SAFEGUARDING THE FEDERAL SOFTWARE SUPPLY CHAIN

HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY, INFORMATION TECHNOLOGY, AND GOVERNMENT INNOVATION

OF THE

COMMITTEE ON OVERSIGHT AND ACCOUNTABILITY

HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTEENTH CONGRESS

FIRST SESSION

NOVEMBER 29, 2023

Serial No. 118–77

Printed for the use of the Committee on Oversight and Accountability

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

U.S. GOVERNMENT PUBLISHING OFFICE
54–310 PDF WASHINGTON : 2024

COMMITTEE ON OVERSIGHT AND ACCOUNTABILITY

JAMES COMER, Kentucky, Chairman

JIM JORDAN, Ohio
MIKE TURNER, Ohio
PAUL GOSAR, Arizona
VIRGINIA FOXX, North Carolina
GLENN GROTHMAN, Wisconsin
GARY PALMER, Alabama
CLAY HIGGINS, Louisiana
PETE SESSIONS, Texas
ANDY BIGGS, Arizona
NANCY MACE, South Carolina
JAKE LATURNER, Kansas
PAT FALLON, Texas
BYRON DONALDS, Florida
KELLY ARMSTRONG, North Dakota
SCOTT PERRY, Pennsylvania
WILLIAM TIMMONS, South Carolina
TIM BURCHETT, Tennessee
MARJORIE TAYLOR GREENE, Georgia
LISA MCCLAIN, Michigan
LAUREN BOEBERT, Colorado
RUSSELL FRY, South Carolina
ANNA PAULINA LUNA, Florida
CHUCK EDWARDS, North Carolina
NICK LANGWORTHY, New York
ERIC BURLISON, Missouri

JAMIE RASKIN, Maryland, *Ranking Minority Member*
ELEANOR HOLMES NORTON, District of Columbia
STEPHEN F. LYNCH, Massachusetts
GERALD E. CONNOLLY, Virginia
RAJA KRISHNAMOORTHI, Illinois
RO KHANNA, California
KWEISI MFUME, Maryland
ALEXANDRIA OCASIO-CORTEZ, New York
KATIE PORTER, California
CORI BUSH, Missouri
JIMMY GOMEZ, California
SHONTEL BROWN, Ohio
MELANIE STANSBURY, New Mexico
ROBERT GARCIA, California
MAXWELL FROST, Florida
SUMMER LEE, Pennsylvania
GREG CASAR, Texas
JASMINE CROCKETT, Texas
DAN GOLDMAN, New York
JARED MOSKOWITZ, Florida
RASHIDA TLAIB, Michigand

MARK MARIN, Staff Director
JESSICA DONLON, Deputy Staff Director and General Counsel
RAJ BHARWANI, Senior Professional Staff Member
LAUREN LOMBARDO, Deputy Policy Director
PETER WARREN, Senior Advisor
MALLORY COGAR, Deputy Director of Operations and Chief Clerk

CONTACT NUMBER: 202-225-5074

JULIE TAGEN, Minority Staff Director

CONTACT NUMBER: 202-225-5051

SUBCOMMITTEE ON CYBERSECURITY, INFORMATION TECHNOLOGY, AND GOVERNMENT INNOVATION

NANCY MACE, South Carolina, Chairwoman

WILLIAM TIMMONS, South Carolina
TIM BURCHETT, Tennessee
MARJORIE TAYLOR GREENE, Georgia
ANNA PAULINA LUNA, Florida
CHUCK EDWARDS, North Carolina
NICK LANGWORTHY, New York
ERIC BURLISON, Missouri
Vacancy

GERALD E. CONNOLLY, Virginia *Ranking Minority Member*
RO KHANNA, California
STEPHEN F. LYNCH, Massachusetts
KWEISI MFUME, Maryland
JIMMY GOMEZ, California
JARED MOSKOWITZ, Florida
Vacancy

C O N T E N T S

WITNESSES

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

INDEX OF DOCUMENTS

Documents are available at: docs.house.gov.

SAFEGUARDING THE FEDERAL SOFTWARE SUPPLY CHAIN

Wednesday, November 29, 2023

HOUSE OF REPRESENTATIVES
COMMITTEE ON OVERSIGHT AND ACCOUNTABILITY
SUBCOMMITTEE ON CYBERSECURITY, INFORMATION TECHNOLOGY, AND GOVERNMENT INNOVATION
Washington, D.C.

The Subcommittee met, pursuant to notice, at 2:21 p.m., in room 2247, Rayburn House Office Building, Hon. Nancy Mace [Chairwoman of the Subcommittee] presiding.

Present: Representatives Mace, Timmons, Langworthy, Connolly, and Lynch.

Ms. MACE. Good afternoon, everyone. The Subcommittee on Cybersecurity, Information Technology, and Government Innovation will now come to order.

And good afternoon. We welcome everyone who is here this afternoon.

Without objection, the Chair may declare a recess at any time. And I will recognize myself for the purpose of making an opening statement.

Good afternoon, and welcome to this hearing of the Subcommittee of Cybersecurity, Information Technology, and Government Innovation.

Today more than ever, Federal agencies rely on information technology to carry out core functions of government. Digital information systems are used to help provide healthcare to veterans, pay Social Security beneficiaries, protect the homeland, administer our system of justice, and much more. The broad deployment of IT systems creates efficiencies and streamlines the government service delivery process. So, there is no disputing the gains from digital government are real, but so, too, as you all know and why you are here this afternoon, are the risks.

Our increase in dependence on computer hardware and software has created an irresistible target for malicious cyber actors. These include foreign enemies who seek to do us harm and domestic activists bent on disruption, along with criminals chiefly seeking to line their own pockets. We know these risks from hard experience. A series of hacks have exploited vulnerabilities in software used to operate major Federal and non-Federal computer systems.

For example, the 2020 SolarWinds breach, many of you are aware of, amongst the largest ever, was perpetrated by Russia-

based cyber criminals who gained access to systems and data by injecting malware into a widely used software update.

More major software hacks have followed since then. That includes one involving Log4j, a common software component. And this past May, the popular file transfer software, Moveit, was compromised.

These intrusions disrupt operations, they are costly and time-consuming to address for companies of all sizes. And they risk the exfiltration of sensitive data, including the personal identifiable information of millions of Americans. Ultimately, they erode trust and the ability of our government to execute its core functions reliably and securely.

