Stenographic Transcript
Before the

Subcommittee on Cybersecurity

COMMITTEE ON
ARMED SERVICES

UNITED STATES SENATE

TO RECEIVE TESTIMONY ON FUTURE CYBERSECURITY ARCHITECTURES

Wednesday, April 14, 2021

Washington, D.C.

ALDERSON COURT REPORTING
1111 14TH STREET NW
SUITE 1050
WASHINGTON, D.C. 20005
(202) 289-2260
www.aldersonreporting.com

TO RECEIVE TESTIMONY ON FUTURE CYBERSECURITY ARCHITECTURES

Wednesday, April 14, 2021

U.S. Senate
Subcommittee on Cybersecurity
Committee on Armed Services
Washington, D.C.

The subcommittee met, pursuant to notice, at 2:33 p.m. in Room SR-222, Russell Senate Office Building, Hon. Joe Manchin, chairman of the subcommittee, presiding.

Committee Members Present: Senators Manchin [presiding], Gillibrand, Blumenthal, Rosen, Rounds, Wicker, Ernst, and Blackburn.

OPENING STATEMENT OF HON. JOE MANCHIN, U.S. SENATOR FROM WEST VIRGINIA

Senator Manchin: The hearing will come to order.

First of all, good afternoon to my fellow members and our three witnesses, and I appreciate so much you all being here. Joanie, it’s good to have you too.

We have Senator Rounds on the phone with us. He is with his wife, and she’s having some procedures, and they’re together right now, so we’re just glad to have him on the phone with us.

The focus of today’s hearing is on what the Defense Department needs to do to improve its defenses against modern and very sophisticated cyber attacks like the SolarWinds campaign waged by Russia, and the Microsoft Exchange email server operation waged by China. These hacking operations subverted tens of thousands of critical government and industry networks and undermined trust in the information infrastructure that supports our economy, our government, and our private lives.

We’re holding this hearing today in open session because it is vitally important for the American people to learn how the Federal Government is going to respond and to better protect the nation. This is a very serious business, and I know you all understand that very well. Hardly months passed between one appalling breach and the next. We have never experienced the like in our history as a nation.

For many years, our effort to shore up cyber defenses focused on making it hard for adversaries to break into our networks. We built the digital equivalent of higher castle walls and moats. These are important and necessary, but it has proven so far to be impossible to keep intruders out, for there are always many other ways to get inside. And once inside, hackers can easily move about unnoticed and unchallenged because everyone and every device inside the perimeter is trusted.

There is even a saying for this: A network that is only defended at the perimeter is like a candy with a hard shell that is soft and chewy inside. In fact, cybersecurity professionals have known this truth for years and have been developing, and even deploying and applying, concept technologies for dealing with it.

The dreadful SolarWinds and Microsoft breaches are simply the exclamation marks at the end of the sentence. We have to assume at all times that our networks have been penetrated, that at every moment adversaries are inside our system. We have to act on the possibility that every action and transaction on our networks is being conducted by an adversary. We have to constantly challenge and verify the identities and the credentials of all the users.

For shorthand, these basic network design concepts and operational imperatives are called zero trust. I'm asking our witnesses to explain to the committee and the American people what zero trust means in plain English, without acronyms or jargon. We need to know what the essential building blocks of a zero trust network look like and where we are in terms of defining and acquiring these building blocks.

I now ask my good friend, Senator Rounds, and the subcommittee Ranking Member, for his opening remarks before turning to our witnesses.

Senator Rounds?

STATEMENT OF HON. MIKE ROUNDS, U.S. SENATOR FROM SOUTH DAKOTA

Senator Rounds: Mr. Chairman, thank you. I really do appreciate being able to work with you on this very important subject. I'd also like to thank our witnesses for appearing before us today to discuss this important topic.

Over the last few months we've learned a lot about the details and scope of the SolarWinds breach. We now know that an advanced, persistent threat actor, Russia, compromised the supply chain of a software company, SolarWinds, and inserted a back door into a genuine version of the SolarWinds software product. Russia then used this back door, among other techniques, to initiate a campaign of cyber attacks against U.S. Government agencies, critical infrastructure entities, and private-sector organizations.

In the last few weeks we have also learned of another troubling breach attributed by private industry to a Chinese group known as Hafnium. This breach exploits four newly-disclosed vulnerabilities in Microsoft Exchange. Microsoft has released a patch which is currently being deployed across the Federal Government, including DOD, but it will take considerable effort to assure that these hackers are removed from the networks.

Both of these breaches show that the capabilities and skills of malicious cyber actors are becoming more sophisticated and demonstrate the importance of improving the cybersecurity of our Department of Defense Information Networks, also known as the DODIN. Previous cybersecurity initiatives have focused on cybersecurity practices known as perimeter defense, as the Chairman noted, essentially building a bigger and stronger series of walls to protect our networks. These breaches make it clear that this approach is no longer adequate and we must implement stronger cybersecurity defenses known as the zero trust architectures that can protect our systems if an attacker gains access to the network.

