.

Mr. KRISHNAMOORTHI. Thank you very much, Mr. LaTurner. Congresswoman Kelly?

[No response.]

Mr. KRISHNAMOORTHI. Congresswoman Kelly?

[No response.]

Mr. KRISHNAMOORTHI. Congresswoman Kelly, can you hear me?

[No response.]

Mr. KRISHNAMOORTHI. Robin? She just responded. Congresswoman Kelly, you are recognized for five minutes.

Ms. KELLY. Oh my goodness. I can't believe it. OK. Let me get the thing up. Thank you so much, Mr. Chair, and thank you to the witnesses. Can you hear me?

Mr. KRISHNAMOORTHI. Yes.

Ms. KELLY. OK. The SolarWinds hack reflects a disturbing new paradox for the security of U.S. computer and information technology systems. Regular software updates and patches are often critical for correcting known vulnerabilities and preventing cyberattacks. Many of my colleagues will recall the March 2017 Equifax data breach that resulted in the loss of massive amounts of personal and sensitive data. In that case, the hackers exploited a widely known vulnerability that should have been patched several months earlier. Mr. Mandia, can you tell us why regular software updates and patching is important for protecting an individual or a business's systems and networks?

Mr. MANDIA. Absolutely. When you are patching, what you are trying to do is close the window of vulnerability, period. You know, software, there is always first-to-market versus secure-to-market, and a lot of times it is hard to find security imperfections in software ahead of time because it is hard to predict the thousands of different ways people may use your software. So, I have heard people say building software is like building a bridge. It is not. Bridges follow the laws of physics. Software does not. But the bottom line is this: there is always a gap between what attackers can do and the capability and the safeguards that we have. When you get a

patch, the faster you patch it, you are reducing your window of vulnerability.

Ms. KELLY. Thank you. In the case of SolarWinds, a software update itself, a trojan horse, ended up installing malware on the victims' computer networks. I am concerned that at a time when regular software updates are as important as ever, the SolarWinds attack might deter individual customers and systems administrators alike from installing needed software updates. Mr. Mandia, what would you say to customers or systems administrators who may be concerned or reluctant to download updates or patches for software for fear that updates might contain malware?

Mr. MANDIA. Well, I can tell you even in the SolarWinds breach, we have to remember the funnel. Over 17,000 companies were stage 1 victims, but the attacker only accessed 100. This was a manual attack, not an automated virus. There is a human on a keyboard. This is a threat group that doesn't target everybody all the time, so the risk is far less based on the constraints that the hacker had or the attack group had based on manual labor. The bottom line is everybody is now recognizing the rules of the road are that foreign intelligence services are hacking the supply chain, and everybody is wondering is there another implant in some other software. So, I think that there is going to be more inspection, where the capability to inspect exists, for all updates on a go-forward basis, and the industry is going to change both how software is created and how software is vetted.

Ms. KELLY. Thank you so much. Mr. Ramakrishna, SolarWinds has reported that the company has 33,000 Orion users. You later identified that 18,000 had downloaded an effective version of Orion during a three-month period. My question is, customers have to manually download updates from you, correct?

Mr. RAMAKRISHNA. Congressman Kelly, that is true, yes.

Ms. KELLY. This would suggest that just over half of your customers downloaded an update during three months, to say nothing of whether or not they actually installed it, correct?

Mr. RAMAKRISHNA. That is correct.

Ms. KELLY. And then at the same time, the customers that did download the update exposed their systems to this malware.

Mr. RAMAKRISHNA. That is a potential, yes, Congresswoman. As Mr. Mandia described it, once the patch with the affected code is installed at a customer site, in certain installations, not everywhere, not in every place, they try to connect back to essentially their home server to see if they can actually get connectivity and then potentially start doing some things manually to break through the defenses once they have gotten in, which is——

Ms. KELLY. OK. I got you. Mr. Smith, let me turn to you quickly. Does it concern you that users may think twice about downloading an update, and can you explain?

Mr. SMITH. I think it should concern us all. I think Kevin Mandia put it well. I mean, I do think that this will strengthen the process that is used to build and vet software, but I would still say the message to the consumers of America should be clear: you are far safer if you update your software. It is a little bit like thinking——

Ms. KELLY. And what——

Mr. SMITH. Well, one seat belt may have a defect, but you should still put on your seatbelt. You are going to be far safer every day if you update your software.

Ms. KELLY. Thank you so much, and thank you to all the witnesses. And I yield back the balance of my time.

Mr. KRISHNAMOORTHI. Thank you, Congresswoman Kelly. Next, I would like to recognize the gentlelady from Tennessee, Congresswoman Harshbarger. You are on the clock.

Mrs. HARSHBARGER. Thank you, Mr. Chairman. I guess I just have a statement first, and then I will go into a question. Since we don't know how the malicious code was inserted into the software updates, which is unbelievable, and several of you have said that the U.S. Government needs a national strategy to strengthen how we share threat intelligence between the U.S. Government and the private sector, you know, we are constantly patching and adopting continuous updates, and it has been a standard of cybersecurity best practices measures for years. I guess I was looking at testimony from Tuesday, and, Mr. Mandia, in your testimony, you mentioned that the adversary was able to disarm some of your sensors as part of the intrusion. Can you tell us what you mean by that?

Mr. MANDIA. Absolutely. When the implant in the SolarWinds software ran, one of the first things it did, 11 days after it installed—mind you, it slept for the first 11 days—is it looked at the system it was running on, and it looked for common safeguards, like Windows Defender, like CrowdStrike, like FireEye's Endpoint, and it shut them off. And, again, the implant ran at system level. It had the permissions to do whatever it needed to do, so it just said, "What security is running? Kill it," and that is why we couldn't detect it in the first stage of the attack.

Mrs. HARSHBARGER. Thank you for that. Also, Mr. Smith, in your testimony on Tuesday, you said that while the adversaries had gained access to your source code, you don't consider the code to be particularly sensitive. And I guess from media reporting, it has been suggested that this effort by the adversary allowed it to exploit the identity and authentication features of Microsoft in other breaches of entities. Can you tell me a little bit about that?

Mr. SMITH. Yes, there are two different concepts in your question. I mean, first, you know, we share our source code broadly. We share it with all of our employees, and the secrecy and the security protection of our technology is not based on the secrecy of the code itself. We live in a world where, you know, much code is published, you know, to the world on the internet in open source form. The second part of your question then goes to, you know, our services overall, and I would say a couple of things. In no instance did we identify any action or case where anyone was able to use Microsoft's services as a vector of attack, as a means to attack any other customer. There are, you know, discussions that, you know, have ensued, rightly so, about the use of some industry-standard approaches for the authentication of accounts. Microsoft, like everybody in this business, supports these industry-wide standards. One of the standards, in particular, is 13 years old. It is called SAML.

It has been superseded, in our view, by something we have been encouraging customers and developers to move to since, but there was a vulnerability, so to speak, in SAML that was exploited in a

small percentage—and I think that is important to underscore as well—a small percentage of the instances that we saw. And it was only exploited after someone had already basically gotten elevated privileges, for example, by stealing a key or breaking a password. But nonetheless, I think this is quite rightly raising questions, how do we address this issue in the future. We are focused on that. Others are focused on it. I do think it is something that we will want to continue to work to address.

Mrs. HARSHBARGER. You know, honestly, coming from the private sector to the government sector, you know, we trust that those apps that we are installing, those updates on our Apple phone, on our watch, on anything that we do in a business environment or the government environment, we assume that it is safe because it has been vetted. I guess my question is, how can we be assured in the future that these software updates are going to be safe, and, in your best estimate, you know, how soon are we going to be attacked again, I guess is my question. We update every day something, and that makes me a little fearful going into the future.

Mr. SMITH. Well, I think there are two things that we need to do to better secure this kind of software updating. The first, as Kevin Mandia was saying before, is we are going to need to work with everyone who creates software to secure what is called their build process and to vet the software that is built. You know, at a company like Microsoft, we have an extraordinary range of controls to address that, but, you know, software is being built by companies and other organizations, large and small. And second, I think this is why it is so important for the government itself to send a message to the world that this type of indiscriminate and disproportionate tampering with the software supply chain is a violation of international norms and rules, and there will be accountability when foreign governments do this.

Mr. KRISHNAMOORTHI. Thank you. The gentlewoman's time is up.

Mrs. HARSHBARGER. Thank you, Mr. Chairman.

Mr. KRISHNAMOORTHI. Let me now turn to Congressman Eric Swalwell, the distinguished member from California. You are on the clock. You are muted.

Mr. SWALWELL. Thank you, Mr. Chairman. Thank you, panelists. This attack, I think it is pretty clear, was done by Russia, likely its intelligence services. That is what public reporting has shown. So, Mr. Smith, we know that Russia does not have much use for economic espionage. They are just not a country that is stood up in a way that they can benefit like our other adversary, China, who commits economic espionage every single day. However, this attack does touch not only on public-sector networks, but also private-sector networks. How much worse could this have been if an adversary, like China, had gone as far down the stack as Russia?

Mr. SMITH. I don't know that I have the best answer to that question. I guess I would say we need to recognize that we live in a world where there are multiple governments that are investing in these kinds of cyber intrusion capabilities. They may act based on different motives, and they may use what they obtain for different purposes, and we do see that in a somewhat diversified way around the world. I guess you could say, you know, it can always be worse. It could have been worse, and obviously it could have

been much better. I think the most important thing is that we learn from this, recognize that it is a dangerous world in which we live, and we are going to have to strengthen our defenses.

Mr. SWALWELL. Mr. Smith, earlier my colleague, Mr. Krishnamoorthi, who is also on the Intelligence Committee with me, asked you whether the House of Representatives, Senate, or Office of the President's systems had been penetrated that had Microsoft platforms, and I believe you said no. How about in the last election cycle, in the current cycle we are in? Microsoft was quite helpful in actually being the first to report that, I think, some campaigns had been breached even before the U.S. Government had told Congress. Have you seen any recent attacks against members of the House or the Senate and against their campaigns?

Mr. SMITH. I am not aware of anything since the last election ended. That doesn't mean that there hasn't been anything, but nothing has crossed my desk. You know, we certainly did see a series of intrusions, hacks, attacks, if you will, during the last electoral cycle, as you mentioned. You know, we did bring that information forward. You know, we have created an offering called AccountGuard that we provide free of charge to every Member of Congress, every political campaign, to think tanks, to the political parties, if they are using Office 365. We provide this at no additional cost, and what we do is employ our Threat Intelligence Center to constantly look for these kinds of attacks and then let people know if we find something, and we do that immediately.