So, we need to ensure the software we use is safe. It is a challenging risk; the Federal Government spends about a hundred billion annually in IT goods and services, including software. When you acquire a product, you inherit any risks associated with its supply chain. And the software supply chain is often opaque, its providence is often unclear, including that of the underlying source code. And even if the origins are known, it could also have been later altered or tampered with.

Congress has taken some steps to shore up the software supply chain. Section 889 of the 2019 NDAA prohibited Federal agencies from buying certain telecom and video surveillance equipment, including that made by specific companies tied to China. Congress also authorized the creation of Federal Acquisition Supply Council or FASC as a centralized interagency hub to identify and mitigate government IT procurement risks.

One way to make the software supply chain more transparent is through SBOMs. An SBOM, or Software Bill of Materials is analogous to a food nutrition label. It reveals the origin and component elements of software, as well as modifications later made. An SBOM can help government purchasers identify software vulnerabilities, like source code originating from China or Russia. The goal is to secure the software supply chain without unduly shrinking the pool of software providers and products available to the government. We do not want to give up the benefits we all gain from software-driven efficiencies, including the savings they yield to taxpayers. That is why we have a representative of the Federal contractor community testifying here today, along with experts on the methods and intentions of cyber threat actors.

But before we hear from them, do you want to make an opening statement.

Mr. LYNCH. I think the Ranking Member will be along. So, if we could go to introduction of the witnesses.

Ms. MACE. We will pause. When Mr. Connolly gets here, he will do his opening statement.

Mr. LYNCH. Thank you.

Ms. MACE. All right. So next, I am pleased to introduce our witnesses for today's hearing. Thank you for being jammed up there today. You guys look super cozy. Small desk, four people.

Our first witness is Dr. James Lewis, Senior Vice President, Director of Strategic Technologies Program at the Center for Strategic and International Studies.

Our second witness is Mr. Jamil Jaffer, founder and Executive Director of the National Security Institute at George Mason University's Antonin Scalia Law School.

Our third witness is Mr. Roger Waldron, President of The Coalition of Government Procurement.

And our fourth and final witness today is Ms. Jennifer Bisceglie, founder and CEO of Interos, Inc.

Welcome, everyone, and we are pleased to have you this afternoon.

So, pursuant to Committee Rule 9(g), the witnesses will please stand and raise your right hands.

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

Let the record show the witnesses all answered in the affirmative. We appreciate all of you being here today and look forward to your testimony. I will remind our witnesses—I do not know what that was—we appreciate everybody being here today. I will remind the witnesses that we have read your written statements, and they will appear in full in the hearing record. Please limit your oral statements to 5 minutes. And as a reminder, please press the button on the microphone in front of you so that it is on, and everyone can hear you. When you begin to speak, the light in front of you will turn green. And after 4 minutes, the light will turn yellow. When the red light comes on, your 5 minutes has expired, and I will politely ask you to stop, to please wrap up.

So, our first witness, Dr. Lewis, I invite you to please begin your opening statement.

STATEMENT OF JAMES LEWIS
SENIOR VICE PRESIDENT
AND DIRECTOR
STRATEGIC TECHNOLOGIES PROGRAM
CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

Dr. LEWIS. Thank you, and I thank the Committee for the opportunity to testify. Forty-five years ago, China's leaders realized that the economy was in shambles, and they decided to open China to the West. This economic opening created immense business opportunities for the world, and the U.S. expected that the relationship with China would steadily improve. It was profitable for both sides, but there were always problems, and chief among those problems was that China decided that to modernize and grow, it needed to acquire technology. China did this in many ways, but chief among them is cyber espionage.

China leads in intellectual property theft and now collects the personal information of American citizens. Chinese intelligence services exploit information technology, including devices, software, internet apps, and the cloud. Anything that connects to the internet creates an opportunity for spying. And when China provides the software, it makes this task easier.

The way that software is built creates opportunities. Software products blend code from a variety of sources. This could include software from China or other hostile nations. One concern is the use of Chinese software development kits, basically chunks of code

that can be inserted into bigger programs. This has been done in many U.S. commercial products. The use of Chinese software creates opportunities for espionage and the disruption of services. A Federal user may download a shopping or travel app for personal use and not know that it includes Chinese software.

The problem is that the U.S. and China have deeply interconnected supply chains. This interconnection creates vulnerability and risks, but they cannot be undone overnight. We can, however, manage this risk.

Since the 2021 SolarWinds incident, the U.S. has taken a number of steps to improve software supply chain security—changes to the Federal acquisition regulations, and to FedRAMP, will lead to acquisition of more secure software and services.

Other important measures include the Software Bill of Materials process that you mentioned, SBOM, managed now by the Department of Homeland Security, and the new Department of Commerce Office of Information and Communications Technology. SBOMs provide insight into the source of the software products. We often do not know where the code came from. And since there can be multiple participants—a prime, a sub, tertiary suppliers—SBOMs are crucial. It lets the U.S. identify software that comes from risky sources in a way we cannot now do. Commerce's ICTS office will review information technology subject to its jurisdiction and can prohibit or impose measures on transactions that create risk.

The office was really created to deal with TikTok, to make an approach to TikTok that would withstand judicial scrutiny. So, they are beginning their work. I think everyone is optimistic about them. The office also builds on the work of several executive orders in this Administration, and its predecessor, issued in the last few years.

Safeguarding the Federal software supply chain points to the need for a thorough review of software applications and internet-connected devices acquired by the Federal Government. SBOM, the new office, the executive orders, and changes in the acquisition regulations will let the United States better manage a complex national security problem. But we are only at the start. I thank the Committee for the opportunity to testify and look forward to your questions.

Ms. MACE. Thank you. I will now recognize Mr. Jaffer for your opening statement.

STATEMENT OF JAMIL JAFFER
FOUNDER AND EXECUTIVE DIRECTOR
NATIONAL SECURITY INSTITUTE
ANTONIN SCALIA LAW SCHOOL
GEORGE MASON UNIVERSITY

Mr. JAFFER. Chairwoman Mace, Ranking Member Connolly, and Members of the Subcommittee, thank you for the opportunity to testify today about the threat facing our Nation from potential vulnerabilities in the Federal software supply chain.

Let me start out by saying we are in a constant, if low level, state of conflict with adversaries in a cyber domain today. Russia has come after our government, our think tanks, our universities, our critical infrastructure. They are deep inside our systems. They

have long-term sustained access to almost every aspect of the U.S. Government and the private sector, including our water supply, our electric supply, our banking system.

The same is true of China. China is deep inside our networks and has been for years. They look to exploit that—both Russia and China today look to exploit that capability primarily for intelligence collection and to establish a capability to remain on our infrastructure to use in the case of conflict. They do not attempt today to use it for that purpose.