Over the years, the Department has come to depend on a large number of cybersecurity tools to defend our networks, each with its own defense capabilities but challenging to use cohesively. So the Senate Armed Services Committee has focused on integrating complementary cybersecurity tools and capabilities, what is referred to as cybersecurity orchestration. The National Security Agency, or NSA, has conducted a multi-year effort known as the Integrated Adaptive Cyber Defense, or IACD, in cooperation with commercial industry to develop the mature cybersecurity orchestration technologies.

For Fiscal Years 2019 and 2020 National Defense Authorization Act, both included provisions requiring the Department of Defense to conduct pilot programs for security orchestration. Technologies like orchestration can better integrate the tools we already have to provide a stronger baseline defense by sharing information between complementary cybersecurity tools.

I look forward to hearing today what the Department has done regarding the orchestration pilot that we have required in the previous NDAA, and to hearing about the efforts by the Department to implement the broader zero trust architecture.

Thank you again to our witnesses for coming here today.

Now, since I’m not going to be there in person today, Mr. Chairman, I plan to submit my questions for the record.

Senator Manchin?

[The prepared statement of Senator Rounds follows:]

Senator Manchin: Thank you, Senator Rounds. We wish your beautiful wife Jean all the best and hope to see you soon.

Before we begin, I want to welcome our distinguished witnesses today and thank them for their service to our nation.

We have with us Mr. David McKeown, Mr. Rob Joyce, and Admiral William Chase.

Mr. McKeown is the Deputy Chief Information Officer for Cybersecurity, with 33 years of experience in the Air Force and the Office of the Secretary of Defense.

Mr. Rob Joyce has a stellar career in NSA on both the collections side and the defense of cybersecurity side of the agency. He is newly returned from London, where he served as NSA’s top signal intelligence representative to the United Kingdom. Prior to that assignment, he served as President Trump’s cybersecurity coordinator on the National Security Council staff. He is newly assigned to lead NSA’s Cybersecurity Directorate.

Admiral Chase was recently confirmed by the Senate for his second star.

Congratulations, sir.

He is currently serving as the Senior Military Advisor for Cyber Policy to the Under Secretary of Defense for Policy and the Deputy Principal Cyber Advisor to the

Secretary of Defense.

I understand that, in the interest of time, our three witnesses' opening statements have been consolidated into one, which will be presented by Mr. McKeown.

STATEMENT OF DAVID MCKEOWN, SENIOR INFORMATION SECURITY OFFICER/CHIEF INFORMATION OFFICER FOR CYBERSECURITY, DEPARTMENT OF DEFENSE

Mr. McKeown: Good afternoon, Mr. Chairman, Ranking Member, and distinguished members of the subcommittee. Thank you for the opportunity to testify today regarding the efforts of the Department of Defense to accelerate implementation of a zero trust framework across the Department of Defense Information Network, commonly referred to as the DODIN, in a response to the recent SolarWinds Orion and Microsoft Exchange server incidents.

My name is David McKeown, and I am the Department of Defense Deputy Chief Information Officer for Cybersecurity and the Chief Information Security Officer. Alongside me is Mr. Rob Joyce, Director of the Cybersecurity Directorate at the National Security Agency, and Rear Admiral Bill Chase, Deputy Principal Cyber Advisor to the Secretary of Defense and Senior Military Advisor for Cyber Policy to the Under Secretary of Defense for Policy.

As the owner of the Department of Defense’s Cybersecurity Strategy’s Roadmap and Reference Architectures, I drive the continuous improvement and modernization of our cyber defense posture. I ensure that services, combatant commands, defense agencies, and field activities correctly implement enterprise-wide cybersecurity policies, capabilities, procedures, and training on an appropriate timeline. As such, I lead and oversee implementation of the zero trust framework across the DOD.

Mr. Joyce is the leader of NSA's newly-formed Cybersecurity Directorate, which is responsible for the agency's cybersecurity mission and is charged with directly advancing the nation's, the Federal Government's, and the Department of Defense's cybersecurity through technical development, partnerships, and provision of technical advice. As the lead for the intelligence community's and the Department of Defense's most technically capable cybersecurity component, he can provide valuable technical feedback to the subcommittee today based on the agency's considerable cybersecurity expertise and zero trust piloting.

Rear Admiral Chase is the Military Deputy to the Principal Cyber Advisor to the Secretary of Defense. In his current function he oversees and coordinates implementation of the DOD Cyber Strategy, which includes a number of initiatives relevant to the cybersecurity modernization. He can speak to strategic considerations that the Department must incorporate into its implementation plan for zero trust, including those relevant to the service's implementation of OSD cybersecurity policy, acquisition programs, and architectures.

Recent incidents surrounding the SolarWinds Orion and Microsoft Exchange software suites have demonstrated to the public and private sector that our adversaries are increasingly determined and resourceful when engaging in cyber crime and espionage. Novel attacks against networks worldwide will only continue to increase.

We have long recognized that zero trust is the defensive capability best situated to counter the current and future tactics, techniques, and procedures utilized by our adversaries. These recent events have led us to accelerate the implementation of our zero trust framework.

Zero trust represents a paradigm shift in how we design our networks that significantly decreases the potential efficacy of adversary attacks. Currently, untrusted users, machines, applications, and other entities are kept outside of our network perimeter while trusted ones are allowed inside. We have developed advanced capabilities to monitor traffic flowing between untrusted networks, such as the Internet, and our trusted networks to identify attempted attacks or exfiltration of data.