Mr. SWALWELL. Thank you, Mr. Smith. Mr. Ramakrishna, you alluded earlier that you believe that having some sort of, not incentive, but safe harbor to disclose breaches would likely result in more cyber companies or companies writ large disclosing breaches. Can you elaborate on that? How could we make sure that, one, consumers are able to hold companies accountable if there is a breach that the company was responsible for, but that we would still be able to see companies disclose breaches early to protect consumers? And I think in tort law, for example, you know, if your restaurant is being sued because a deck collapsed and the restaurant took measures to fix the deck, they could still be sued for the injuries of the deck collapse, but it could not be used against them if they sought to fix the deck collapse. Can you just talk about how can you make sure consumers are protected, but industry is still disclosing and has an incentive to do so?

Mr. RAMAKRISHNA. Congressman, thanks for that question. Where we are coming from on this topic is that, as companies discover malware and other vulnerabilities, the fact of the matter is no matter how many resources any one of our companies have, no matter what level of controls we have, all of our software has some form of vulnerabilities or another. When we discover those, we should be able to not only fix them, but also share them with others such that each one of us are not discovering the same issues over and over again and, in that process, losing time. So, where we are coming from is the early disclosure so that we don't have to repeat the same situation over and over again, both at the customer level as well as at a software supplier level, must be eliminated.

So, the challenge here is one of potential litigation and one of, as I described it, victimizing the victim itself for coming out. And

those are things that need to be eliminated or those stigmas need to be eliminated for more of us to come out and speak openly. Obviously, today, three of us have come and spoken about it. We should get more vendors and more customers to speak up so that we can together solve this problem. It is not purely one of resources. It is one of how resources use information and share it for our collective benefit.

Mr. SWALWELL. Thank you. I yield back.

Mr. KRISHNAMOORTHI. Thank you so much, Mr. Swalwell. Next, I would like to recognize the gentlewoman from Iowa, Mrs. Marionette Miller-Meeks.

Mrs. MILLER-MEEKS. Thank you so much, Mr. Chair. I want to also thank the extraordinary knowledge of our witnesses' testimony. And also, as a former Army veteran, or as an Army veteran, I want to thank Mr. Mandia specifically for his service. This is a tremendously important hearing, and as I have listened to the testimony of our witnesses and both the insightful questions from my colleagues and the answers provided by our expert witnesses, I am reminded of pulling a single thread which then unravels an entire garment. You know, we are all a weak link in this system.

So, like many people, I am a doctor. I interface with a hospital system and have protected health information that I am concerned about and concerned about my own financial information. But when I have to change my password every two months and when I have to do my security training every year, I perceive it as a nuisance, and I don't think I am alone in that. However, what you all have brought to our acute awareness and alarm, we are all each individually a weak link as we interface and interact both in our private lives and with state and Federal Governments.

So, Mr. Ramakrishna, as the CEO of SolarWinds, and, granted, only a very brief time, and I can only imagine coming into an organization as the CEO with this overhanging your new tenure, you have been very forthright about some of SolarWinds' security culture challenges from the past and how you have leaned into improvements to the security culture, particularly around software development practices. We need to use events like these as collective learning moments to raise the overall tide level for everyone. The stakes are just too high to stand idly by. What role do you think companies like SolarWinds have to use their experiences and past challenges to promote better practices ecosystem-wide?

Mr. RAMAKRISHNA. Congresswoman, thank you for your question. We take our obligation to be a very active participant in this. While we were subject to this attack, we have learned a lot as well, and I will elaborate on one specific thing. I am happy to elaborate further as you please. As it relates to supply chain, one of the key challenges that we have uncovered as part of this attack is, typically all of us as software vendors use our certificate to sign the product that we deliver as the mark of integrity of the software that we deliver. Obviously, in this particular unique supply chain attack, that mechanism is not sufficient.

So, one of the improvements that we are making, which we are also publishing both to CISA and others as well as our industry colleagues, is a different way and an enhanced way of building software that gives more confidence and trust to customers as to how

it needs to be done that does not only rely on age-old ways of signing with our certificates, and instead, having parallel build environments that are managed and accessed by different sets of engineers. And that is an investment that we are making in that process to ensure that, across parallel build environments, the integrity of what we deliver is assessed and not compromised. So, that is a unique way of doing things and an extended way of doing things based on this very specific learning that we intend to publish externally as well.

Mrs. MILLER-MEEKS. Thank you so much for that. And, Mr. Smith, before my time expires, you alluded to this earlier when you spoke about training your customers. And so do we need to have more broad-based security training for all of us as individuals, again, as we interact and interface with both local, state, and Federal Government entities? As I mentioned, it has been raised to my alarm that we are all a weak link, and I am going to have better security measures going forward.

Mr. SMITH. Well, I first want to say we really appreciate the leadership you have provided in focusing on state and local needs, and, you know, highlighting some of the kinds of ransomware attacks in a place like Iowa, because I do think that that really highlights that this happens in, you know, every part of the country. I hope we don't need to ask every individual as a consumer to, you know, suddenly spend a lot more time than they do today. Our goal is to make it easy and simple for individual consumers to simply, you know, turn on something like Microsoft Defender and let it go to work. But I think when we get to organizations—a hospital, a school, a municipality, a state agency—you know, that is where we need more personnel. We do need more training, and we are going to need more tools, which we are absolutely committed to providing.

Mrs. MILLER-MEEKS. Thank you so much. I yield back my time.

Ms. NORTON. [Presiding.] We will take a recess at this time. We are not through. Excuse me. There is somebody there ready to go, so excuse me. I understand that Miss Rice of New York is prepared to come forward at this time. Miss Rice, you are recognized for five minutes.

Miss RICE. Thank you so much, and I want to thank our witnesses today. This is incredibly enlightening at a critical time. But I also want to thank my colleagues on both sides of the aisle because the one message that I am getting loud and clear is that we can be doing better. It is one thing to have all of our witnesses here talking about what they are doing, but we need to actually act as well.

So, Mr. Smith, a consistent theme in today's conversation has been that the U.S. Government needs to improve and incentivize intelligence sharing between Federal agencies and the private sector. I believe that you have called for the Federal Government, and forgive me, I had to

[inaudible] so I left for a little while. I don't know if you addressed this. But you have called for the Federal Government to impose clear cyberattack reporting requirements on the private sector, and you have pointed to the EU's law requiring digital service providers to notify authorities of incidents as a model to follow.

Would you consider the EU the gold standard around the globe, and are there any other countries we can look at to emulate what they are doing and recreate it here?

Mr. SMITH. Well, I definitely think we should learn from what the European Union is doing. I don't know if I would call them the gold standard, and there are others worth looking at as well, and I should do some more homework and get you some more examples. I think we need something that works for the United States, and I think we can put something like that together. Yes, I think we have had good conversation here on some of the specifics. You know, it is not something that needs to apply to everyone in the country, but it definitely should apply, at a minimum, to, you know, those entities like my own that are part of the critical infrastructure for the country and that are obtaining this kind of information. I think we can put together a gold standard ourselves as a Nation in terms of reporting the right information to the right people as rapidly as possible, and then I think, critically, sharing back the right information in an appropriate way as well so that we are better informed about what to look for.

Miss RICE. Well, I hesitate to speak for every one of my colleagues on this hearing, but I, of course, stand ready to work on that with you. Mr. Mandia, in a similar vein, you have argued that the U.S. should establish a confidential information sharing solution to encourage public/private communication after breaches. And I believe you pointed to the FAA's Aviation Safety Reporting System, which uses non-punitive anonymous reporting to encourage the private sector to communicate about threats. To your knowledge, do any countries take a similar approach to encouraging the private sector to identify and address threats?

Mr. MANDIA. I think nobody does it exactly right. I have seen a lot of nations go through a lot of different evolutions, you know. I look at the U.K. They do a better job, in my opinion, of private and public partnership. They have more centralization of how they respond to incidents such as this. You look at Israel, much smaller scale, but, you know, they have their Iron Dome in how they approach threat intelligence sharing there.

But my remarks were basically about if the threat intelligence sharing is not confidential, then as a reporter of threat intel, you have to get your arms around all the liabilities first, and it just creates too much delay, too much time, and the intel won't be actionable. So, I believe threat intelligence needs to be shared quickly, and I think you can define first responders in the industry, folks who respond to unauthorized, unlawful, or unacceptable behavior. If you do that for a living or provide those services and you see something, you can report that very confidentially. You can defend the Nation. You can get it to the right government entities, and, quite frankly, let the company get their arms around, "So, what did we lose?"

And realize this: a lot of disclosure creates fear, uncertainty, and doubt that is unnecessary. Most organizations, when they have a breach, lack the expertise to get a full scope of what did we lose and what should we do about it. They can't do it, and they are just going to scare the heck out of everybody by saying, "Hey, we had a breach," and everybody goes, "Well, what does that mean? What

does it mean to me?" And it could just be a small thing, a small matter that doesn't impact the consumers. So, every organization will need some time.

Miss RICE. So, let me just ask you, Mr. Smith and Mr. Mandia, you know, what we are talking about today shows a level of human weakness and bad cyber hygiene. What steps could we take here in Congress? I mean, I am calling for all of the members to be required to have cyber education, which we are not required to do. How can we improve our cyber hygiene at the Federal level?

Mr. SMITH. Kevin, do you want to go, or do you want me to go first?

Mr. MANDIA. Brad, you can go first.

Mr. SMITH. OK. Well, I would say, first of all, I think your question is very important in the sense that everybody talks about technology, but, ultimately, it is always about people. And I think what it really connects with is the need to have, you know, consistent training, consistent implementation of what we all recognize today, our best practices, and ultimately an expansion of the work force in the cybersecurity field so that we have more trained people who can support all of the organizations and customers across the country.

Ms. NORTON. The gentlewoman's time has expired. The witnesses have asked for a 10-minute recess. They are really entitled to that. This is a long hearing because there are two committees meeting and asking questions, but we don't want it to go on forever, so we will take a 10-minute recess at this time.

[Recess.]

Ms. NORTON. The committee will reconvene. We have a very large set of members because there are two committees. This is a joint hearing. That is why this is going on for so long. I want to call on the next member on my list. It is Mr. Clyde of Georgia. You are recognized for five minutes.

Mr. CLYDE. Thank you, Madam Chairwoman. As a Navy officer, a Navy combat veteran, I am quite aware that our military is tasked with protecting our Nation, and we take that very seriously and have been very successful in doing that for over a century. But cyberattacks on our country are something that literally can go right through whatever military protections we have, and can affect especially our civilian population in ways that can be devastating for medium businesses, large businesses, and even small businesses. So, several of you have said that the U.S. Government needs a national strategy to strengthen how we share threat intelligence between the government and the private sector. So, would each of you give me an idea of how you would see this playing out? What role do you see CISA playing to help support this, especially when it concerns the private sector? And I guess we could start with the CEO of SolarWinds.