Other nation state actors, unfortunately, likewise have significant capability. The Iranians and North Koreans, while being somewhat further behind than the Russians and Chinese, have today a significant capability to access and influence our critical infrastructure and our government.

This is a challenge because today the world is on fire. We have a war going on in the heart of Europe between Russia and Ukraine. We have a war going on between Israel and Hamas, a nation state Iranian-backed threat actor. We also see constant, consistent threats to our allies and partners in the Indo-Pacific, including Taiwan, Japan, South Korea, and Australia by China, and a consistent set of launches of ballistic missiles, nuclear capable ballistic missiles by North Korea. Each of these nation states has cyber capabilities. Many of which they deploy today across the globe and here in the United States by exploiting software vulnerabilities in the supply chain.

So, the challenge we face is one that is not insignificant, to the contrary it is one that is massive, serious, and present today, and we must address. Now, there are a number of things that we as the Federal Government can do to address these problems and a number of important steps that the Chairwoman herself mentioned—section 889 is a step in the right direction. We have also banned certain types of capabilities.

The U.S. Government once bought Russian antivirus software in the form of Kaspersky. We have now barred that from U.S. Government systems, and that is a good thing. As are the bars on Huawei, ZTE, and other Chinese capabilities.

But the problem goes deeper, as Jim has correctly laid out, a number of nation state actors play in the open-source software space, and they engage in efforts to exploit providers in the U.S. Government. We saw that perhaps famously in the case of the SolarWinds hack that the Chairwoman referred to earlier. But we also saw it long before that in the case of the NotPetya attack conducted by Russia against Ukraine, but that spilled worldwide and caused over $10 billion of damages.

So, the government can take action to strengthen its own systems. We can talk about buying software that is secure by design and resilient by design. These are things that the government and today the Administration has talked about extensively. CISA has put out guidance on secure by design. The National Cybersecurity Strategy refers to resilience by design concepts as well.

But it goes beyond simply buying better and more capable software. It requires our government actors and our government procurers to be able to procure the leading edge of software technology to buy from U.S. startups. We have talked for decades about the

need for the U.S. Government to be more forward leaning and more capable and more flexible when it comes to buying capabilities.

The challenge, of course, is one of priorities and one of risk-taking. Our Federal Government officers should not be risk-taking when it comes to buying foreign software. They should, however, take risks and lean forward when it comes to buying American startup software and capabilities as we think about how to better defend the Nation and cyber domain. That requires culture change within the executive branch and culture change within the executive branch's overseers here in Congress.

Finally, the U.S. Government cannot simply remain on the defensive. If we are going to really effectively address threats to our government and industry in the cyber domain, we have got to go on the offensive. That requires taking the fight to the enemy. We have done quite a bit of that by leaning forward on active defense and persistent engagement. We need to do more. It does not work when our government is unwilling to lean forward, take the fight to the enemy in any domain, much as in cyberspace. Deterrence can and does work in the cyber domain. We just do not practice it.

Thank you for the opportunity to address the Committee, and I look forward to your questions.

Ms. MACE. Thank you. I will now recognize Mr. Waldron for your opening statement.

STATEMENT OF ROGER WALDRON
PRESIDENT
THE COALITION FOR GOVERNMENT PROCUREMENT

Mr. WALDRON. Good afternoon, Chairwoman Mace, Ranking Member Connolly, and Members of the Subcommittee. Thank you for the opportunity to appear before you to address the Federal software supply chain. The Coalition for Government Procurement is a nonprofit, nonpartisan association of firms selling commercial services and products to Federal Government. Our members collectively account for more than $145 billion in mission support for the Federal customer. Our members include small, medium, and large business concerns from across the commercial market. They include software, commercial software firms, cloud providers, system integrators, and IT suppliers. As such, they are well aware of the challenges involved in addressing vulnerabilities in the Federal software supply chain.

The threat for near-peer adversaries and other bad actors has made cybersecurity and supply chain risk management fundamental to Federal procurement in the commercial sector. Recognizing the importance of this matter, there are three points I would like to make.

First, the government should continue prioritizing buying commercial solutions where appropriate. The Federal Acquisition Streamlining Act of 1994 established a preference for the acquisition of commercial items. This preference reduces risk, increases competition, improves pricing, provides greater access to innovation, and it improves security. Commercial software firms recognize that security failure risks reputational harm which would translate into loss of business. For this reason, drawing on their experience across industry sectors, like healthcare, banking, finance, and en-

ergy, they understand that they must invest in security, and they do so. Government should capitalize on this expertise.

Second, cybersecurity requirements reporting and other administrative compliance regimes should not burden commercial firms unnecessarily. Some requirements are necessary, but unnecessarily burdensome requirements drive companies out of the government marketplace, reducing government access to the innovation and capabilities of the commercial market.

As the Administration's recent draft memo on the Federal Risk and Authorization Management Program, FedRAMPs stated: "Unthinking adherence to standard agency practices in a commercial environment could lead to unexpected or undesirable security outcomes."

Some government mandates for certifying commercial products could create compliance risks when the mandates are not required outside of the government or are ambiguous. The government should accept commercial standards whenever possible, and required certification should focus on what is being provided actually meets those standards.

Third, and finally, the Federal cybersecurity and software supply chain framework is in a state of flux and coordination is needed. There are various pending rules and regulations, like FedRAMP; first cloud cybersecurity; CMMC, the Cybersecurity Maturity Model Certification that DOD contractors are going to have to sign up to; NIST 800–171 is in the process of being rewritten; software bill of materials. There are several proposed FAR cybersecurity clauses and more to come. Section 889, any activities of the Federal Acquisition Security Council, all of which are in various stages of government review and/or public comment.

The government has the opportunity here to provide needed harmonization of these rules and regulations to assure an efficient and consistently implemented cyber regime. Coordination could be achieved by further establishing roles and responsibilities for CISA and for the activities of the Federal Acquisition Security Council to manage cybersecurity and supply chain obligations and reporting for Federal contractors. This will reduce duplication and overlap in the cybersecurity and software supply chain framework. Such consistency will assure that all stakeholders understand the rules of engagement in the government space and will be more able to easily adjust as those rules evolve to meet the challenges of a dynamic cyber and supply chain environment.

In closing, Chairwoman Mace, Ranking Member Connolly, and Members of the Subcommittee, thank you for the opportunity to appear before you today. I look forward to addressing any questions you might have.

Ms. MACE. Thank you. I will now recognize Ms. Bisceglie for your introductory statement.