The limitations of this defense are exposed when the adversary is able to establish a foothold on a device within our perimeter on our trusted network. This can be accomplished through tactics, techniques, and procedures such as phishing, web attacks, compromising software we have installed on our trusted network, as in the case of SolarWinds Orion or Microsoft Exchange, or via an insider threat.

Zero trust requires that we constantly interrogate the trust relationships formed by entities on our network and deny by default, only allowing access by an approved user and device. As a result, should an internal or external malicious actor gain access to the DODIN, they would be prevented from moving laterally to other parts of the network, escalating their privileges, or exfiltrating data.

While our perimeter and layer defense tools remain central to defending against most adversary attack vectors, zero trust significantly decreases the potential benefit to the adversary should an attack manage to bypass these defenses.

Our zero trust framework assumes compromise and accordingly leverages existing and emerging cyber defense capability to analyze each transaction on our network prior to approval. Existing investments in areas such as endpoint security and identity credential and access management will be integrated with new investments and tools such as software-defined environments, continuous multifactor authentication, artificial intelligence and machine learning to build our next-generation framework.

These are a sampling of the pillars that make up our zero trust strategy. We provide a more detailed explanation in our statement for the record.

When an adversary attempts an attack, they utilize a variety of tactics to increase the likelihood of success. Each day, millions of these attempted attacks are automatically thwarted by our perimeter defenses, utilizing vectors that we have identified and tuned our defenses to block. Others are intercepted by our network defenders in U.S. Cyber Command who are extensively trained in recognizing and responding to adversary tactics. Still others are prevented by our enforcement of cyber hygiene, such as requiring that all of our devices remain up to date on critical patches and privileged user accounts are closely monitored.

Zero trust provides next-generation assurance that an advanced attack will not be successful. To provide an example, an adversary successfully hijacks a device on our network utilizing one of many possible attack techniques. This gives them a foothold they can then use to traverse to other computers, other network segments, harvest credentials, escalate their privileges, exfiltrate data, or initiate a denial-of-service attack. Under our zero trust framework, that device would automatically be assessed by our comply-to-connect capability to determine if it has the necessary credentials and is properly secured.

Simultaneously, our access management system will determine if the user attempting to access the network with that device is behaving unusually, using non-standard credentials, attempting to access from a location where they do not normally work or at a time when they are not normally in the office.

All of these processes will be centrally monitored by an automated system. If something does not match up, our system will automatically challenge the user and machine to provide additional credentials and other verification. Access to the network beyond that device will be blocked, and sensitive data will remain safely encrypted.

The events associated with the attack will be constantly tracked, and our human defenders will be notified so they can monitor suspicious behaviors, alert the local network operator of potential attack, and take additional actions to repel and deter the attacker.

DOD has been laying the foundation for the implementation of the zero trust framework across the DODIN. This is a significant effort but one we have no doubt we can achieve. Through our current effort to accelerate this implementation, we will leverage our recently approved zero trust reference architecture as a blueprint to integrate existing and new cyber defense capabilities that are critical to enable zero trust.

As we continue to transition to the cloud, we will ensure that these environments are built from the ground up utilizing our zero trust architecture. Cloud One and Platform One, developed by the Air Force, are prime examples of environments with native zero trust design.

We will also continue to expand our pilot programs which provide strategic insights and allow us to work out the particulars of deploying zero trust on our broader network.

While we have focused today on the implementation of zero trust framework on our own networks, we will also continue to engage with Congress, Federal civilian departments and agencies, the private sector, and our allies to promote a whole-of-community unified defense. We view the DOD as a leader and partner in this implementation of a zero trust framework and a pioneer of the cyber capabilities that make such a framework possible.

We would like to thank you for the opportunity to share our perspective, and I’m happy to answer any questions you might have.

[The prepared statement of Mr. McKeown follows:]

Senator Manchin: Thank you, sir.

With this beginning our open hearing, members have the opportunity to question via Webex, so we’re going to keep the seniority order for questions as we do during full committee hearings for Armed Services.

My first question will be to Mr. Joyce. As you know, Russia in the SolarWinds hack and China in the Microsoft hack both launched their attacks from and exfiltrated stolen data through servers rented from the U.S. cloud providers. So my question would be with your thorough background in collection at the NSA, can you tell us in the open setting if you’ve noticed collaboration between our adversaries in cyber operations? Have they essentially been ignoring each other, or are we aware of any cyber operations they have conducted against one another?

Mr. Joyce: So, Senator, I think you’ll understand the sensitivity of that question and my ask that we take that in a closed hearing.

Senator Manchin: Let me try this one, then. I trust that we’re taking action to breed distrust between our adversaries. Can you give us a general example of what we’re doing to discourage future cooperation, or is that too sensitive?

Mr. Joyce: So, Senator, I do think that I can talk to some of the activities.

Senator Manchin: Sure.