Mr. RAMAKRISHNA. Congressman Clyde, thank you again for the question. In terms of CISA, there are a few things that we can work with CISA on as part of a private sector entity. One is CISA can essentially be the clearinghouse of all threat information that is given to it by the public sector. That is No. 1, and the converse is true from a private sector information gathering standpoint as well. Once it has got a coordinated set of information, it can take

the responsibility to disseminate it to all impacted and potentially impacted parties as well. That will ensure that we are all coordinated, that we are fast and agile in learning and responding. The other major area that I would suggest is CISA can be a big influencer in establishing best practices and disseminating best practices across the entire value chain, not just in the threat aspect of it, but in the standardization of it, such that as things become more standard and more of us in the private sector follow, then potential for leakage across private sector entities is significantly reduced and diminished.

Mr. CLYDE. Thank you. I appreciate that. Mr. Thompson, any comments from you, sir?

Mr. THOMPSON. Yes. The only thing I would add to what Sudhakar said is I do believe that CISA has an opportunity, based on where it sits in the government, to really coordinate resources from both the private and public sector. I think as private sector software companies, we would be willing to dedicate some amount of resources to work with CISA in coming up with cybersecurity strategies for both the private and public sector. But someone is going to have to be the coordinator of that, and I think CISA might be, if resourced appropriately, be in the right position to be able to do that.

Mr. CLYDE. Thank you very much. Mr. Mandia?

Mr. MANDIA. Yes, not too much to add to that other than when I think about intel sharing, if there is intel in, it makes sense that it goes to a single entity and the government. If there is intel out, that has got to be communicable to all the technology companies that safeguard the Nation in the private sector, public sector. And then there has got to be a prioritization, that there is probably different industries—healthcare, utilities, telecom—that rise above some of the others that you got to make sure abide by certain legislation standards or regulations, and most of those are regulated industries. But that is how I think about it: intel in, then intel has got to get out, and then we get a Nation that can put shields up a lot faster than it can today.

Mr. CLYDE. Thank you. Thank you. And last, Mr. Smith.

Mr. SMITH. Yes, I think these provided good perspectives. The one thing I would add is, obviously this is a paradigm where CISA would be responsible for the assessment of threat data that is being reported domestically from companies inside the United States. You know, at the same time, you still have the NSA, which has this critical responsibility and role with respect to data, that it is able to identify from outside the United States. And then for the government as a whole, you need to have, you know, both of these sources to get the full picture of the threats to the country.

Mr. CLYDE. OK. Thank you very much. We had quite a serious ransomware attack in my district to a private company that basically shut them down for five weeks and cost them almost $10 million, so this is very, very important what we are doing here. Thank you, Madam Chairwoman, and I yield back.

Ms. NORTON. I thank the gentleman for his questions, and his time has expired. I call on Ms. Tlaib of Michigan now. Ms. Tlaib, you are recognized for five minutes.

Ms. TLAIB. Thank you so much, Chairwoman. Mr. Thompson, you served at SolarWinds for 14 years, including 10 as its CEO, so I just want to make sure it is fair to say that you know this company better than anyone. I think Bloomberg News said two former employees viewed your company's security lapses as so significant that they said they viewed a major breach as inevitable. So, one of those employees, Mr. Ian Thornton-Trump, said that he warned the company in 2017 of security risks, but found the company's executives were, and I quote, "unwilling to make the corrections." So, Mr. Thompson, I am sure you were expecting this question, but, you know, did you all take immediate action when these concerns were raised?

Mr. THOMPSON. So, I believe we have taken this security of our customers, of our company, of our products seriously my entire tenure at SolarWinds. I believe we have invested at the appropriate level. In fact, over the last four years, we were spending at a level meaningfully higher than the industry average.

Ms. TLAIB. When did you all start investing in security?

Mr. THOMPSON. We have been investing in security since we got here, but obviously that security investment has grown as the company has grown. But if you look back to 2016, in 2016, we really looked at the business. We looked at where it was, and we began to invest at a higher level. We brought in a CTO who had been a CIO for many years. In early 2017, we brought in a very experienced CIO. We then added a VP of security who deals with product security——

Ms. TLAIB. And this all happened in 2016?

Mr. THOMPSON. In 2016 and 2017.

Ms. TLAIB. So, Mr. Thompson, is it true, and this is something when the committee told me, I was kind of in disbelief. If all that was going on, then why in 2019 it was said that you could easily access your server by simply using the password "SolarWinds123?"

Mr. THOMPSON. So, that related to a mistake that an intern made, and they violated our password policies, and they posted that password on their own private GitHub account. As soon as it was identified and brought to the attention of my security team, they took that down.

Ms. TLAIB. Yes. You know, it just doesn't, you know, invoke a lot of confidence when many of us when we hear it is an intern could have done that, and, again, that same password was used to access your server. The other one, is it true that SolarWinds did not create a role of a vice president of security until 2017?

Mr. THOMPSON. So, we did not have a role for vice president of security, but as I have said, we had a very sophisticated CIO and a CTO who had been a CIO at a very large Fortune 500 company, and we had a security team, and we had a security process. We just didn't have a VP of security prior to that day.

Ms. TLAIB. So, with all those people, two years later, 2019—I don't know if they were in place—you know, how fast did you fix the issue with the "SolarWinds123" password to access your servers?

Mr. THOMPSON. As soon as it was identified to us, it was fixed almost——

Ms. TLAIB. Days, weeks, months? How long?

Mr. THOMPSON. Faster than days once we found out about it.

Ms. TLAIB. Well, it also has been reported that back in October, another security company, Palo Alto Networks, raised concerns with SolarWinds about—am I saying it right, Orion product—based on behavior that they had observed, which is now believed to be related to the cyberattack. What steps did you all take to ensure that this issue was investigated, Mr. Thompson?

Mr. THOMPSON. So, I will pass that to Sudhakar because I have not been the CEO since December 31 of 2020, and there have been a lot of investigation work done since then. So, I will let Sudhakar respond to that.

Mr. RAMAKRISHNA. Thank you, Kevin.

Ms. TLAIB. You got any interns messing up, Mr. new CEO? So, I would love to hear about what you all are doing about these concerns raised in October.

Mr. RAMAKRISHNA. We heard about it from Palo Alto as a possible victim of the malware that was delivered as part of the Orion code and related issues. It wasn't about the security hygiene or security posture of SolarWinds itself. In fact, we are a customer of Palo Alto's, and we have 44 pairs of Palo Alto infrastructure protecting us, not just from a firewall standpoint, but also doing some threat hunting within our environments today.

Ms. TLAIB. Well, I appreciate all of that. I just want my colleagues to understand it is not only that we need to find out what they were able to access, but the fact that, you know, SolarWinds did have a weak security culture that, you know, ran right up against this attack. And we need to acknowledge that because, I mean, I understand that there was just a recent post on LinkedIn for different security positions you guys may have posted recently. And so I just really want to make sure that, again, my colleagues, that we are all doing our due diligence in regards to some of these companies that we contract out to, to protect the privacy and protect our country from these kinds of attacks. With that, I yield. Thank you so much.

Ms. NORTON. The gentlewoman's time has expired, and I thank her for yielding. Mr. Fallon of Texas is next.

[No response.]

Ms. NORTON. Mr. Fallon, are you there?

Mr. FALLON. Yes, ma'am. Can you hear me?

Ms. NORTON. I can hear you. You can proceed.

Mr. FALLON. Well, thank you very much, and I want to thank the witnesses for bearing with us in a joint committee. I know it has been a long day thus far. You know, what alarmed me when I was reading through sourcing material was the fact that, and it really got my attention, was the fact that the Secretary of Homeland Security's own email had been compromised. Mr. Mandia, thank you for your service to our country. I wanted to ask, in your opinion, what would have happened and how much more damage would or could have been done if your company hadn't discovered this breach in December 2020?

Mr. MANDIA. Well, you know, I think over time, people would have come across enough smoke to find the fire, so it would have been discovered in time and people would have connected the dots. We just happen to be a forensic firm and, you know, special ops

met special ops. We responded appropriately with the right skill sets, found the implant. In regard to what could have happened, the attacker had unfettered access to over 17,000 different organizations and nobody saw it. So, this attacker stayed laser focused on stealing specific information. They showed, arguably, constraint, and they didn't do anything destructive, but in reality, sir, it would have been easier for this attacker to destroy data than do the operations that they did. So, I think there was a range of options for the threat actor to behave like, and they behaved in a manner to steal emails and documents that they were targeted in collecting.

Mr. FALLON. Just to followup on that, if they chose to start destroying data, would that have, in and of itself, kind of raised red flags, and would they have discovered it then? Is that the reason why they wanted to do that?

Mr. MANDIA. I think there is a line of, you know, you are going to start noticing if machines get shut down or if data starts getting deleted. My observation on the rules of the playground in cyber, maybe we don't have written rules that everybody follows all the time, and maybe it is hard to get people to agree as to what is fair game for espionage, but here is one thing I do know. I don't think any modern nation wants to see modern nations' A-teams break in and start changing data, deleting data, putting industrial control system malware in place, and doing certain things that I still haven't seen done by those threat actors that are representing a foreign intelligence service. So, there are still another couple levels of escalation that have not, at least I haven't witnessed yet in cyberspace.

Mr. FALLON. OK. Thank you. Mr. Thompson, in retrospect, was this breach, in your opinion, preventable, and if so, what should SolarWinds have done differently?

Mr. THOMPSON. So, I will answer part of that question, and I will let Sudhakar answer some of it because, as I said, I have been gone since December 31. But this attacker designed this attack to be very, very difficult to find. They were incredibly patient. They moved very slowly. And the software was of tremendous complexity, and so it was designed in a way that made it very difficult for anyone to detect whether it was us or whether it was FireEye or Microsoft, which is why it took as long as it did. And I will let Sudhakar add what we have learned since December.

Mr. FALLON. Thank you.

Mr. RAMAKRISHNA. Congressman Fallon, in addition to Mr. Thompson's comments, the way we looked at it is, given the novelty of the supply chain attack and, as I described it, the attacker hiding in plain sight, the fundamental things that we are looking at is what do we learn from this. How do we protect supply chains of companies like SolarWinds and our industry peers going forward? That led us to build the initiative that we call Secure by Design internally, which provides specific guidelines and execution tactics of how to protect internal environments, how to make build systems a lot more robust, including access to the build systems, and then how to evolve software development life cycles to be much more secure development life cycles where you are not testing security after something is delivered, but designed as you build it. And I believe that is the responsibility of the industry to take more

ownership of and share that not just amongst us, but also with our government colleagues who also build software.