STATEMENT OF JENNIFER BISCEGLIE
FOUNDER & CEO
INTEROS, INC.

Ms. BISCEGLIE. Thank you. And good afternoon, Chairman Mace and Members of the Subcommittee. Thank you for inviting me to

testify as a subject matter expert on supply chain risk management with today's focus on securing the Federal software supply chain.

My company, Interos, is built on almost 30 years of personal experience in global supply chain risk management. Over the past 19 years since I started Interos, I have seen the discussions turn from a lack of understanding of this issue to simple compliance and resiliency, and now the product integrity or software pedigree or SBOM to preempt and protect from intentional, malicious attack.

To support our customers, Interos began to build out of what is now the world's largest business relationship graph. Using artificial intelligence, we are responsible for mapping and continuously monitoring the business relationships, business dealings, and supply chains of more than 300 million businesses around the world and the billions of relationships between them.

I will first share two of our observations, and then follow those with four recommendations. First, we believe we are still struggling with finding a common definition for the supply chain risk management as well as a standard way to measure the challenge. And I think you heard that from my peers on the panel today.

As we tend to separate hardware from software from service supply chains, we will continue to create artificial silos and increase the available attack vector for both the intended and unintended enemy. When in actuality, all we are talking about is simply who is doing business with each other and what risks those relationships might entail.

Our second observation is that supply chain risk management must be viewed as an investment versus an expense. Interos is the technology of choice for the only true supply chain mismanagement shared service in the world currently hosted by the U.S. Navy to help them provide the transparency and pedigree of what is coming into various offices in the Navy, as well as the ongoing monitoring of said national security systems in a proactive and information sharing way. However, none of this is happening through a federally funded program of record. We are still handling supply chain security across the Federal Government as a rob Peter to pay Paul fashion.

We have four recommendations for the Committee to consider to better protect our Nation's critical infrastructure. First, awareness in education are critical to communicate that supply chain risk impacts everyone within the Federal infrastructure which actually instructs the private sector.

Second, actually fund the programs. Assign someone within the agency to only issue and measure the success. Even with reports from GAO, updates to FITARA and FISMA, the various executive orders, we can point to the prioritization without alignment or uniform rollouts, which drives up the costs and makes management as well as effectiveness very difficult.

Third, make automated supply chain security for hardware, software, and services be the cost of doing business, not only with the Federal Government, but also between private sector organizations. How many more examples of the ripple effect of our business connections and how easily disturbances can be shared. Everything from NotPetya, to the Target Breach, to Log4j, Moveit, SolarWinds, not to mention as already been mentioned today, we are also tar-

gets for countries such as China, Russia, and Iran. Why do we let public and private sector organizations continue to fund service-based supply or risk assessments and not leverage technology for continuously monitoring the problem?

Finally, and simply, implement contractual language that is effective and will actually be used. In addition, there are multiple industry associations working on standards for supply chain mismanagement, such as those in the room today. Doing as much as possible via internal policy changes and contractual language as a way to inform suppliers of how to do business with you and to mitigate risks coming into your organization is a much less expensive way to approach the problem than regulation and legislation.

In conclusion, the solution needs to be viewed as an investment in national security, not just an expense, which moves us into the offense position, as was just mentioned, and needs to include upscaling the people responsible for buying and using software supply chain security requirements, not just putting the requirement in a contract as wording. It is the use of the SBOM—to KNOW/PREVENT/FIX, as Google likes to say—will make the difference for the Federal software supply chain, this country's security posture, and our global competitiveness. Thank you for the opportunity to present our views, and I look forward to answering any questions.

Ms. MACE. Thank you. I would now like to recognize myself for 5 minutes of questioning. I will start with you, Mr. Jaffer, and good afternoon.

Your written testimony states that for far too long the U.S. has been taking cyber attacks and hacks on the chin with limited response. In the cyber domain, we have largely been unwilling to establish, much less enforce effective red lines.

My first question to you, Mr. Jaffer, this afternoon. Should this Administration draw a line in the sand to deter cyber warfare launched from China, Russia, and other enemy nation states?

Mr. JAFFER. Thanks, Chairwoman. Yes, I absolutely think we need to make very clear our red lines in the cyber domain. Part of the challenge that I think that we face in this domain is that we talk about our concerns, but we do not actually effective them. We do not talk about what our capabilities are on the cyber domain. We do not talk about what our red lines are. We do not talk about what we would do if those red lines are crossed. And then worst, the world is seeing on the rare occasion the U.S. established red lines, we do not enforce them. And that is the real fundamental failure. The reason why deterrence is not working in the cyber domain, and we keep getting hit over and over, and our adversaries come at us even more in a more challenging way is because they are testing our boundaries. Until we set clear boundaries and enforce them, this will continue and get worse. That actually makes it more dangerous——

Ms. MACE. How do we change the behavior?

Mr. JAFFER. Look, I think we have to extract consequences and costs, and we have to do it in a way that is seen not just by that threat actor, but by other threat actors as well. That is the only way we are going to see real deterrence in this domain. Frankly, it applies across the board, not just in cyber, but it is more present in cyber than others.

Ms. MACE. Yes. Government purchasers need to take more risks and being willing to buy from small American startup companies. As you mentioned before in your testimony, how would taking those risks help safeguard the software supply chain, for example?

Mr. JAFFER. Well, you just heard about what Interos does and the capabilities it brings to bear. This is the kind of company and other companies like it that have leading-edge capabilities. Whether it is software supply chain management or in actual defensive capabilities or, you know, lean forward offensive capabilities. Until we can really buy the best and brightest in technology across the board, which is built here in the United States, it is going to be impossible for the government to be at the cutting edge. We do not buy it because we have got these huge programs of record that make it easy for people to buy from existing contractors and not lean forward.

Ms. MACE. Yes, I agree. Ms. Bisceglie, I have a couple of questions for you. In your written testimony it states that the use of the SBOM that will make the difference for the Federal software supply chain, this country's security posture, and our global competitiveness. Do you think SBOMs can make software purchasing safe, the way that nutrition labels let us know if the food we buy is healthy, for example?

Ms. BISCEGLIE. Yes, I think it is a great question. I think it goes back to the implementation. And I think that you just mentioned the same thing. It is not a compliance activity. And I think we are so focused in this government, and even in the private sector often about reputation and brand, and say, hey, I think I did enough because FITARA, FISMA, FedRAMP, what have you, they all said I did it, and I checked the box. That is the problem. When you think about SBOM or a food in an ingredient list, that is a compliance activity. It is really what is the red line? What is——

Ms. MACE. Is FITARA outdated?