Mr. Joyce: One thing that NSA has worked hard to do is to understand the adversary's plans and intentions, and then we work with partners such as the Federal Bureau of Investigation, U.S. Cyber Command, Department of Homeland Security, and we, through those activities, have been issuing guidance that talks about the tradecraft of the adversaries, the things they do, the techniques they're using, and the indicators that would help us find them in our networks. And so by doing that, we feel that what we're doing is we're taking away the tools and capabilities of these adversaries by exposing the implants and the malware. They then lose that capability and they have to go back and try to redevelop it.

Senator Manchin: Admiral Chase, this is for all the witnesses, and I have a last question for Mr. McKeown. But to Admiral Chase, most of all of your prepared testimony includes statements about how this or that action "would allow our network defenders to continue to outpace the adversary." Are we really outpacing the adversaries, or is this basically wishful thinking, or we're actually there where you think we need to be?

Admiral Chase: Senator Manchin, we can always do better. But there is a sense of urgency that I think the world has seen from the supply chain attacks. So the idea that we could ever rest on what we have is certainly a false one. We want to do better.

The good news is we’re taking this with urgency. Additional good news is we’re not starting from scratch. Some of the very issues that you talked about in your opening statement, the orchestration, the comply-to-connect that you asked us to build pilots into to learn from, have had significant success just over the last couple of years in being able to see our networks in unprecedented ways.

Are we finished? Absolutely not. We’ve taken the beginning steps and are only now starting to understand how much better we can be about it. We’re always looking for the insights that come from our NSA and IC partners to be able to build on those and to go faster. This is probably the arms race of our time. We’ll get to continue to do this for a very long time. As the adversaries get better, the defenses will get better.

Senator Manchin: Thank you.

Mr. McKeown, massive Russian SolarWinds infection was discovered by the cybersecurity company FireEye through what is now a standard industry technique called threat hunting. The threat hunting concept, like the zero trust model, is based on the assumption that adversaries are always inside one’s network undetected instead of passively waiting to accidentally discover such intrusions, which are well documented. Research shows it allows intruders to remain undetected for many months, and even years. Threat hunting involves actively looking for indications of compromise.

It’s a technique that CYBERCOM already applies with its cyber protection teams, but we really need to expand the threat hunting as the private-sector companies have done. So why isn’t threat hunting listed as one of your zero trust pillars?

Mr. McKeown: Chairman Manchin, you’re absolutely correct that threat hunting is an important tool set capability within our arsenal. What we’re building here with zero trust is going to enable local cybersecurity service providers with a lot of the same capabilities that threat hunters have when they arrive on the scene.

Threat hunters are a scarce resource. We don’t have the ability to put them everywhere and have them be there all the time monitoring everything. The techniques that they employ when they go out on a network, trying to clear it of any adversary that might be on there, are very similar to what we’re implementing here with zero trust. So we’re kind of taking a paradigm that was built by the cyber protection teams and we’re moving it closer to the fight where the local cybersecurity providers and the local operators can see that data.

As a consequence, when the hunt teams do come in, they're going to be able to more rapidly respond because many of the same tools, a lot of the logs, a lot of the information that they would potentially take days and weeks to collect are going to be there for them right off the bat.

Senator Manchin: What you're telling us is the most common hunting technique is to put a little software program on every computer in an enterprise that creates a small record of every significant action the computer takes and sends those records to a big repository for analysis.

Mr. McKeown: Yes, sir. And we're going to be doing that exact same thing on all the devices and all the traffic that's happening on the network itself. And we're going to be doing artificial intelligence and ML learning on that data to maybe uncover new and novel attacks, as well.

Senator Manchin: Thank you.

Senator Ernst?

Senator Ernst: Great. Thank you, Mr. Chair. I really appreciate it, and as well to our Ranking Member Rounds.

Gentlemen, thank you for being here today and providing testimony for us. I do believe that our current and future cyber capabilities, including that architecture, are critical to the overall national security, of course, and we have to make sure that we're getting it right, which is why I'm glad we're having this discussion today.

But what we need to know is how to make sure that we have the correct incentives available, that we have the right architecture -- we've talked a little bit about that -- and the authorities, as well, to make sure that we're protecting all Americans and deterring our adversaries. So I appreciate that you're joining us, giving some good insight.

Mr. Joyce, I'll start with you, please. When General Nakasone testified before our committee a few weeks ago, he said that the problem is not that intelligence agencies cannot connect all of the dots. It's that we cannot see all of the dots. And he was referring to adversary cyber attacks on U.S. soil. So, in your opinion, how do we ensure and incentivize the right balance of information sharing between private companies, as well as our governmental agencies?

Mr. Joyce: Thank you, Senator. I think you raise an important topic. What we understand is the private sector owns and operates a lot of our networks. All of the international traffic that would come at the Department, that would come at our critical infrastructure, that would come at sensitive government networks actually traverses these commercial networks. So we have to have a special relationship with these companies so that we can understand as defenders when they see a threat, and we also have to have a way for the government to inform them about the sensitive special things that we know so that they can operate on their networks to protect our equities.

It is true that over time we've put a lot of energy into some of this information sharing, but we still haven't gotten it right. The fact that the foreign actors like Russia and China are renting computers inside the U.S. to launch their attacks shows that they appreciate they can get inside our cycle and ability to get that information, and they're safer there than operating outside.