Mr. FALLON. Thank you. And I have one quick last question for Mr. Mandia. While the experts seem to think that this was a nation-state-sponsored attack, I am guessing because of the complexity of it all, but I am a lay person. I just look at it in layperson's terms. Why are we so sure that it was nation-state-sponsored attack and not just a group of highly talented, albeit nefarious, cybercriminals?

Mr. MANDIA. So, I started responding to breaches in the United States Air Force by 1995. Back then, most of the breaches we responded to were not attractive nuisances. It was dot-gov against dot-gov, dot-mil against dot-mil. I have got about seven reasons why I believe it is a foreign intelligence service. I will give you two. FireEye was attacked by over 20 different IP addresses, and we were a Stage 2 victim of this attack after we did a SolarWinds update. The systems used to attack us were used in exactly zero other breaches. That is very uncommon, sir. What normally happens, if I am a threat actor and I am doing ransomware, I have the same infrastructure for every attack I do. We went through our partners Microsoft, our partners in the intel community. None of the systems are used to attack anybody but FireEye. I have got six other technical reasons. I am happy to take them offline with you.

Mr. FALLON. Thank you.

Mr. MANDIA. I have virtually no doubt, 10 minutes into the first briefing I got on our incident, this was a foreign intelligence hack, and I had a good idea which one.

Mr. FALLON. Thank you very much. Thank you, Madam Chair. I yield back.

Ms. NORTON. Yes, the gentleman's time has expired. Mr. Correa of California.

[No response.]

Ms. NORTON. Mr. Correa of California, are you——

Mr. CORREA. Can you hear me OK, Madam Chair?

Ms. NORTON. I can hear you now, sir.

Mr. CORREA. Thank you, ma'am. I want to thank all of our chairs and ranking members for this most important hearing. I wanted to ask a question of all our guests, Mr. Ramakrishna, Mr. Smith, Mr. Mandia. The question is as follows: Is this a political diplomatic issue, or is this a technical issue? And I ask this question because, Mr. Smith, during your presentation you said that we needed to strengthen international law and the consequences for violation of international law. Yet I recently read a report that talked about the Chinese intelligence, that they had stolen our espionage code and essentially customized it and were using it against us. So, those folks overseas, are they better than we are now? Are Russia, China, and others better than we are in this cyber battlefield, and if they are, how do we stop them? So, again, my question is, is this an international law consequences issue, or is this a technical issue? To all our guests, please.

Mr. SMITH. Well, I am happy to field that first. You know, I think you framed the question well. Is it a diplomatic issue or is it a technical issue? Yes. That is a way of saying it is both, and we need to deal with it on both levels. And I don't believe for a mo-

ment that we live in a world where our adversaries are more capable than our own government, but we do live in a world where there is an asymmetry. It is easier to play offense than it is to play defense. When you play offense, you can scan the horizon and look for the weakest point, and then that is where you direct your energy. And when you are on the defensive, that means you need to scan and secure the entire horizon.

So, on the technical side, that means that there this enormously important work to strengthen all of our cyber defenses, and it equally makes it a critical diplomatic and international legal issue because it simply must be the case that there are certain acts that are put off limits and for which there are international and diplomatic consequences. And this kind of indiscriminate and disproportionate attack on the software supply chain is and should be one of them.

Mr. CORREA. Mr. Ramakrishna, Mr. Mandia, go ahead.

Mr. RAMAKRISHNA. Congressman Correa, I agree with my colleague, Brad Smith, that it is a technology as well as a political diplomatic issue. Especially as it relates to the private sector, we have to learn and anticipate issues like this and collaborate together on coming up with best practices similar to the ones that we are trying to do at SolarWinds with our Secure by Design and some new things that our colleagues at Microsoft and FireEye, CrowdStrike, KPMG are doing. Additionally, I think internally within the United States, we need to look at our disclosure rules and, as we have all been saying, encourage more of us to come forward and disclose without fear of being punished either in the public or legally. So, that is as it relates to us in the U.S.

And then diplomatically, setting some ground rules, holding people accountable, and driving consequences is, I would say, the help that we can get from the government. And last but not least, the point I have highlighted a couple of times today with regards to the need for speed and agility in terms of information sharing and information dissemination might require some help from lawmakers such as yourself.

Mr. CORREA. Thank you. Mr. Mandia?

Mr. MANDIA. Yes, I think everything both the witnesses have said is exactly right. It is a diplomatic issue. It is a technical issue. What I have learned over 20 years-plus in responding to security breaches, sir, is that all the threats we respond to literally mimic real-world geopolitical conditions and really economic alliances as well. So, when you look at what the threat is to the United States in cyber, it is North Korea, it is Iran, China cyberespionage, it is Russia, and then it is just folks who are safe harbors for ransomware, so it is going to take diplomacy. It is going to take technology. It will be both.

Mr. CORREA. In my last seconds I have, Mr. Smith, you talked about a community college being enough to get cyber education. Do you have a list of community colleges that offer that education now?

Mr. SMITH. I will see what we have.

Mr. CORREA. Do you know of any? Do you know of any?

Mr. SMITH. Oh yes.

Mr. CORREA. It is not a "gotcha" question. Are you showing us how far we have got to go?

Mr. SMITH. No, actually the community colleges of the country have created the kinds of courses that we need. They have become a much more common part of the curriculum. You know, we have a robust cybersecurity profession in the United States. We just need to make it larger. And so I think we can harness what exists and expand the capacity and basically make it financially easier for people to go get these courses and education.

Ms. NORTON. The gentleman's time has expired, and I thank the gentleman for his questions. Mr. Gimenez of Florida?

[No response.]

Ms. NORTON. Mr. Gimenez of Florida, are you there?

[No response.]

Ms. NORTON. You are recognized for five minutes.

[No response.]

Ms. NORTON. You are recognized for five minutes. I see you, but I don't hear you.

[No response.]

Ms. NORTON. I will go to the next person. Mr. Donalds of Florida.

[No response.]

Ms. NORTON. Mr. Donalds, are you there?

[No response.]

Ms. NORTON. Let us then go to Ms. Porter of where?

Ms. PORTER. I am from California, ma'am.

Ms. NORTON. All right. Ms. Porter of California. Sorry.

Ms. PORTER. Thank you so much. Mr. Ramakrishna, we are here today to talk about a major security breach. Why are security breaches a problem? Very briefly just in a few words, what are we worried about?

Mr. RAMAKRISHNA. They could impact people at a personal level through theft of credentials. They could impact companies with regards to breach of sensitive information and data, and they could impact——

Ms. PORTER. Wonderful. Mr. Ramakrishna, do you want to please provide your home address for the committee today and the American public?

Mr. RAMAKRISHNA. I am happy to provide it, Representative. I would like take down record and provide it offline.

Ms. PORTER. So, you don't want to share it with the whole world, like with Russia.

Mr. RAMAKRISHNA. Yes.

Ms. PORTER. So, you would agree that the information that got hacked is national security information that is damaging to national security implications. It could literally put lives at risk. You don't want to even give out your address, much less personal security information. What kind of legal liability is SolarWinds facing for this hack?

Mr. RAMAKRISHNA. Congresswoman Porter, we have our standard end user licensing agreements that we signed with every one of our customers, including our Federal customers, and we are bound by those.

Ms. PORTER. So, your customers can sue you? There is a law that makes you legally liable for this data breach.

Mr. RAMAKRISHNA. I do not have the details of it, Congresswoman. I am happy to find out those specifics from our teams and furnish them to you.

Ms. PORTER. OK. Mr. Ramakrishna, does this look familiar to you?

Mr. RAMAKRISHNA. Yes.

Ms. PORTER. "SolarWinds123." Is it true that some servers at your company were secured with this Cracker Jack password, "SolarWinds123?

Mr. RAMAKRISHNA. Congresswoman, I believe that was a password that an intern used on one of his GitHub servers back in 2017, which was reported to our security team and it was immediately removed. And that particular——

Ms. PORTER. Mr. Ramakrishna, reclaiming my time, I have got a stronger password than "SolarWinds123" to stop my kids from watching too much YouTube on their iPad. You and your company were supposed to be preventing the Russians from reading Defense Department emails. Do you agree that companies like yours should be held liable when they don't follow best practices? Yes or no.

Mr. RAMAKRISHNA. Congresswoman——

Ms. PORTER. Should there a national breach law?

Mr. RAMAKRISHNA. We believe we take our security as well as the security of our customers very, very——

Ms. PORTER. Reclaiming my time, Mr. Ramakrishna. I am sure you take everything seriously. You seem like a very serious person. But I am asking you, should there be a breach law. Let's move on. Mr. Smith, should there be a law requiring companies to notify Federal law enforcement when they have had a cybersecurity breach, yes or no?

Mr. SMITH. Yes, I believe there should be a law that applies to some, and then we should decide who they notify. I am not sure it should be law enforcement. It could be an organization like CISA.

Ms. PORTER. Excellent. Mr. Smith, thank you for that. Earlier this week, you told the Senate Intelligence Committee that it took "courage" for FireEye and SolarWinds to reveal this hack to authorities. What did you mean by that?

Mr. SMITH. What I mean is you have three companies here today because we have chosen to share information. At Microsoft, we have published 32 blogs about what we observed and what we have seen. If I take my colleagues at Google and Amazon and put them together, they have published one blog. They didn't get an invitation here as a result.

Ms. PORTER. OK. So, Mr. Smith, I appreciate that, but you are not really saying we should give you some kind of Scout badge for telling the Federal Government that the Russians are waist deep in your source code. I mean——

Mr. SMITH. No, I did not ask for any kind of badge.

Ms. PORTER. Well, that is good because I am not going to give you one, so we are in agreement.

Mr. SMITH. I didn't think you would.

Ms. PORTER. Do engineers or people at Microsoft, to come forward and reveal these kinds of breaches, do they have protection? Can they do so without fear of retaliation?

Mr. SMITH. Within our company? It is their job to bring this kind of information——

Ms. PORTER. Is that true at every company, Mr. Smith? Should it be true at every company?

Mr. SMITH. I think it should be true at every company. Yes, I believe that.

Ms. PORTER. There should be whistleblower protection so that companies don't have to rely on corporate courage.

Mr. SMITH. Well, I think that you need whistleblower protection, but, more important than that, we need to pay more people to make it their mission in life, their job, to do this kind of threat hunting, find these kinds of problems, surface them so then companies can solve them.

Ms. PORTER. Thank you very much. My time has expired.

Mr. SMITH. Thank you.