Ms. BISCEGLIE. Yes.

Ms. MACE. Yes, very much so. And should we update it and maybe make it better current with the times and the technology?

Ms. BISCEGLIE. I think the move to look at something much more operationally focused and dynamic versus standard based——

Ms. MACE. Yes, Congress just wants to do what we always have done and that is outdated, and that hurts us, correct?

Ms. BISCEGLIE. I do not think it keeps up with the time with the best and the brightest.

Ms. MACE. Yes. Thank you. Then your written testimony also states that Interos has built the world's largest business relationship graph. We have talked about AI before, and I am very impressed with what your company is doing with AI and the supply chain is extremely impressive. But it uses AI to continuously monitor the supply chains of millions of businesses around the world and billions of relationships between them. So, is AI a game-changer for the supply chain security, how do you see that, and how do we make sure the government makes use of it?

Ms. BISCEGLIE. I think automation is a game-changer for supply chain security. Because supply chains are dynamic, and they change, and they are uncontrollable. So, we have to leverage tech-

nology and get out of human manual processes in an effort to make a difference. And AI is definitely the path to do that.

Ms. MACE. OK. Thank you so much. I have a question for you, Mr. Lewis, Dr. Lewis. Your testimony says major Chinese software companies may be placing chunks of code in popular apps and online services. It says they are in effect invisible, embedded in a larger American product. So, China could use back doors into our computer systems so they can spy on us and disrupt file services. Would you agree?

Dr. LEWIS. Unfortunately, they have created back doors in code and used it.

Ms. MACE. Is it just the code? Is it just software? Are they also putting software in hardware that we buy? Our government buys Chinese hardware, don't they?

Dr. LEWIS. They are a full-service intelligence operation. But they have already used, in two cases, this kind of software.

Ms. MACE. But I cannot understand why we buy Chinese tech products for government agencies. It is mind-boggling to me. All right. With that, I will yield back. And I see my colleague, Mr. Connolly, my friend from Virginia, I would like to recognize you.

Mr. CONNOLLY. Thank you. Thank you, Madam Chairwoman. I am sorry I am late. We had a markup at Foreign Affairs, and Foreign Affairs is still under construction, so we are meeting in the big room in the visitor center. So, we had recorded votes I had to make. So, I am so sorry.

Madam Chair, if it is more convenient for you, I can wait on the opening statement. Whatever you wish.

Ms. MACE. Do you want to make your opening in closing?

Mr. CONNOLLY. Yes, if that works. OK. Great. So, I will start my questioning. Thank you so much.

Mr. Jaffer, you are a cybersecurity expert and Executive Director of the National Security Institute at the Antonin Scalia School of Law.

Mr. JAFFER. At George Mason University in your district.

Mr. CONNOLLY. Also known as ASS Law. Would you agree that adopting zero trust security model is important to supply chain risk management?

Mr. JAFFER. Absolutely. Zero trust is a critical capability that we need to apply across the software supply chain and more generally across the government networks. That being said, it is not a silver bullet. Zero trust can be applied in a million different ways. You have got to do it. You have got to do it right. And, frankly, you have got to buy more secure software at the outset. And we have got to really hold the threat actors that are coming at us accountable. Today they can exploit U.S. Government systems with virtual impunity and pay almost no cost and certainly no public cost. That comes at a price as well.

Mr. CONNOLLY. How about continuous monitoring and automated response and conducting regular security training for employees?

Mr. JAFFER. Well, you have hit on something that I am a big fan of. I believe continuous monitoring is critical. The idea that we do not continuously monitor out networks or employees is crazy given that we have complete authority to do so today. And security training is critical. But it has got to be, again, as Ms. Bisceglie said, it

cannot be check-the-box training. It has got to be actually consistent, capable, and the like.

Mr. CONNOLLY. Right. Because you got to remember what the goal is. It is not training. It is to prevent bad things from happening.

Mr. JAFFER. Exactly. Good point.

Mr. CONNOLLY. Do you think it would be worthwhile for Congress to conduct oversight in how agencies are doing in each of these categories we just discussed?

Mr. JAFFER. Of course.

Mr. CONNOLLY. Ah. So, you are aware of the fact that the FITARA scorecard and our bipartisan FISMA metric in fact, already does that.

Mr. JAFFER. I am.

Mr. CONNOLLY. Should we do more of it?

Mr. JAFFER. I think, as Ms. Bisceglie said, you can do more of it better, I would say. It needs to be smarter, more flexible, more capable. The problem is, say, FITARA is a check-the-box exercise, right? It is a bunch of rules. You have got to go through it. Everything you buy, or a lot of stuff you buy has got to be purchased through FITARA and reviewed. The problem is it does not really do the job effectively. So, scorecards are great, but they have to be flexible and good. And they have got to also allow you to buy highly capable moderate software.

Mr. CONNOLLY. Have you worked in the Federal Government, Mr. Jaffer?

Mr. JAFFER. I have, unfortunately.

Mr. CONNOLLY. I think you understand we have to get basics first.

Mr. JAFFER. Agreed.

Mr. CONNOLLY. And the fact of the matter is that scorecard says $30 billion according to the GAO. I challenge anyone to find another Federal piece of legislation that has effectuated government savings of $30 billion.

Mr. JAFFER. Congressman, I am—saving government money and our taxpayer dollars is 100 percent the right thing, but we also want good security. And we want to buy modern capable software products.

Mr. CONNOLLY. Exactly. That is the goal, Mr. Jaffer.

Mr. JAFFER. Agreed.

Mr. CONNOLLY. We need to retire legacy systems. We need to make sure we are up in the 21st century. We need to make sure everything can be encrypted and protected on behalf of the American taxpayer. And I think that is the goal.

Mr. JAFFER. Totally.

Mr. CONNOLLY. Ms. Bisceglie—have I pronounced that correctly?

Ms. BISCEGLIE. Yes, Bisceglie.

Mr. CONNOLLY. Ms. Bisceglie, why is it important that cloud service providers meet certain privacy controls, like identifying and enumerating system vendors?

Ms. BISCEGLIE. Oh, I think, again, it creates a red line or a base that we all have to adhere to. And I think it is a start. I think it is an education. And I think it gives us some level of protection, but it does not keep you away from the conversation you were just

having with Mr. Jaffer, which continuous monitoring in a dynamic environment is where we need to live.

Mr. CONNOLLY. Right. And what about developing and enforcing risk management plans for supply chains and establishing risk management teams for those supply chains.