I think when General Nakasone raised the point about seeing the dots, he wasn't giving an authorities set. He was talking about the need for us to solve the problem of getting people to put together those dots, put them on the table, and take the parts we both have to bring the other solution.

Senator Ernst: Right. And I've heard from Iowans as well on the issue when we talk about cyber attacks, and there are cyber attacks that are coming from domestic organizations, sometimes from outside threats that truly are threats, but they're coming after financial institutions, maybe they're coming after medical systems. So they get very concerned about sharing information about those attacks when it may deal with very private information of our United States citizens. So that's always been a concern. Your thoughts on that?

Mr. Joyce: That’s an outstanding point, Senator. But the thing we have to recognize and find the techniques is to share the tradecraft and the activity, not the data they’re targeting but actually the ways that the foreign adversaries are coming at those networks and trying to exploit them.

Senator Ernst: Yes, that’s a very, very good point. Thank you.

And then how are we actually partnering with some of those private entities? Is there written memoranda for information sharing agreements? How do you go about that? Is it that an attack has occurred, and so you’ll go to that entity and say please share the information? How does that occur?

Mr. Joyce: What we found is that after an attack has occurred, we’re too late, right? We have to get left of theft. We have to be in a mode where we’re deterring, denying, and keeping the adversary out of these networks in advance. So that means we’ve got to have the partnerships and communication in advance.

One thing we do have the authority to do under the Department of Defense is help protect the defense industrial base, and that has given us the authority to be able to have relationships where we can take things we know in very sensitive channels, downgrade those, and then provide them without all of the sensitive activity around it, the things you talked about that might make personal information concerns, and provide those to the network owner and operator so they can take action before it even gets to those companies.

Senator Ernst: Thank you. I like that “left of theft.” That’s very good.

Let’s talk a little bit about constraints. Admiral, if you would, during his testimony General Nakasone also described how foreign hackers are exploiting the legal constraints which prevent U.S. intelligence agencies from monitoring this domestic infrastructure. So what authorities should this subcommittee and our committee consider to make sure that we are protecting the overall architecture now, and then as well moving into the future?

Admiral Chase: Thank you, Senator. For the DOD architecture, I believe we have the authorities. We are right now using the pilots that we have done in the past year, year-and-a-half, to take the insights from that and try to understand how we can accelerate this in an urgent way. With regard to NSA or cyber authorities, I’ll leave that to Mr. Joyce to build on or not. Maybe we’ve already covered most of that.

But I think from an internal perspective, we have the authorities to do things within the DOD networks, but it’s a question of time. Really what we’re talking about when we say zero trust is a large culture change that’s taken private companies when they do this many years. It will probably take us -- this is a journey. We’ve begun the first steps actually in the past, but we need to accelerate in order to get there as quickly as we can because our data and our assets are at risk.

Senator Ernst: Okay, thank you very much.

I apologize. I am way over time. I yield back. Thank you.

Senator Manchin: No problem at all.

Senator Blumenthal?

Senator Blumenthal: Thanks, Mr. Chairman. Thanks for having this hearing.

Thank you all for your service, and thanks for being here today.

I appreciate that the Department of Defense zero trust concept is a kind of holistic approach to security, and I noted that Mr. Joyce once said, and I’m quoting, “If you really want to protect your network, you really have to know your network,” which kind of makes sense. But it’s an important shift in mindset, and it’s a change in the way that Federal agencies have been doing business, and I have become alarmed that this very commonsense and important approach ought to be adopted elsewhere. Or, to put it differently, I’m alarmed that it hasn’t been adopted in other agencies, civilian agencies, of our government where cybersecurity is equally important, for example in the Department of Justice or the Department of Homeland Security, where confidential, secret information could be compromised and, in fact, may have been compromised in the Microsoft Exchange and SolarWinds hacking.

So my question, my first question is to what extent can civilian agencies make use of this model, and do you plan to share some of these lessons with those civilian agencies?

Mr. Joyce: Senator, thanks for the question. We absolutely will be sharing the lessons learned and the reference architecture of these models. NSA has been embarking on a zero trust pilot. We've worked with the elements in the DOD, like DISA and Cyber Command, to bring together the best in industry and to practice in an environment and find out what's real and what's vaporware, frankly.

From that we have published a number of our findings as to what the architecture looks like, and we will continue to put out, in the unclassified space, publicly available not only to the Department but also to other government agencies and even our commercial entities, our best practices and the things we've learned.

Senator Blumenthal: Talking about those commercial partners, are they required to be audited, be reviewed for their practices in dealing with you?

Mr. Joyce: It depends on what activity we're using them for, Senator. For the standard products? No, there is not a defined audit in the base of technologies. But as you get to more and more sensitive uses, we have requirements and standards for the software development practices and continue to learn from things, like the SolarWinds supply chain hack.

Senator Blumenthal: My understanding is that you've concluded that the Department of Defense was not compromised by either SolarWinds or Microsoft Exchange. Is that understanding correct?