Ms. NORTON. I thank the gentlewoman for her questions. I recognize Mr. Meijer of Michigan for five minutes.

Mr. MEIJER. Thank you, Madam Chair, and ranking member, and to our witnesses who are here today, and I just want to kind of echo my gratitude for actually stepping forward. I am not sure it is within our congressional prerogative to offer merit badges, but I just want to thank you. You know, on February 17, Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger announced that hackers had launched the attack from obviously inside the United States using our own infrastructure. This is a question for the panel. Can you explain the unique challenges that are presented when we are having to mitigate the efforts of a foreign actor, but one that is using our own internal systems or domestic-based systems?

Mr. SMITH. Well, I will offer a couple of thoughts. We are in, like, hour five now, so we are sort of taking turns. You know, we have a well-established ability as a government, as a country through the National Security Agency to look at what is going on beyond our borders. You know, the question is, how do we take stock of what is going on inside the United States, especially when a foreign government can basically use a credit card and a false ID to get access to a server, you know, in the U.S. data center. It is not an easy problem to solve. I think we all would recognize we don't want to live in a country where there is, you know, extraordinary domestic surveillance, so we have to ask ourselves, well, how do we collect the information when there are these kinds of threats. And I think the first thing we should do is call on what I would hope would be, you know, sort of the loyalty of companies in the country to step forward voluntarily and share information.

But clearly that is not sufficient. It is not doing the job. And so I think we should put in place a legal obligation that certainly applies to, you know, companies that are in the critical infrastructure business, people that are the first responders. At Microsoft, we are a first responder. That is why we would say we would recognize that it is reasonable for this kind of law to apply to us. That creates the data that goes to the government. There needs to be careful thought to how it is used, with whom it is shared, when it is shared back with others in the private sector.

Mr. MEIJER. Thank you, Mr. Smith. I would hope that, you know, that sense of shared collective self-interest, not necessarily originating from a patriotic impulse, but at least just an awareness and understanding that when we are dealing with cybersecurity, the contagion component of it is essential. I mean, we are obviously referring to this as the "SolarWinds hack," and I know many have referred to it and are looking to kind of change that to "Holiday Bear," you know, the shift of the name. The tainting of the reputation all too often goes toward those who are willing to acknowledge what had occurred and to share it rather than not. And I guess on that point, Mr. Ramakrishna, I guess if you can just put it simply, I mean, why did you come forward to testify today?

Mr. RAMAKRISHNA. Congressman, we believe it is our obligation to learn from incidents such as this and be an active participant in the recovery and the remediation. As we heard earlier today, we need to bounce forward from this, not so much bounce back only. So, we have taken our learnings very seriously and have created an initiative within our company that we are sharing very publicly, and so I considered it my obligation to be very active in the bouncing forward aspect of this.

Mr. MEIJER. Thank you. And then just one kind of, I guess, more specific question, Mr. Ramakrishna. You know, I think it was determined by analysts that 30 percent of the victims had no direct connection to SolarWinds, but were still targets of the broader campaign. Can you share, you know, what methods were used to arrive at this understanding and, I guess, why they weren't targeted in a separate effort, why they were targeted using the SolarWinds access?

Mr. RAMAKRISHNA. That is not a study that we conducted, so I don't really have the specifics as it relates to the numbers. But the way I would describe this is, as I engage with national defenders across the world—for instance, we have spoken to the U.K. Cybersecurity Center—and as we were discussing other matters with them, they said they are actively investigating other supply chain attacks within the U.K. and other places. A few days ago, a French company reported a supply chain attack as well, so the point here being, multiple different vectors are being used. SolarWinds was one of them, but there are many different ways that threat actors are coming into various systems.

Earlier in the conversation today, I described the intruders as behaving like Transformer toys where they are changing their personalities and personas constantly, and that is the reason why I am urging all of us to share information as quickly as possible so we can together thwart these attacks.

Mr. MEIJER. Thank you, Madam Chairwoman. My time has expired.

Ms. NORTON. The gentleman's time has expired. I thank him for his questions. Mr. Gimenez of Florida.

Mr. GIMENEZ. Thank you. I hope everybody can hear me now. Thank you so much. I have got a couple of questions. Mr. Ramakrishna, you said that you are an American-based company and you talk about the supply chain. When you are developing software, especially

[inaudible], is it a bunch of people in a room developing the software, or do you, you know, sub that out to other parts of your supply chain, many of which could be offshore?

Mr. RAMAKRISHNA. Congressman, in this particular context, when we refer to supply chain, these are employees of ours that may be globally deployed. So, like many American companies, we have a global work force, and we have employees all over the world that contribute to the development of our software, which essentially is part of a supply chain that we deliver.

Mr. GIMENEZ. Where in the supply chain was this malware embedded?

Mr. RAMAKRISHNA. It was on a platform which we call the Orion platform. That is a product of ours.

Mr. GIMENEZ. No, I understand that, but where exactly? You said this software is developed from all around the world. Where was this malware embedded? Where did it come from?

Mr. RAMAKRISHNA. It is difficult for me to pinpoint a location, Congressman. This particular software is built in a combination of our various development centers, including in the U.S. and in non-U.S. locations.

Mr. GIMENEZ. So, somebody got access to your software development platform?

Mr. RAMAKRISHNA. Basically, what has happened is somebody got access to one of our build servers and hid a piece of malware on it that was observing when products were being built. And as products were being built, in one particular file, they were able to replace that and keep it in the building process.

Mr. GIMENEZ. Did you run the software through security checks before you introduced it into the general public?

Mr. RAMAKRISHNA. There are secured development practices that we had been adopting that were part of our standard software development processes, Congressman, which we have since learned on what else we can do. So, that is the initiative that I was describing earlier called Secure by Design.

Mr. GIMENEZ. Mr. Smith, you said that everybody should adhere to best practices. Are you saying that those Federal agencies that were infected do not adhere to best practices?

Mr. SMITH. I don't want to speak to any specific Federal agency. I will say that across 60 customers, you know, we saw typically a failure in one area or another to adhere to best practices. You know, we saw, for example, that, you know, passwords or keys were not kept in a secure location. We saw that there wasn't a practice called-least privileged access where you really try to give an individual access to only a limited part of the network. We saw instances, you know, for example, where there might not have been the use of multi-factor authentication. We definitely saw lapses which could have prevented the impact among certain customers of what happened.

Mr. GIMENEZ. Thank you. I appreciate that. Would it be fair to say that China, Russia, North Korea, Iran are the major players in this cyberwar that we are engaged in?

Mr. SMITH. Well, at Microsoft, we publish what we call a security defense report—I am forgetting the precise name; it came out in

September—and we catalogued all the nation-states, and all, except one nation-state actor, was from those four countries.

Mr. GIMENEZ. From those four countries, right?

Mr. SMITH. Yes, that is right.

Mr. GIMENEZ. OK. How would you gauge our United States offensive capabilities in cyberwarfare?

Mr. SMITH. I am definitely not the expert on that.

Mr. GIMENEZ. Fair enough. OK. And, sir, at Microsoft, are you in China? Are you in Russia?

Mr. SMITH. We do have personnel in both countries, yes.

Mr. GIMENEZ. In the Chinese subsidiary, are there Chinese interests that have an ownership stake in Microsoft?

Mr. SMITH. Not that I am aware of. We do certain work with joint ventures, but we operate through Microsoft Corporation and we operate through wholly owned subsidiaries. I am not aware of any other kind of structure.

Mr. GIMENEZ. Because, I mean, I have been made aware that if you are doing business in China, they need to have 51 percent ownership to do business in China. That doesn't apply to you?

Mr. SMITH. It certainly doesn't apply to Microsoft. I would want to go back. You know, it is a big company, and there are other companies we have acquired in recent years, and I would want to go back and look specifically at the ownership structure for each of those. We run through our own company.

Ms. NORTON. The gentleman——

Mr. GIMENEZ. Thank you, Madam Chair. I know my time is up, and I yield my time.

Ms. NORTON. I thank the gentleman for his questions. Next would be Mr. Johnson of Georgia.

Mr. JOHNSON. Thank you, Madam Chair.

Ms. NORTON. You may be muted, Mr. Johnson.

[No response.]

Ms. NORTON. Mr. Johnson, can you hear me?

[No response.]

Ms. NORTON. He may be having bandwidth problems. We may have to go on to another member while we wait for Mr. Johnson of Georgia, but just a moment, please, until I see who is next. Witnesses are in and out with votes, so it is difficult to know who is available. Just a moment, please.

[Pause.]

Ms. NORTON. Let us take a five-minute recess to see if there are members available. I apologize to our witnesses, but with the rolling votes, we are having this difficulty seeing who is available, but we will back in five minutes. Thank you.

[Recess.]

Ms. NORTON. I believe Ms. Porter of California is available. Ms. Porter, you are recognized for five minutes.

Ms. PORTER. Thank you so much, Ms. Norton, but I don't see Mr. Smith in the hearing. Is he available?

Ms. NORTON. There he is.

Ms. PORTER. Thank you so much, Mr. Smith. I see you now. It seems like one of the takeaways from this hearing is that successful cyberattacks are really a matter of when, not if. When investigating a cyber breach, it is helpful for companies to have com-

prehensive logs to review so that they know who accessed what, what settings were changed, and so on. Is that right? Those logs can be helpful.

Mr. SMITH. Generally, logs can be helpful. That is correct.

Ms. PORTER. And it is the cloud companies like Microsoft who keep those logs. The attacker who first got into SolarWinds' network did so in September 2019. How long does Microsoft keep network logs for?

Mr. SMITH. Well, logs are kept in a variety of circumstances, and they are kept by all kinds of companies, and they are kept by IT administrators, so I cannot give you a specific——

Ms. PORTER. Mr. Smith, how long do you keep logs for at Microsoft?

Mr. SMITH. I don't know. I would have to go ask, you know, and it would depend on which service and the like.

Ms. PORTER. So, based on my information, what I understand is that the range is fairly short, something between seven days and 60 days, and it depends, as you just said yourself, on what services the client has purchased, they can purchase to keep the logs more as part of a package. Everyone on this panel has said that successful attacks are basically inevitable, but you didn't sell the DOD the logs that they would need to be able to fully assess the damage?

Mr. SMITH. Well, I think the premise of that question is a little bit off, to be honest. First of all, there was no indication, to my knowledge, that the DOD was attacked. Second, I don't know what the DOD has purchased, you know, from us. Third, I don't know how long the logs would go back, you know, for services that we do provide to the DOD.

Ms. PORTER. Mr. Smith, do you own a toaster?

Mr. SMITH. I sure do. I own one.

Ms. PORTER. When you use that toaster, do you expect it to catch fire?