Ms. BISCEGLIE. I could not agree more. And I think under several administrations ago, you started seeing teams being set up. What I shared in my testimony is that none of this is funded. And that is a problem.

Mr. CONNOLLY. Yes. So, we passed a bill in the last Congress finally authorizing FedRAMP. And FedRAMP, in fact, enforces those cybersecurity measures. Are you familiar with those provisions?

Ms. BISCEGLIE. Yes. I am going through it right now.

Mr. CONNOLLY. Good.

Ms. BISCEGLIE. I also think, though, again, that the compliance activity, I think it is a good baseline. It is not risk management.

Mr. CONNOLLY. Yes.

Ms. BISCEGLIE. And you brought up a really good point a few minutes ago. We have to remember the enemy we are fighting against, which is not ourselves, it is not the FAR. And necessarily, saving money could be at odds with security.

Mr. CONNOLLY. Yes, that is true.

Ms. BISCEGLIE. You know, we need to remember that.

Mr. CONNOLLY. And it is absolutely true. And I think Mr. Jaffer was getting at the same point. You want to measure the right things.

Ms. BISCEGLIE. Correct.

Mr. CONNOLLY. And the right things we want are efficacious outcomes. So, training and awareness is a means to that end. It cannot be the end in and of itself. And I think previously we have written legislation that unwittingly rewarded the wrong metric. And so, we would have testimony from Federal agencies coming here saying 95 percent of our staff can be trained and made aware. And you think, OK, but are hacks more successful or less? Are there more of them or fewer? And, of course, that was a different question and a different answer. So, I could not agree with you more. Thank you. I yield back.

Ms. MACE. Thank you. I will now recognize Mr. Timmons of South Carolina for 5 minutes.

Mr. TIMMONS. Thank you, Madam Chairman. Mr. Jaffer, you talked about holding foreign adversaries, foreign actors accountable, creating a policy that would create an avenue for retribution or accountability, whatever you want to call it. I very much agree with you. I think we have a big problem right now because if a foreign adversary, a government fired a rocket and blew up a building, we would make the business that owned the building whole and then we would go to war. But if that same foreign adversary does a cyber-attack and cost that business hundreds of millions of dollars, their insurance is not going to pay for it because it is foreign government, and we are not going to do anything. So that is a problem.

So, the question then comes what do we do? And I mean I think that the Federal Government needs to take the position that if a foreign government engages in a cyber-attack on a U.S. business or

a U.S. entity, that they will then make the business—the government, the Federal Government, the U.S. Government will make that business whole, and then using whatever mechanisms we want, get the money or get retribution from the attacking country. Do you agree with that general premise?

Mr. JAFFER. Look, I think as a general matter we have got to hold foreign nation state actors that come after us, whether it is our companies, our critical infrastructure, our government, accountable. We do not do enough of that today, right? That could be done in a variety of ways. It can be we prosecute them. The Justice Department have indicted dozens of Chinese state actors, dozens of Russian state actors. We are never going to get them into U.S. courts, right, but it sends a message.

The real question, though, is how do you hold them accountable in the cyber domain or in other domains where they actually feel the pain. And today, nobody that comes after us, particularly the big nation states, feel any pain when they come after U.S. Government. Rarely the President might go to Xi Jinping and say, I have got a problem in these sectors, right? But by and large, we do not do that, and then we do not actually extract costs. That is the key in my mind.

Mr. TIMMONS. Assuming—let us just move the conversation of attribution. Let us just say that everybody agrees that it was China.

Mr. JAFFER. Right.

Mr. TIMMONS. I mean, why would we not use economic sanctions to say: The cyber-attack costs this much. We paid that. We are going to do economic sanctions to address this. And if you do it again, we are going to multiply it by two. And, by the way, any other country in the world, if you do it, you are going to start out with a dollar for dollar, and then we are going to do two dollars for one dollar.

Mr. JAFFER. Exactly. If we could extract that kind of cost and make it really cost them, they are going to think twice about using it. They might still do it at times, but it is going to reduce the overall amount of these things happening by a significant portion.

Mr. TIMMONS. How do you then reconcile the issue where a lot of the cyber-attacks are coming from Eastern European, Southeast Asian countries that have limited rule of law, and the countries are not necessarily able to hold the people accountable? I mean, I guess, in my mind, in that scenario you say that this person at this address attacked us, and it cost us this amount. We will give you assistance to prosecute these people, to hold them to account. And if you want to let us help you do that, we will not charge you any money. We will then prosecute that person. But if you do not want to help us, if you do not want to address the lawlessness in your country that is adversely impacting our citizens, our economy, then we will extract dollar for dollar from you. And if they do it again, we will do the same thing, two for one.

Mr. JAFFER. Three quick thoughts on that. One, it cannot just be an economic penalty. There has got to be other consequences as well. Economic penalties are good, we need to do more on that front.

No. 2, you know as a former prosecutor and a member of the Air National Guard, right, we can encounter in the terrorism scenario,

right? Where countries cannot control their own space, and it causes an impact. We say we are going to unilaterally take action. You cannot just say it is not my problem, right?

Then, third, I think at the end of the day, what this really requires is the U.S. Government being clear about what policies are, where our lines are, and what we are going to do. And then when those things happen, we have to take action. We have gotten too used to setting red lines or not setting them at all because we are afraid of enforcing anything.

Mr. TIMMONS. I definitely agree with you on that. Are you aware of any cyber-attack that has resulted in a loss of life.

Mr. JAFFER. So, you know we have seen a lot of these ransomware attacks. There are a couple going on actually today, where hospitals were affected. We have heard that at least in one or two instances people have not made it to the hospital or may have suffered a heart attack or died as a result. Beyond that, right, we know that typically in the military context, cyber is used as an enabling capability and can enable attacks will actually have a real loss of life. So, the trillions of dollars our economy has lost is also huge and cannot be underestimated as a cost as well.

Mr. TIMMONS. My biggest fear is it is going to require a huge loss of life such as a cyber-attack on critical infrastructure in the Northeast during a cold spell, where we are unable to heat our homes for millions of Americans. We would be unable do anything to address that. So, I think that Congress needs to act to increase the overall cybersecurity posture of the U.S. economy and the U.S. Government. And I look forward to working with you all in that endeavor. With that, I yield back.

Ms. MACE. Thank you. I will now recognize Mr. Lynch for 5 minutes.