Mr. McKeown: Senator, that's correct. For SolarWinds, we did an enumeration of the number of copies that we had in our environment, total, and those that were potentially compromisable. There were 560 that did have the back door. There was a total of 1,500 copies of SolarWinds. We looked through all of our sensors. We found no indications of compromise. In a few instances we sent out hunt teams to do a more thorough examination to make sure, and to date no compromise.

Same thing with the Microsoft. We quickly enumerated that, focusing on those servers that were public facing. There were very few that were, but we quickly patched those and found no indicators of compromise.

And if I could, sir, I would like to also add on to the discussion of sharing with industry about zero trust. We've actually learned a lot from industry on zero trust. There are a number of companies that were leveraging what they have done in the past, very significant efforts on the part of some of the companies that took them 10 years, their journey, to get to full zero trust implementation. But in these two instances what we found is the companies that came to the surface with all the indicators of compromise and uncovered the fact that we were being compromised, they were employing similar zero trust concepts in their networks. So we're learning from them, as well.

Senator Blumenthal: And just two quick final questions. Have you completed your review of the SolarWinds and Microsoft Exchange hacks?

Mr. McKeown: Well, the operations associated with them are still ongoing. We're keeping that open. We've been working with both vendors on the patches and deploying those. We have, I think, finished all of our work as far as hunting, going out there where we thought maybe compromise existed. We are certainly -- if somebody in the community comes up with more indicators of compromise, as soon as we get those we check it across the environment. So I would say it's going to be ongoing for some time in that regard.

Senator Blumenthal: Have you publicly confirmed your conclusions as to who was responsible for each of them? I think we've received that information through the press, but I'm wondering whether you can confirm in this setting.

Mr. McKeown: I don't think we can confirm that in this setting, sir. We can take that offline.

Senator Blumenthal: Thank you, Mr. Chairman.

Senator Manchin: Thank you, Senator.

Senator Blackburn?

Senator Blackburn: Thank you, Mr. Chairman. And thank you to our witnesses.

I have one question I want to go back to. Mr. Joyce, I think it was you. You said you all had the authorities that you needed within DOD to address the issues, the cybersecurity issues with networks. Tell me what else you would need working outside of DOD with some of our partners to address some of the challenges that were there. Are they the same or is there a difference?

Mr. Joyce: Senator, I would offer that there are a number of authorities that the U.S. Government can bring to bear on these cyber intrusions, and each of the departments and agencies have a critical lane and role to play in those authorities. So, for instance, the Department of Homeland Security and CISA have some exceptional capabilities to work with industry, and in their authorities they have the liability protections that are often needed for companies to feel safe. In FBI, they have the ability to go out and work with victims and through the Department of Justice go out and gather evidence under legal authorities inside the U.S. We at NSA have the ability to use the foreign intelligence capacity and capabilities of NSA to reach out and understand what's happening in foreign space directed at the U.S., or sometimes the plans and intentions and capabilities of those adversaries. And then you have folks like Cyber Command who are out there trying to actively contest some of the activities and push back. In the end, it's the fabric of that community that really gives us a number of capabilities.

So what we're constantly working on is what is the optimum strategy to take all of those authorities that we each possess and play them in a symphony orchestra instead of individual bands and make good music together.

Senator Blackburn: Yes, I appreciate that analogy. Being somebody from Nashville, we appreciate that. But how willingly do the different agencies share that information?

Mr. Joyce: I'll take that. The sharing is outstanding, Senator.

Senator Blackburn: Okay.

Mr. Joyce: We have made it our policy as we work with commercial companies, because sometimes we will have an initial relationship with a company, we make sure they understand when they're sharing with NSA that they're sharing with a government team.

Senator Blackburn: Okay. So you take a whole-of-government approach in sharing that information; correct?

Mr. Joyce: Yes, Senator. We have to, absolutely.

Senator Blackburn: Okay, that's great.

Now, let me ask you another question relative to Huawei. Admiral Chase, I think this is best directed at you. We've got Huawei gear that is proliferating in networks all across the globe. Some of our allies have stepped up and have dropped Huawei, especially in relation to 5G. So how can we look at a zero trust structure and still ensure that we can safely transfer information, sensitive information, or share information with our allies even when we know we have some embedded vulnerabilities in this Huawei architecture?

Admiral Chase: I think some of what you're talking about has to do with the infrastructure that we don't own.

Senator Blackburn: Correct.

Admiral Chase: In some cases this is very much -- we have to assume that is compromised. Do we have encryption that goes over the top of that? How we share that matters a lot, and we'll have to be careful with that. There are probably other insights from the IC that Mr. Joyce might be able to share progress on.

Mr. Joyce: Senator, with respect to Huawei, I think that highlights, combined with things we've learned like the SolarWinds hack, how important it is that we make sure that the supply chain involves technologies and vendors that we can trust. Are we willing to put them in the middle of our critical infrastructure and capabilities? And in the case of Huawei, there are situations where the Department knows that they're going to have to operate in foreign space, and those countries are going to be choosing to use that gear. So we have to provide the technologies and the understanding that can allow our forces, our diplomats, our government employees to be safe transiting those networks. But what we don't want to do is give them that advantage when we can choose not to.