Mr. SMITH. I sure as heck don't. No, I do not.

Ms. PORTER. So, imagine you were selling toasters, Mr. Smith, and you knew that toasters you were selling were going to explode 1 day. It was a matter of when, not if, but you sold those toasters anyway. What would happen to the company that you were running that sold those toasters?

Mr. SMITH. Well, look, we are not in the toaster business and we are not talking about toasters, but I would not want to work at a toaster company that had toasters that they knew were going to explode 1 day.

Ms. PORTER. Toaster companies are held—You are lawyers. You know the standard of strict liability. They are legally liable if they sell a product knowing that there is a likelihood that it will become defective or not work, if it doesn't have all the necessary safety features, for example. Why should Microsoft, or should Microsoft, let me ask you, be held to a similar liability standard, maybe not strict liability, but at least negligence, if you are selling server services and not selling sufficient logs as part of that in order to really do the work of stopping and identifying cyberbreaches?

Mr. SMITH. Well, let's separate two things. One, the specific, what logs are we providing, et cetera, that is a factual question that neither you nor I right now have the information about. I do

take your broader question, and I think it is basically this: should companies be held to a duty of care? Should they be obliged to follow reasonable cybersecurity practices? Yes, we do, and I think it is important to recognize that every one of these hacks didn't take place in the cloud. They took place on premise, on the networks, in the server rooms of these customers. They were the ones that had the logs, not us, for those intrusions.

Ms. PORTER. OK. So, you would agree that we need a national breach law, some kind of standard that sets out what the standard of care is, and that if you don't follow the standard of care, you could be held liable.

Mr. SMITH. Well, I would separate that from what I actually think is the most important issue in this hearing, which is, for certain companies, first responders, critical infrastructure providers, to let the government know whenever there is an attack. This is more like letting 9–1–1 know that someone has broken into a house. It doesn't matter whether a duty of care was followed or not. There is a burglar in the house. We need to go, you know, send the police to get them out.

Ms. PORTER. So, but, Mr. Smith, reclaiming my time. If we want people to do that notification, to make that 9–1–1 call, do you support whistleblower protection for employees who make those disclosures?

Mr. SMITH. Look, I haven't thought about that. I would be happy to think about it. I don't think you need whistleblower protection. We just need to create a system that puts the obligation on the companies themselves that have this information, and I think if that obligation is in place, other companies will follow. Look, we at Microsoft have been reporting this kind of information sharing. We have been publishing blogs without any legal duty to do so.

Ms. NORTON. The gentlelady's time has expired. I believe she was able to speak again because somebody yielded her time to speak again. I want people to understand that. I call on Mr. Garbarino of New York. You have five minutes, Mr. Garbarino.

Mr. GARBARINO. Thank you very much, Madam Chairwoman. To the two witnesses from SolarWinds, the committee is concerned that many of the current governmental procurement certification regimes are only check-the-box exercises and don't actually buy down risk. Can you discuss the various certification regimes that SolarWinds products were required to meet in order to be to be put on the GSA scale and made available to government agencies? Either Mr. Thompson or Mr. Ramakrishna.

Mr. RAMAKRISHNA. Sorry. Go ahead——

Mr. THOMPSON. No, go ahead, Sudhakar.

Mr. RAMAKRISHNA. Congressman, we comply to the standards that we have to comply to to ensure that the Federal Government can deploy our products. For instance, the FIPS certifications are required by the government and we comply to those. So, as it relates to Federal agencies, their compliance requirements, we have conformance working with our partners and directly with our customers themselves across the board. If you would like a full list of our compliance certificates, I am happy to furnish them to you as well.

Mr. GARBARINO. Well, what were you required to do? What was SolarWinds required to go through in order to be put on the list? What is GSA requiring? You know, is it enough? Should they require more before something can be made available to government agencies?

Mr. RAMAKRISHNA. To the best of my understanding, it is not so much a set of requirements that need to be added. Coming back to the issue at hand, I would doubt if more specification may have helped this particular case as much as an understanding of how these supply chain attacks are evolving, and for us as the private sector to take corrective steps and learnings from this experience and implement them and obviously pass that on from a software development and a secure development standpoint as well. To me, it does not appear to be a requirements thing at this point.

Mr. GARBARINO. OK. Mr. Thompson, anything additional?

Mr. THOMPSON. The only thing I would add is that different areas of the Federal Government require different levels of certification, and in every area of the Federal Government where we were allowed to sell, we had the required certifications. Whether that was COE, whether that was APL, Common Criteria, we had the required certifications. But I would agree with Sudhakar. Some of those certifications, while they do have security testing requirements that our products went through, and I think that that helps to ensure the security of the products, I think as you think about this particular breach and what happened, I don't think those certification requirements are designed to capture something like this.

Mr. GARBARINO. OK. So, is it fair to say we should now update to try to address it so this doesn't again or so other things don't happen again?

Mr. THOMPSON. Yes, I think that is a good question for CISA to ask them in terms of what could be done because I don't really have all the answers there. But I do think we have to think about together, private and public sector, how we do we work together more closely to make sure products are secure. And a lot of the panelists have talked about how do we share information very, very quickly so we can address issues as they occur, because nation-states will come up with new vectors of attack. They will come up with a new one tomorrow, and they will come up with a new one the day after, and the only way to protect ourselves is to let everyone know what those vectors are so that we can respond to them.

Mr. GARBARINO. I appreciate that. Thank you. Mr. Smith, a question for you. Can you help the committee understand Microsoft's statement: "We found no evidence of access to production services or customer data. The investigation also found no indications that our systems at Microsoft were used to attack others." What exactly are you saying here? Can you help us understand what did and didn't happen in your view? In your testimony on Tuesday, you mentioned that some Office 365 accounts were compromised through simple password guesses and sprays. How were the other accounts compromised?

Mr. SMITH. Sure. Well, what that statement says is three things. It says that our build systems were secure and they were not penetrated in any way, that we had no customer data that was touched

in any way, and that we found no evidence that any of our services or products were used as a vector of attack to launch an attack against anyone else. What we did find in certain instances was once this intruder was inside a network of, say, a customer, you know, say a Federal agency, one of the things it was able to do was get access to an account that had what we call elevated privileges, like an IT administrator. It was able to find the password or get the key to get into that account. When it was in that account, they found that that individual had access, say, to the Office 365 email of a portion or all of several customers. And so once they were there, then they went into the Office 365 cloud service and that is when we identified their presence.

Ms. NORTON. The gentleman——

Mr. GARBARINO. Thank you very much. I yield back.

Ms. NORTON. The gentleman's time has expired. I thank him for his questions. I recognize Mr. Johnson of Georgia.

Mr. JOHNSON. Thank you. Can you hear me now, Madam Chair?

Ms. NORTON. I can, and you are recognized for five minutes.

Mr. JOHNSON. Thank you. Technology advancements have created a world that looks unrecognizable compared to our lives just 30 short years ago, but Americans have grown accustomed to these changes. They have adapted. The average person not only may not understand the nuts and bolts of technology, but they do understand the risk of not being careful with it. Many of us use two-point authentication for our email, a third of Americans change their passwords annually, and we all know better than to make our passwords "JohnSmith123." Companies that work with millions of individuals' personally identifiable information should be held to a high standard that at least reflects what ordinary people employ in their day-to-day affairs using technology.

The SolarWinds preparedness and response to this hack were, at best, incredibly negligent and, at worst, criminal. And unfortunately we have seen a lot of data breaches that have dealt with the lack of protection for sensitive data. Hospitals, governments, county and local governments have been held hostage, hospitals, even government agencies. I believe eight or nine government agencies using SolarWinds software were able to be hacked into. Mr. Mandia, why was the SolarWinds breach so dangerous to our national security?

Mr. MANDIA. Well, that is a great question. First, I would like to comment that even if you are compliant, and almost every one of the 1,000 victims we respond to every year are, I am not convinced compliance in any standard regulation or legislation is going to stop a Russian foreign intelligence service from successfully breaching an organization, which is what happened here. The reason that the breach that we are describing was so entrenched is the fact that it was surreptitious and clandestine for nine months, and the threat actor behind it looks to be a foreign intelligence service. That is why. I don't think it impacts the general consumer that goes home every day. They are not thinking about this, but the government agencies that were impacted and the companies impacted are thinking about it. So, I think——

Mr. JOHNSON. Well, what can our enemies who hacked into our national data base, what can they do with the information that

they obtained, or what is possible that they could do with that information?

Mr. MANDIA. That is going to be one of the most complex questions to answer in this, sir, is that emails and documents were taken, and, quite frankly, the people targeted, all that information that was taken, I believe the threat actor is still learning how they can use that information. It is going to emerge over years, and it is going to take months and months for organizations to get their arms around all the possible uses of the stolen documents. You know, this breach, to me, from what I can observe, and I was a first-hand victim of it, wasn't about stealing the information of consumers' PII. This is about stealing documents that were relevant to the collection requirements of another nation.

Mr. JOHNSON. Well, it is national security secrets that can affect the lives and indeed the freedom of Americans and the safety of Americans, the physical well-being of Americans. Isn't that correct?

Mr. MANDIA. What can happen from this breach is yet to be told. Each victim had a different——

Mr. JOHNSON. A lot of damage to our national security could have been done and probably was done as a result of this breach. What standard should we build for our most precious infrastructure, like our voting systems, our hospitals, our electricity grids, our government secrets? What kind of national standards should there be in place to protect those secrets and guard against successful attacks like this one that are bound to occur in the future?

Mr. MANDIA. That is the question for me. You know, when you think about modern cyberdefense, first and foremost, every airplane has a data flight recorder. Overall, if you capture everything all the time, which is very hard to do, mind you, with encryption and other things, but it is always good to have something there that recorded everything in case something gets missed. Modern cyberdefense is going to take learning systems—AI—and it is going to take machine learning, and it is going to take expertise on the frontlines constantly being automated by systems. We are going through that transformation, sir, now in the industry. The bottom line is we can't have stagnant defense. We have to have defense that evolves at computer speed, not the signatures of yesterday, but the AI of tomorrow.

Mr. JOHNSON. Thank you. I yield back.

Ms. NORTON. The gentleman's time has expired. I thank him for his questions. Mrs. Cammack of Florida.

Mrs. CAMMACK. Thank you so much, Madam Chair. Good afternoon. Thank you to our witnesses for hanging in there. I know it has been a lengthy day, but I do appreciate your candid comments and your patience as we work through this. Just a few weeks ago, the Homeland Security hearing that we had, we looked at cybersecurity threats facing our Nation today and how we must improve our resilience in this area. The SolarWinds attack was one of the issues discussed in that hearing, so I am very glad that you are all with us here today to discuss this again.