Mr. LYNCH. Thank you, Madam Chair. Thank you, Ranking Member, as well, for putting together such a great panel. We are all aware of the Log4j mess that occurred back in 2020. And because of the omnipresence of that software on millions and millions of computers, it has taken us a long time to get the patches out there and to deal with that. And now there was a two or 3 weeks ago, we had a North Korean—a similar operation where a North Korean connected attackers injected, again, malicious code into a widely distributed software component in multiple applications, and we are at this again.

So, how do we address this in a timely way so that our response is actually effective? Because, Ms. Bisceglie, this is only going to become more common, right? This is an activity that is—especially with the success they are having, right? There is no reason for them not to continue to do this for either—I think Norton Korea is doing it to raise revenue, but they are also doing it to get information as well.

Ms. BISCEGLIE. I think the thing to realize is that a lot of the success is being enabled simply because technology connects us all. And if we can think about what came out of pandemic and realize that whether you are a physical supply chain or a digital or cyber supply chain, we are just hyper connected to everybody else. And so, the enablement is there. I think it is the reasons that folks are doing this that need to be considered. And I think a couple things

I would like to point out, though. One, to your point, it is not going away. So, if you think about the fight that we have been having for the last 10-plus years just simply on cyber hygiene, supply chain risk hygiene needs to be leveled up. And I think the Ranking Member brought up a really good point. It cannot be training and awareness for the sake of training and awareness. But folks have realized what supply chain security is about and why they are doing it and what they are trying to protect. It is not just nation states that are trying to get us, it is bored 18-year-olds sitting in their parents' basements that are seeing what they can steal, and we have seen a lot of examples from that.

Mr. LYNCH. So, what is the Navy doing that others are not doing, and is that—can we replicate that across the governmentwide?

Ms. BISCEGLIE. We absolutely can. And the contract, and the program is set up to do that. And I want to thank a lot of the Committee Members here for supporting it. If you think about how we, as a Federal Government, are funded, we are normally funded program by program. So, the Columbia class versus the Virginia class versus the F–35, they only look at their own discreet supply chains. And this is the very first funded program that looks across supply chains. And so, if I were to get very specific, we had the opportunity to support the Navy for 6 years before the Navy actually went to an enterprise-wide capability. We took 80 weapons programs and just leveraged our technology to map out 3 tiers. So prime, tier 2, and tier 3, 60,000 suppliers. You can imagine how many times the same supplier was in multiple places.

So, when SolarWinds happened, we were able to show them the ripple effect of which programs are going to be affected. It showed, for the first time, cross program funding and the power of resiliency. That is what the Navy has done. And the last Fiscal Year that we just finished, they actually extended the capability to the Missile Defense Agency and the DOD CIO cyber capability. So, they are already seeing cross agency success, not just cross program, and it is absolutely set up to look across the entire department.

Mr. LYNCH. So, the efficacy of continuous monitoring, would it be possible—I mean, is that what the Navy is employing in order to——

Ms. BISCEGLIE. Absolutely.

Mr. LYNCH [continuing]. Now that they are doing it across several supply chains?

Ms. BISCEGLIE. They are. They are a hundred percent continuous monitoring real time.

Mr. LYNCH. And they are using AI to do that?

Ms. BISCEGLIE. They are.

Mr. LYNCH. OK.

Ms. BISCEGLIE. So, you think about what happens should ACME Incorporated have a ransomware attack. Instead of every program having to do the research to figure out if they are going to be impacted, the artificial intelligence platform is able to actually alert them and tell them where the impact is coming from. It allows them to be responsive that much faster, which goes back to your original question, which is how do we get better at this?

Mr. LYNCH. In our contracting world, we have preferred customers, preferred firms that we deal with. So, we could basically say, in order to be a preferred customer, you have to have this protocol or this framework that is in compliance with our supply chain security. And like—I think you mentioned it earlier in your testimony, you said make it a cost of doing business, right? So, when a company comes to do business with the United States as a contractor, they have to have this in place. How disruptive would that be to our contracting process?

Ms. BISCEGLIE. A lot less disruptive than when something goes wrong.

Mr. LYNCH. Fair enough. Fair enough. Yes.

Dr. Lewis, anything else you would like to add to that?

Dr. LEWIS. A couple points that are probably worth the Committee looking at further. I only talked to a retired admiral, so maybe they do not know what they are doing. But I do not think anybody would rank the Navy in first place when it comes to cybersecurity. Something to look at. Second, there has been a long discussion for about a decade on the issue of accountability, and this Administration is doing OK on it, better than some of its predecessors, and that goes back to Clinton.

But we are not ready to get into a game of whack-a-mole where a Chinese company hacked somebody, and then we do something back. Because that is not going to stop them. So, we do need a more comprehensive approach. Just these are topics you might want to look at because they have been discussed for a long time. There is, just recently, the Administration had something called the counter ransomware initiative that had 48 countries, and it talked about these issues. How do we go back to people? And one thing to remember is other countries are not where the U.S. is. They are not ready to go to war over a cyber-attack. So, it is a complicated picture. Supply chain is part of it, but just part.

Mr. LYNCH. Madam Chair, thanks for your courtesy. I appreciate that. I yield back.

Ms. MACE. Generosity. Mr. Langworthy, you are now recognized for 5 minutes.

Mr. LANGWORTHY. Thank you, Madam Chair. Each year Federal agencies spend more than a hundred billion dollars on IT and cyber-related investments. It is not always clear, however, that the source and providence of each technology component. This is especially true for software. In Executive Order 14028 entitled, "Improving Our Nation's Cybersecurity", the National Institute for Standards and Technology was required to issue guidance regarding how vendors provide Federal purchasers a software bill of materials, SBOM, essentially an ingredient list for software that details every component, library, and module that makes up the product.

Mr. Waldron, do you believe Executive Order 14028 is heading in the right direction? Do you believe that the Federal Government is considering implementing SBOM guidance or requirements?

Mr. WALDRON. Yes, it is the right direction. The question is the execution on the contracting side. In looking at developing some standard formats. The issue in Federal procurement is the Federal acquisition regulation, agencies have all kinds of supplemental reg-

ulations. When you start developing an SBOM and a format, you have got to talk to industry. You have got to sit down with industry, come up with a common nomenclature, understanding what is going to—actually what is actually going to be reported as part of those ingredients.

Companies take this really seriously. It is a certification in a certain sense. When you submit that to the Federal Government, you are saying this is our software bill of materials, and the government is going to rely on that. And it creates compliance issues and risks for industry, too. So, they want to get it right. So, the more government and industry can talk about it to implement it more effectively, that is going to be critically important moving forward.