Senator Blackburn: Okay. My time has expired. Admiral Chase, I've got a couple of questions relative to the Guard and some of their partnerships and U.S. Cyber Command, so I will submit those. And I thank you all for the time today.

Mr. Joyce: Thank you, Senator.

Senator Manchin: Thank you, Senator.

And now we have Senator Gillibrand via Webex.

Senator Gillibrand: Thank you, Mr. Chairman. I appreciate it very much.

I just want to continue along the line of questioning that we just had. I’ve seen mixed reporting on this issue. Are U.S. systems still susceptible to SolarWinds and Hafnium hacks? And will this attack end only after every system has been patched?

Mr. McKeown: If you did not patch any of the Hafnium vulnerabilities, I would say that you’re still susceptible. As far as SolarWinds goes, all of the capability to beacon out to their command and control system has been severed. So even if that is vulnerable at this time, it is unlikely that that attack would be successful. But definitely on the Hafnium, patching needs to continue.

Senator Gillibrand: What kind of personnel would be needed to develop, maintain, and enforce your trust architecture, and how might their experience, their skill, and other elements of their background be distinct from other subdivisions of cyber personnel?

Mr. McKeown: Good question, Senator. We don’t feel like we have to create a zero trust workforce. What we need to do, as we discussed earlier, many of the things that are components of zero trust we’re already doing. We just need to round out the portfolio of all the capabilities and train our existing cyber defenders and hunt teams on those new capabilities.

Senator Gillibrand: And is this consistent with our current recruitment strategies across the national security enterprise?

Mr. McKeown: Absolutely.

Senator Gillibrand: And, as we’re all aware, many elements of our space operations rely heavily on our cyber capabilities, and vice versa. Can you speak to what initial training is required for our cyber personnel who deal with space operations and how their roles or training may change when applying zero trust principles?

Mr. McKeown: Senator, I can’t speak specifically to what that will look like for the space operations folks, but these principles that we’re employing here can be transferred to any platform, any IT platform that you may think of. So in terms of space systems, which are heavily reliant on IT, we can definitely employ these same pillars of zero trust and employ the same architecture.

So we would seek to train them in the same way as I spoke of earlier with our existing IT technicians, just rounding out their capabilities and working with their architects as well so that they understand the principles of zero trust so that when they design a new system, they built it in.

Senator Gillibrand: If the Department of Defense was able to frustrate the SolarWinds and Microsoft Exchange attacks, why is zero trust so important? And what capabilities in place across the DOD allowed it to frustrate the SolarWinds and Microsoft Exchange attacks?

Mr. Joyce: Senator, I think we should be very proud that we weren't the victims of that exploitation, and it is because of the efforts the Department has made over the last several years to increase the agility and responsiveness of the operators inside the networks.

A few things have been done. The consolidation of the capabilities to defend the DODIN gave us what is a huge advantage in speed to be able to order the modification and protection changes necessary for any specific threat. It also gave a hierarchy to report back the state of activities. So, for instance, when there's a vulnerability in Microsoft Exchange, there can be a cascaded order to go down to say issue the patch and run these checks to find out if you're exploited and report back up. So, as Senator Blumenthal relayed earlier, you have to know your network to defend your network, and the changes the Department has been making in the DODIN under the DODIN Command and Cyber Command is they have really upped the bar in the ability to know the network, which directly translates to the ability to keep people out.

Senator Gillibrand: For Mr. Joyce, let me just -- I only have a couple of minutes left. DOD and the NSA developed strategies as recommended by the National Institute of Standards and Technology for migrating to zero trust architecture, and one of the major challenges facing the Department and the NSA in moving to a zero trust architecture. Do DOD and NSA have plans to address these challenges?

Mr. Joyce: Yes, Senator, absolutely. The coalition looking at zero trust includes our NIST partners, folks across the Department and, as Mr. McKeown indicated, the best practices of industry. The biggest challenge, quite frankly, in the Department is the scope and scale of the amount of change that has to happen. There is an enormous amount of networks, devices, and legacy equipment, and if you’re going to design something from scratch and whole cloth, the zero trust transition is very easy. If you’ve got to go through and make sure you have a smooth migration, it’s a harder problem. But the thing I would ask you to take away is the journey to zero trust in and of itself will improve the Department’s ability to defend itself all the way along the way. So we don’t have to get all the way to zero trust to reap the benefits.

Senator Gillibrand: Thank you, Mr. Chairman.

Senator Manchin: Thank you, Senator.

And now we have Senator Rosen via Webex.

Senator Rosen: Thank you, Mr. Chairman, appreciate it. Thank you to all the witnesses for being here.

I really want to build upon what Senator Gillibrand is talking about with zero trust architecture and really the role of artificial intelligence and what that may play in this. Of course, the National Security Commission on Artificial Intelligence released its final report earlier this year and highlighted the risks of the United States failing to compete in the AI era. The final report presents strategies to defend against AI threats by responsibly deploying AI for national security and win in the broader technology competition.

When it comes to network security, of course, something we’re all always interested in and that is particularly timely, AI can absolutely detect behavior patterns and help us understand how, when, and what users interact on the network. For example, deviations from normal network behavior could indicate malicious activity.