As you all know, cybersecurity is only growing in importance for our national security as more of our everyday lives move into a cyber world, such as committee hearings. Normal operations for areas ranging from critical infrastructure to consumer products are

all moving to cyberspace, especially in the wake of the COVID–19 pandemic. This shift simultaneously exposes all of these operations to greater cybersecurity threats. So, I want to focus now on the relationship between the Federal Government and the private sector with regards to cybersecurity. In this area, cybersecurity is a unique landscape for private/public partnerships in information sharing and collaboration, which depends on mutual coordination. All levels of government and the private sector are targets now for our adversaries, non-state actors, and several of you have touched on the need for a national strategy to share intelligence between government and U.S. businesses.

So, I want to open this up to the panel. You all have touched on the importance of intelligence sharing between the public and private sector moving forward and the barriers in this area. So, in short, how can we make this information sharing easier for businesses, but also for government? What concrete steps can we take as legislators to facilitate this process? And I will start with Mr. Brad Smith with Microsoft.

Mr. SMITH. No, it is a really important question, and I think, to some degree, it starts with identifying who needs to report, what they need to report, to whom they need to report it, and how. I do think one thing that is worth touching upon that we really haven't perhaps talked about at this hearing is the critical need to enable people who have this information to report it easily and in a streamlined manner, because we are acting as the first responders. And, in a sense, when an incident is unfolding, you know, we are fighting a fire, and you don't want to take people away from the fire so they are filling out a lot of forms and doing things that are going to detract from their ability to respond. So, I would hope that one design principle that would be built into this would be the need to do it simply, efficiently, and in a manner that is sensitive to the work that is needed while an incident is unfolding.

Mrs. CAMMACK. Excellent. Thank you, Mr. Smith. And as you know, government is not known for their efficiency or their ability for data bases across agencies to talk to one another, so I appreciate your comments and actually would love to followup with you at a later time, but I am short on time. So, Kevin, can you elaborate on that a bit?

Mr. MANDIA. Yes, I think Mr. Smith got it right. I would add to it the confidentiality of it. If it is not confidential threat intelligence sharing, people are going to be worried about the liabilities to it, period. And, by the way, whether you did everything right on security or everything wrong, everybody's security program, to some extent, is a Maginot Line, period. And what we have learned with this one is hacking the supply chain was the blitzkrieg around the Maginot Line in the United States, so we will widen the line. We will broaden it. We will create our learning systems. Tech is getting better every single day. But whether somebody deserves to be compromised or not, however people interpret that, it takes time to figure out what you lost, so that confidentiality of the threat intelligence data sharing is critical.

Mrs. CAMMACK. Excellent. Thank you. I have got about a minute remaining, so really quickly, and again, I will open this up to the panel. What specific supply chain vulnerabilities should be ad-

dressed to limit exposure to these threats that we are seeing in cyberspace? Total free-for-all. Go for it.

Mr. RAMAKRISHNA. I would be happy to start on this one because we are in a unique position to apply our learnings to the broader industry here. And we have defined some very specific things that need to be done in the context of secure software development as it relates to the supply chain issues that we discussed in this hearing, and we plan to publish those as well. It is not one specific thing that may impact the supply chain, and we need to look at it holistically across the build environments, and also stress test our methodologies to date of delivering integrity in software and improve those. I am happy to share the details of those. We have published those, but we will share more details with you offline.

Mrs. CAMMACK. I appreciate that. Thank you so much. And I know I am out of time, so with that, I yield back. Thank you.

Ms. NORTON. I thank the gentlelady for her questions. Ms. Barragán of California.

Ms. BARRAGÁN. Thank you, Madam Chairwoman, for holding this very important hearing. Mr. Smith, Microsoft has stated that it has spent over $1 billion in security investments annually, but you recently also stated in an interview with the New York Times that you first learned of the attack when you were contacted by FireEye. How did Microsoft miss this attack, and how can customers like the U.S. Government trust Microsoft to uncover future vulnerabilities when Microsoft missed the worst intrusion of U.S. Government agencies, as quoted by Reuters?

Mr. SMITH. Well, I think to put it in its simplest terms, all 60 of the Microsoft customers who were attacked had their networks penetrated on premise, meaning in their server room in their building. It was not in our cloud services. It is like, you know, if someone broke into your house, but not my house, I would not know until you told me, or, in this case, what they did was they went into your house, they found the keys, the passwords, so that they could go into the service in the cloud. Once they got that, once they stole your keys, once they entered our cloud service, we saw them, and then we called you, and we said, "Did you know that they are in your house? Did you know that they have stolen your keys? Did you know that they have now entered the service that we can see, and did you know that, unlike AWS, unlike even, I think, Google, at Microsoft we let you know as soon as we find out that someone has penetrated your network?" And it doesn't matter whether it had anything to do with our service.

Ms. BARRAGÁN. Well then, Mr. Smith, if it had nothing to do with Microsoft, what did the billion dollars that you spent go to?

Mr. SMITH. Oh, it goes to better technology to protect the Microsoft products that you use. It goes to the Microsoft Threat Intelligence Center so that we can find these kinds of services. It goes to the Microsoft Detection and Response Team. It goes to the Microsoft Digital Crimes Unit. It goes to all the work that we do to protect the cybersecurity of our customers, of this country, and of the other countries that we support. And believe me, the billion dollars a year, that is just scratching the surface. We spend more than that every year.

Ms. BARRAGÁN. Thank you, Mr. Smith. You know, I represent the Port of Los Angeles, and cybersecurity is very important, and one disturbing fact from this breach is that Microsoft and FireEye products and services exist in most organizations. This breach and security could happen to the many thousands of other entities that utilize the software. Mr. Smith, you are now saying, "It wasn't us, it was somebody else," and so it kind of begs the question, you know, what have Microsoft and FireEye done to ensure that source codes are not compromised?

Mr. SMITH. Well, we do work every day to protect every aspect of cybersecurity. The first thing I would say is, fundamentally, cybersecurity today does not turn on the secrecy of source code. Most source code is published. It is in open-source form, and even when a company like ours uses source code that isn't published publicly, we make it widely available, so there are a wide variety of other practices that are critical for cybersecurity. And I think the message for the Port of Los Angeles——

Ms. BARRAGÁN. OK. Mr. Smith, I don't want to interrupt you. I do want to give a chance for Mr. Mandia to chime in here. Has FireEye done any anything to ensure that the source codes are not compromised? Given Mr. Smith's answer, I don't think I got one to the source code question. Do you have anything to add on this?

Mr. MANDIA. Yes, in our intrusion, the primary focus from this attacker was all about the documents and the communications of folks that did work for the U.S. Government, and our red team tools, which do proactive security assessments. We, like many companies, do everything we can to safeguard all our information, not just our source code, but our email and everything else.

And I would like to remind folks that this was a foreign intelligence service that hacked into 17,000 different organizations. I would ask the Members of Congress to think, is it reasonable for our companies to defend themselves from a foreign intelligence services, is that the bar that we want to set for this Nation's private sector?

Ms. BARRAGÁN. Well, thank you. It is important that we find out what happened, and where the issue is, and what we can do because, as Congress, we need to ensure that we are finding out that information to say, hey, something needs to be fixed, something needs to be done better. Sure, we are going to have those outside threats, but we also need to look to see where it went wrong. And I appreciate the discussion today and look forward to working with everybody to make sure we are able to secure, you know, the software and our agency data. With that, Madam Chairwoman, I yield back.

Ms. NORTON. The gentlelady's time has expired. Ms. Pfluger of Texas. I recognize Ms. Pfluger of Texas for five minutes.

Mr. PFLUGER. Thank you, Madam Chairwoman. Thanks for the——

Ms. NORTON. I am sorry. Mr. Pfluger.

Mr. PFLUGER. That is OK. I don't take offense to that right at this second. Thank you very much. You know, thank you all for a good discussion on this. As a military officer for two decades, you know, protecting every single piece of your architecture obviously is very, very difficult. I do want to talk a little bit, however, about

our national strategy, and specifically I want to take it back to my own home district where we have a Cyber Center of Excellence that is in development at one of the universities, Angelo State University, led by a former general officer in the Air Force, Ronnie Hawkins, who is doing amazing things in a Hispanic-serving institution, minority-serving institution in a very rural part of our country. So, I would like you from the corporate side to comment on what role education plays in our national strategy to make sure that we have the right people that are learning the skills that they need to learn to enter the work force and be a part of cybersecurity. So, we will just go down the line and start with Mr. Smith.

Mr. SMITH. Well, I would say two things. First, I think the kind of initiative that you have recently pursued at Angelo State points the way for the role that a number of colleges and universities and community colleges can play, you know. So, what you have been doing there around the cybersecurity intelligence program, I think it can be built and expanded and help us get the cybersecurity work force the Nation needs. The other thing I would point to is this extraordinary resource that we have as a Nation in terms of veterans coming out of the military every year. You know, every year there are about 200,000 people who leave the military. They enter the private work force.

One of the things that we have done at Microsoft is create, in partnership with the Department of Defense, what we call the Microsoft Software and Systems Academy. And so it has already worked with more than 2,000 individuals leaving the military. We have worked with partners across the industry. We provide education in the last couple of months, say, of somebody's tour of duty, and it guarantees an individual a job interview, a job interview with one of 600 partners that we have brought together. So, that is another way, I think, to add to the cybersecurity work force of the country.

Mr. PFLUGER. Thank you very much. Mr. Ramakrishna, do you have any thoughts on whether or not you believe that our college graduates, are we resource limited right now on the number of graduates who have the requisite skills?

Mr. RAMAKRISHNA. Congressman Pfluger, first of all, I hope everyone in your family and your community is safe given the events in Texas. Related to your question, I would say that looking at only college grads in this context is restrictive. I was mentioning earlier that the internet has to be made more available to every child, every person that is interested in learning and accessing, especially focused on inner-city kids and socioeconomically backward populations, because there is a lot of talent in those circles that need to be unleashed and exposed to these types of topics so that we can have a more aware and a more diverse work force and a set of people that can be brought into society at a higher level from a capability and contribution perspective. I think that is our contribution or our responsibility as private sectors as well.

One specific thing that I would like to offer up there is that as the government facilitates those, as part of the private sector, we could have a buddy system that we could provide to some of those young children to give them better exposure to these technologies and techniques, get them into internships and potentially into em-

ployment as well, and not hold the degree requirements on them because not everybody may be able to, or be able to afford afford, to go to colleges.