Mr. LANGWORTHY. And I must say that SBOM sounds a lot cooler than S-B-O-M. Appreciate that nomenclature. Shifting focus to you, Mr. Jaffer, could SBOMs offer a viable solution for securing the Federal software supply chain?

And additionally, what are some of the concerns or drawbacks associated with SBOMs as a potential solution?

Mr. JAFFER. Well, a couple of things. One, SBOMs can certainly help, but only if you use them for a good purpose, right? So, once you know what is in the software, people have to do something about it. And they have to actually design their software in a way that is secure and resilient inherently and holding people accountable for that rather than sort of what is in your soup. What makes the soup good is important.

The second thing is, look, by exposing everything that is in a bill of materials, right, in the software, it also gives our adversaries information about what to go after. So, there are upsides and downsides. Net/net, I think SBOMs are worthwhile doing, but I agree with what Mr. Waldron said, you have got to do it in a smart way, in a way that is capable, and use it for actually useful purposes.

Mr. LANGWORTHY. Great. Code is changed regularly, so an SBOM that is accurate 1 day may be wrong the next day or even later that day. Are there any solutions to making this process easier for developers, especially small business developers who do not have the resources that the big companies and conglomerates do that have maybe—they have turned away by SBOMs because of the work requirement to maintain them?

Mr. JAFFER. Use technology. You can imagine these things being updated in real time, but of course we are a government that is not, sort of, oriented to operate in that way. We are oriented to operate by stacks of paper. As Mr. Connolly was talking about, right, this is not a common thing. If we can have people update in real time. You know, I mean, look, you can get code in real time on GitHub. Why cannot we use a similar capability to update our SBOMs? It seems obvious. But the government is not good at buying new capable technology at a moment's notice, taking risks—we do not incentivize risk taking, even when it comes to buying American technology, that is crazy.

Mr. LANGWORTHY. So, do you believe AI will impact the SBOM landscape?

Mr. JAFFER. No doubt it will. It could make it better. It could make it more challenging. At the same time, we just have to en-

courage our government and our government procurers to do things that are unusual and not just buying programs of record, buying capabilities, having money to do that. And when they do it, and they do not get it quite right, Congress will hold them accountable, but not punish them. Ultimately, you cannot incentivize risk if you are going to punish somebody for taking risks.

Mr. LANGWORTHY. Would the existence of SBOMs have helped Federal agencies defend or mitigate against the recent high-profile attacks such as SolarWinds.

Mr. JAFFER. It would have let us know what is in there, but stop them, no.

Mr. LANGWORTHY. OK. Well, every passing day brings a surge in both the quality, the quantity, and severity of cybersecurity threats facing our country. In the traditional notion of invulnerability, it no longer holds true, as threats now transcend physical borders originated from adversaries working remotely. We are committed to collaborating with the Oversight Committee and our colleagues to continuously advocate for robust policies that fortify our Federal cybersecurity defenses in response to this evolving threat landscape.

I really appreciate all of you coming in here to testify today. It is very helpful. Thank you, and I yield back.

Ms. MACE. Thank you. In closing, I want to thank our panelists, all of you for being here this afternoon and spending time with us, for your testimony today. And I will yield to the Ranking Member for a statement.

Mr. CONNOLLY. Thank you so much, Madam Chairwoman. I will enter my full statement into the record. And just this last Thanksgiving week and this last weekend, Microsoft reported that a North Korean nation state actor linked to a notorious cyber-crime group, Lazarus, stole a software sign-in key and inserted malware into a legitimate application developed by the Taiwanese multimedia software and AI developer, CyberLink. The malware, known as landload, infiltrates systems by dropping a fake PNG file to deploy malicious code. That code enables unauthorized users to steal sensitive data, establish persistent access to traditionally protected systems, and corrupt other connected systems. Hackers used landload to successfully compromise a hundred devices in multiple countries, including Japan, Taiwan, Canada, and the United States. The fullest extent of that attack and its damage we do not know yet. It is a week old.

And that, on top of SolarWinds, on top of all kinds of other examples we do not even know about, I think, underscores the point that we have got to protect the Nation's assets—supply chain, proprietary information, intellectual property, data bases, privacy.

And I guess I would come back, Mr. Jaffer, I think you made a lot of good points, but I also would gently suggest, you are a little facile about checking the box when it comes to statutory requirements. Because—and that is why I asked you if you had worked for the Federal Government. Because, working for the Federal Government, you know, normal assumptions on how we work in the private sector do not apply.

Ms. Bisceglie pointed out, if you look at weapons systems, we are all in our compartments, and we do not share. We do not work

across the board. It is not our culture. If I have learned in my agency how to protect against cyber-attacks, that does not mean I am going to let you in on the secret.

So, trying to change the culture by having metrics where you are going to be judged and metrics that will materially improve operations and save tax dollars and allow us to be cyber secure is kind of our goal. But you have got to create the architecture. And I have learned the hard way that in bureaucracies, you have got to create metrics people have to meet. And they have got to be meaningful metrics, right, as we discussed.

And, you know, when we began FITARA, there were 250 people in 24 agencies with the title CIO. But who was in charge? Nobody. Everyone could assume responsibility under that system. So, trying to empower a CIO, a primary, Latin primus inter pares, the first among equals, so that there is somebody, and that somebody, according to our scorecard, has to report to the boss.

Because, again, we know org charts matter. Likewise, data centers, not checking a box. We retired 4,000 Federal data centers. We did not even know how many there were when we began. We thought there were only 900. You remember? Vivek Chudgar thought there were 900. We cut it in half. Well, it turned out there were thousands. And we only knew that when we made them have to measure it. We eliminated 4,000 of them saving billions of dollars.

So, I just, you know, we got to be respectful, I think, of the statutory architecture required if we are going to make progress. And next steps, we got to go after those legacy systems. We got to make sure that we are using software and supply chains that can be protected from a cyber point of view, so that we are avoiding what Microsoft reported just last weekend.

So, on that note, thank you. I think this is a thoughtful subject, Madam Chairwoman, thank you for doing it, but I think we have a lot more progress to go. And we cannot assume the basics are in place. I wish we could, but we cannot. Thank you for being here.

Ms. MACE. And I will add to that if our Federal agencies are unwilling to make those changes because they are kings around their own kingdoms, not willing to move forward, it will never happen.

So, with that and without objection, all Members will have five legislative days within which to submit materials, and to submit additional written questions for the witnesses which will be forwarded to the witnesses for their response.

So, if there is no further business, without objection, the Subcommittee stands adjourned.

[Whereupon, at 3:19 p.m., the Subcommittee was adjourned.]