So to Admiral Chase and then Mr. McKeown, how are we going to use -- and I don’t even want to say emerging technology anymore, because AI and machine learning are here, they are becoming more robust every day. How can they support and potentiate DOD’s zero trust architecture?

Admiral Chase: Thank you, Senator, for the question. We can’t just begin with AI as part of the problem. We need to back that up a little bit and do the machine learning that precedes that, the automation that precedes that, and then either data aggregation or federating the things that we want to know about; in other words, the users, the devices, the resources accessed, and bring those to bear. But those also have to have access controls built in. So that’s where the scope and scale is probably going to be difficult for an organization the size of DOD that has all those things already in play. The work is going to have to be federated. We can put broad rules in policy in terms of how we want to go do this, and CIO will certainly be able to lead that aspect.

But getting our arms around all the things that we do have, as I said, the journey is not one that we’re starting on today, but fortunately we began a few years earlier to get after the insights that we need now that we can see more of the network than we ever could. Now is a great time to start classifying the sorts of decisions that we want to make with that information, bringing the automation, the machine learning, and the AI to bear exactly as you described, Senator.

Senator Rosen: Thank you. Does anyone else want to weigh in on this?

Mr. McKeown: Senator Rosen, AI is a critical component not only of zero trust but the DOD is treating it as a critical capability across the board as far as IT goes. And we’re making significant investments in it. I don’t think we’re behind. We recognize we’re in an arms race there, and we are definitely putting resources against this. We are cooperating on the cybersecurity side with elements that have been stood up within the DOD specifically to move us ahead in the AI domain. So we'll be continuing to partner with them and looking for capabilities that can help us.

As the easy attacks are taken away from the enemy, they're going to get more and more sophisticated, and we're definitely going to need AI to rout out these new attacks and tell us what the indicators of compromise look like.

Senator Rosen: Well, thank you. That really set me up for my next question for both of you gentlemen, as well. The DOD contracts, of course, work with commercial entities, specifically the ones related to AI. I want to know, first of all, are we subjecting them to vulnerability reviews? And secondly, you talk about scope and scale. How does IT modernization generally, across the government, not just in DOD but across the whole spectrum of government, how is our investment in IT modernization going to make a difference for our improving or reducing the risk of vulnerability?

Admiral Chase first, then Mr. McKeown.

Admiral Chase: Thank you, Senator. First, just from the impact that that will have, we'll be able to take the talent that we already have, automate the more mundane tasks, and be able to use our everyday force that looks at access control, configuration management, and better be able to posture should this be happening. If so, great. If not, why not? How do we reconfigure the network on the fly, be more agile and pivot things to the IC or the hunt teams that need to be looked at, that are essentially other nations or cybercrime that has managed to penetrate our network? So I think it will enable the reapportionment of the workforce that we do have, to the earlier question about how do we use these things. If we can offload the scope and scale problems through automation and AI, we’ll be better able to repurpose our people.

Senator Rosen: And, Mr. McKeown, any thoughts in my remaining few seconds?

Mr. McKeown: Yes, Senator. As we do modernize our environment, we focus on data as a big pillar, AI as a big pillar. We are definitely looking at the supply chain and the risk that it brings both from a hardware and a software perspective, and we do have some very good partnerships with industry now that are illuminating issues many tiers deep in supply chain, and that’s allowing us to make better decisions about what we acquire and where those devices are allowed to go on our networks.

As far as the software piece of it goes, we have been working with the National Security Council on a whole-of-government effort to examine a gold standard for software development so that we can have better trust that the software that we’re receiving from our suppliers is more secure.

Senator Rosen: Thank you.

My time has expired. Thank you, Mr. Chairman.

Senator Manchin: I want to thank you all.

I have one follow-up question, if I may, and then I think, Mr. McKeown, it might be best for you, but for whoever could help me with this, I’d appreciate it.

We’re all aware of how destabilizing cyber capabilities can be, and that makes them extremely valuable, especially when you consider the minimum investment required to conduct offensive cyber operations. Protecting against cyber attacks is a much more difficult process. With every piece of equipment, personnel, and network, there is potential vulnerability. It’s our job to ensure that we’re investing the resources into the proper programs to maximize our defensive and offensive capabilities.

You stated that an identity, credential, and access management system, or ICAM, is critical to zero trust because we have to constantly verify the identity and the access privileges of every sector of the network.

So with that being said, have we budgeted for that, and are we acquiring that or moving in that direction?

Mr. McKeown: Chairman Manchin, yes, we have budgeted for that. Right now we have a solution, an enterprise-level solution for ICAM that has been developed by the Defense Information Systems Agency. We're currently on-boarding most of the financial systems in the Department onto that. We believe that that will be the exemplar that we adopt across the board throughout the Department. We're planning on making that a fee-for-service, that as they divest of their current authentication mechanisms, that they will on-board to this capability across the Department.

Senator Manchin: Thank you.

Anybody else have anything you want to say before we finish up?

[No response.]

Senator Manchin: Let me just thank you all again. It's been great, and it's been very informative, and we appreciate your expertise and your service to our country. Thank you again.

And with that, we are adjourned.

[Whereupon, at 3:30 p.m., the hearing was adjourned.]