Mr. PFLUGER. Thank you very much. I appreciate that, and I also want to make sure that we acknowledge the fact that access to internet in the form of rural broadband is extremely important in communities like mine that may not have that ability. Very quickly, 30 seconds, Mr. Thompson, your thoughts on this issue?

Mr. THOMPSON. One of the challenges that we have had in the past, we have tried to work with colleges and universities on different programs to provide skill sets that we are in shortage of in the technology field in the United States. I think one of the challenges we had is just the speed at which colleges and universities can move. Getting them to add a new program because of the bureaucracy they have to go through is quite a lengthy process. So, I think if we can find a way to accelerate that and let them develop a cybersecurity training program or a data intelligence program, we need to do that quickly to be able to get more sophisticated workers in the work force to help solve these problems.

Mr. PFLUGER. Thank you very much, and with that, I yield back. Thank you.

Ms. NORTON. The gentleman's time has expired. I thank him for his questions. Next would be Ms. Bush of Missouri.

Ms. BUSH. Thank you, Chairs Maloney and Thompson, for convening this hearing, and I want to start off. So, the number of SolarWinds customers who were potentially affected in this attack, it is extremely concerning. At least 18,000 customers downloaded this malicious update to the SolarWinds product that infiltrated their devices. One concern coming out of the SolarWinds hack is that the attackers could use the foothold that they gained inside these companies and these agencies to then access other companies and, in turn, people. As we have been discussing, the risk is not theoretical. Mr. Mandia, as I understand it, FireEye first disclosed the breach. Chairman Thompson and others have mentioned that cyberbreach notification legislation is urgently needed, and we see that, but I want to be sure I understand. Were you required by law to do so, to disclose?

Mr. MANDIA. Right now, ma'am, most of the disclosure laws protect the personal identifiable information of American citizens, which is not something that we lost. So by law, we weren't, but I just want folks to know that literally within the first 36 to 48 hours, we were telling our government customers we have got a challenge here. We call it Ring Zero. Who do you go to first when you know there is something? As I was first briefed on the intrusion into FireEye, I recognized I doubt we were the first pick. And, in fact, the number in my head was we are probably the 40th organization compromised by this group, so who else is at risk. We did go to the intel communities. We did go to the DOD. We did go to CISA. Long before we went public with public disclosure, we were working with the U.S. Government.

Ms. BUSH. So, do you think that you should be required by law to do so?

Mr. MANDIA. I think if you are a first responder, like we are, to intrusions, because we recognized right away, you know, we are set

up for this sort of thing, and it happened to us. You know, I took the oath to defend the Constitution of United States, you know, I think 30 years ago. It just hits you. I didn't even want the government to communicate with me at that point. I didn't know the scope and scale of this. But I think for first responders, absolutely getting the threat intelligence, because at the time we were telling people about it, ma'am, we really didn't know what had happened other than something had happened. But that was enough that we had to tell the government entities that we work with.

Ms. BUSH. So, the answer is no basically. So, would you say——

Mr. MANDIA. Yes, we didn't have a legal disclosure to, but we felt an obligation to.

Ms. BUSH. OK. So now, would you say anything has changed since the hack that would make us trust private companies like SolarWinds more now?

Mr. MANDIA. Well, I think when you see a breach like this, you don't want the attacker to win twice once they broke in. Well, actually, it would be three times. They broke into SolarWinds. They had what looks to be a very successful deep blast zone type of cyberespionage campaign, and then they harmed American companies both in shareholder lawsuits, liabilities, and investigations. It is like a trifecta for the adversary against us.

Ms. BUSH. Yes.

Mr. MANDIA. So, we got to think of a way where we play team ball as a Nation where we all come together. And I do believe the fastest thing we can do, we have been talking about a lot today, ma'am, get the threat intelligence into an agency in the government, and then from there it gets pushed out to the security community so we can go shields-up a lot faster. Best we can do, ma'am, is maybe somebody is a victim, but we are all as secure as the very last victim in cybercrime.

Ms. BUSH. Thank you. Given that this hack has been traced back from many months, it may be possible that other companies knew about this and didn't tell anyone because they didn't have to. So, Mr. Smith, are you aware of any other companies that may have known about this breach and did not report it?

Mr. SMITH. We notified 60 Microsoft customers, and we have said that 50 percent of those, so call it 30, are communications and technology firms. And we provided that information first to them, so we told them, and we have shared that information to the government. But most of those companies have not disclosed publicly that they were attacked in this way. And, in fact, you have other companies, some of the largest companies in our industry, that are well known to have been involved in this that still have not spoken publicly about what they know. There is no indication that they even informed customers, and I am worried that, to some degree, some other customers or some other companies, some of our competitors even just didn't look very hard. If you don't look, you won't find, and you will go to bed every night being blissfully ignorant thinking you don't have a problem when, in fact, you do.

Ms. BUSH. Thank you, and I yield back.

Ms. NORTON. The gentlewoman's time has expired. I am passing it over now to Ms. Porter to continue to chair the committee.

Ms. PORTER. Thank you, Ms. Norton. I am going to hand it back to you. I believe we have no more members to recognize. Does anyone else wish to be recognized?

Ms. NORTON. Well, we have been here for a long time, and unless someone speaks up with this double hearing, of this hearing involving two committees, I am about to sign off and thank our witnesses for testifying. I find members who had to come back and forth, but it looks like we have reached the limit of members who wish to testify. I want to thank the witnesses again, and at this point——

Ms. PORTER. Ms. Norton?

Ms. NORTON. Yes? Yes, indeed, Ms. Porter.

Ms. PORTER. I see that my colleague, Mr. Torres, has joined.

Ms. NORTON. Ms. Porter, will you take over the hearing from here?

Ms. PORTER. Yes, ma'am.

Ms. NORTON. All right.

Ms. PORTER. [Presiding.] Mr. Torres, the gentleman from New York, is now recognized.

Mr. TORRES. Thank you, Madam Chair. I have a question for the new CEO of SolarWinds. Has your company conducted a post-mortem of what went wrong, the mistakes that your company might have made, and the lessons learned from those mistakes?

Mr. RAMAKRISHNA. Congressman, thank you for the questions. As I came into the company, given my cybersecurity experience from previous companies and having had to deal with cyber incidents in the past, I had to first look at our cyber hygiene and cybersecurity posture as well as our cybersecurity investments. As Mr. Thompson highlighted previously, this did not appear to be or does not appear to be an investment issue. We spent enough on cybersecurity, in fact, more than the average company——

Mr. TORRES. Just in the interest of time constraints, so you have done a post-mortem, but in your judgments, do you believe your company made mistakes? Yes or no.

Mr. RAMAKRISHNA. I think there are opportunities to improve, Congressman.

Mr. TORRES. It is a straightforward question. I am a straightforward person. It is a straightforward question. Did you make mistakes? Yes or no. You can say no, but——

Mr. RAMAKRISHNA. We all make mistakes and——

Mr. TORRES. OK. You made mistakes. Tell me, what mistakes did you make?

Mr. RAMAKRISHNA. As I look at what we have done in the past, and I am looking at it from the standpoint of where we go from here. I haven't looked at specifically——

Mr. TORRES. We have to learn from past mistakes in order to know how to move forward so——

Mr. RAMAKRISHNA. Yes.

Mr. TORRES. We want to concrete examples. Is it true that SolarWinds had no chief information security officer in the lead-up to the SolarWinds breach?

Mr. RAMAKRISHNA. So, the way we have organized ourselves is that instead of calling the person a chief information security officer, we call him a VP of security for a very specific reason. Instead of looking at only infrastructure security, that person is also re-

sponsible for looking at product security. That way we are able to get the best of both worlds and help us all build products as well as take care of our infrastructure. So, it is a——

Mr. TORRES. So, I just want to be clear, you had a VP for security in the lead-up to the SolarWinds breach?

Mr. RAMAKRISHNA. Absolutely, and we have had it since 2017.

Mr. TORRES. You know, so here is the concern I have. The cybersecurity failure of SolarWinds led to a supply chain breach that compromised nine Federal agencies. It is arguably the greatest cybersecurity failure in the history of the United States, and your company is at the heart of it. Given the seismic nature of that cybersecurity failure, can your company be trusted to ever do business with the Federal Government?

Mr. RAMAKRISHNA. Congressman, we take the security and protection of our customers very, very seriously. This particular issue was much more than just SolarWinds. It was a very sophisticated nation-state attack, as we have been discussing here. It has got very little relevance to a security hygiene of a particular company or the security investments of a particular company. It was a coordinated, patient, persistent attack that neither one company, no matter large it is or how many resources it is deploying, or one Federal Government agency is able to coordinate it, which is the subject of today's hearing that we came here to apply our learnings and contribute our learning.

Mr. TORRES. I am going to move on. So, I have a question for FireEye. FireEye managed to do something that the entire cybersecurity apparatus of the Federal Government failed to do. You detected SolarWinds. So, my question for the CEO of FireEye, what does the Federal Government need to do to be more effective at detecting breaches like SolarWinds?

Mr. MANDIA. Well, I think, first, it is team ball. You know, we had talked about the area of responsibility for some of the best capabilities we have, like the NSA's, outside of the Nation. All the fingerprints of this attack actually were inside the Nation. So, you have to expect that the government is going to detect some things, the private sector is going to detect some things, hence, all the dialog, sir, to bring it to one entity that has got purview into both sides of the fence.

I think the government was catching a whiff of it. They were seeing streams of smoke because when I started talking to government agencies, no one was surprised. They were starting to go, oh, I get it. We were all piecing together the same crime scene, but we all had different pieces of evidence. It took us finding the SolarWinds implant and Microsoft's help from the top down, cloud down, looking to start scoping this thing.

Mr. TORRES. I just want to squeeze this in because we have the EINSTEIN system, which operates on a data base of known cyber threats, right?

Mr. MANDIA. Yes, right.

Mr. TORRES. Do you have technology that is effective at detecting anomalous threats that could benefit the Federal Government——

Mr. MANDIA. We do, and there is a lot of other technologies that do as well, but the problem was, you have to have a little bit more visibility than that. So, there were blips on the radar sir, but no-

body could tell what they meant without more context. The implant, when we found that, that was kind of the homerun for context and everybody went "aha." That was the eureka moment.

Mr. TORRES. Thank you. Thank you, Madam Chair.

Ms. PORTER. Thank you, sir. With that, I want to thank our panelists for their remarks, and I want to commend my colleagues for participating in this important hearing.

With that, without objection, all members will have five legislative days within which to submit additional written questions for the witnesses to the chair, which will be forwarded to the witnesses for their response. I ask our witnesses to please respond as promptly as you are able.

Ms. PORTER. This hearing is adjourned.

[Whereupon, at 2:01 p.m., the committee was adjourned.]