Stenographic Transcript
Before the

Subcommittee on Cybersecurity

COMMITTEE ON
ARMED SERVICES

UNITED STATES SENATE

HEARING TO RECEIVE TESTIMONY ON
THE CYBERSECURITY
OF THE DEFENSE INDUSTRIAL BASE

Tuesday, May 18, 2021

Washington, D.C.

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

HEARING TO RECEIVE TESTIMONY ON THE CYBERSECURITY OF THE DEFENSE INDUSTRIAL BASE

Tuesday, May 18, 2021

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

The subcommittee met, pursuant to notice, at 2:28 p.m. in Room SR-222, Russell Senate Office Building, Hon. Joe Manchin III, chairman of the subcommittee, presiding.

Subcommittee members present: Senators Manchin [presiding], Gillibrand, Blumenthal, Rosen, Rounds, Wicker, Ernst, and Blackburn.

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

Senator Manchin: We are going to welcome our members and our two witnesses and I have called this hearing to update the subcommittee on the Department of Defense's efforts to improve the cybersecurity of the Defense Industrial Base.

The Defense Industrial Base cybersecurity is a broad and complex undertaking with many significant facets that need to be examined today; for instance, the Cybersecurity Maturity Model Certification, or the CMMC for short, is intended to establish a minimum guideline for DOD's industrial base partners as to what standards must be met to conduct business with the DOD or Section 1648 of the fiscal year 2020 NDAA, they direct the DOD to establish a framework for the cybersecurity of the Defense Industrial Base which included numerous elements and options for the Department, beyond just the CMMC initiative.

In addition to Section 1648, this subcommittee has enacted a dozen or more legislative provisions relating to the industrial base cybersecurity in the last several years, including recommendations from the Cyberspace Solarium Commission. Of particular interest to me is how DOD is going to hold prime contractors for the cybersecurity performance of their subcontractors in the conduct of the

programs for the DOD. I have been making this point for a couple of years now and I hope the Department has taken this to heart.

But in order to build out our cybersecurity protection with the Defense Industrial Base, we must set a baseline of standards with the CMMC initiative. Previously, DOD required that companies executing Defense contracts implement a series of control and cyber hygiene practices developed by the National Institute for Standards and Technology. Companies were required to certify that they met the standards or to present a plan of action that would bring them into compliance.

Because this program involved self-certification, compliance would suspect and that lack of verified compliance that DOD to propose a CMMC model. To perform contract for DOD, contract work for DOD, a company would have to meet one of the five specified security maturity levels and receive a certification to that effect.

DOD has issued a so-called interim rule under the Defense Federal Acquisition Regulation Process and is beginning a series of pilot programs to test and implement CMMC. CMMC is intended to be financially self-sustaining with companies paying for their assessments and certifications, and those companies then recouping compliance costs as part of their cost estimates to the DOD.

Industrial-based companies, especially smaller contractors, are very concerned about the costs involved in regular on-site assessments, the complexity of complying with cybersecurity practices that they have difficulty understanding and the degree of consistency and fairness in assessing compliance across the expected large number of assessing organizations and many tens of thousands of other companies.

In response to those concerns, Deputy Secretary Hicks, in March, directed an independent review of CMMC. That review was intended to last about a month. We postponed a scheduled subcommittee hearing in April in the hope that we would know the results of this view on this date, May 18. Unfortunately, we have not received the details of the review today. While the review itself is complete, the review team's recommendations are still being finalized and the review is officially connected to internal deliberations and modifications to the interim rule on CMMC.

We do understand, however, that Secretary Hicks will be significant modifications to the program. I hope that what we hear today will be welcome to Congress and the Defense Industrial Base, particularly, our small businesses. In addition to your updates on this CMMC review, I hope to hear concrete plans for how each of you plan to ensure our entire Defense Industrial Base receives the support and guidance

they need to keep our warfighters well supplied and safe.

The relationship between DOD and its private industry contractors should be the gold standard for cybersecurity across the federal government and provide an example to other federal agencies who secure private critical infrastructure. I know this hearing is focused on Defense Industrial Base today, but improving cyber defense is only one side of the coin in our cyber posture.

From the quarterly updates the subcommittee receives on cyber operations, it appears to me that DOD is doing an excellent job at taking the fight to our adversaries, but what concerns me is our inability to know exactly what groups are posing a threat to industry so that we can adequately monitor, intercept, and if required, target them. I make this point because I am worried about the lack of a formalized and concerted whole-of-government response to both, foreign and domestic cyber threats and the lack of authority in a central figure to give these threats the attention they deserve.

The Colonial Pipeline hack is only a recent public example of the threats we face on a daily basis. In order to increase our federal coordination, and I know this is not a perfect comparison, I look at the examples set by a position such as the Director of National Intelligence, which has crucial awareness and the opportunity to

coordinate the intelligence efforts of 17 independent agencies. We have yet to see how successful the national cyber director will be in their role, but it seems to me that each department in the federal government must reinvent the wheel every time a cyber event happens, which costs us time that we could be using to respond, let alone the ability to be aware of the threat before its impacts are critical to our infrastructure.

I am well aware that this falls a bit out of the jurisdiction of this subcommittee, but it is imperative that we are coordinating as seamlessly as possible with private industry, and I believe DOD is on the way to developing a scalable model for that coordination.

I look forward to working with my colleagues to identify a pathway forward to provide better congressional oversight on a whole-of-government approach on our cyber vulnerabilities.

With that, I am going to ask my friend Senator Rounds for his opening statement.

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

Senator Rounds: Senator Manchin, thank you.

I would also like to thank our witnesses, Mr. Jesse Salazar and Rear Admiral William Chase, for appearing before us today to discuss this important topic.

Our hearing today addresses an issue of great concern to me that our subcommittee has been focusing on for the last several years: the cybersecurity of the Defense Industrial Base. Over the last few years, our subcommittee has held several hearings on this topic and we have included many legislative provisions in both, the fiscal year 2020 and fiscal year 2021, National Defense Authorization Acts.

We have heard from the Defense Industrial Base and outside experts who presented a number of concerns that they had with the Department policy. Two years ago on April 10, 2019, the subcommittee held a classified hearing with the Department of Defense witnesses on Defense Industrial Base cybersecurity policy. Unfortunately, we still face many of the same problems today that we faced back then.

In looking back at my opening remarks from that hearing, many of the comments I made are still very much relevant to today's hearings, so I will reiterate those comments in my public statement here today. I think you will find that they mirror what Senator Manchin has

indicated earlier.

Our adversaries have realized that targeting the vulnerable contract base is an extremely profitable enterprise and an alternate method to accessing valuable Department of Defense information. As a result, Russia and China are stealing critical design secrets effectively subsidizing their own defense involvement.

Over the last few years, we have arrived at a few conclusions. First, this is an immensely complex issue that will require a number of small solutions, implemented by a number of different entities across the Department and the Defense Industrial Base. Second, verifying compliance with a security checklist or certification, like the Cybersecurity Maturity Model Certification, or CMMC, being developed by the Department of Defense, while useful, is not a complete solution to the problem.

I am concerned that this approach does little to help businesses meet those standards and certification. It does not account for the particulars of the threat and does not help businesses prioritize personnel or investments.

Third, the Defense Industrial Base must help smaller businesses with the protection of DOD data from malicious cyber actors. The Department cannot simply burden its contractors with increasingly stringent cybersecurity requirements. Doing so, without subsidy or assistance, is

unlikely to particularly improve the cybersecurity of the Defense Industrial Base and will likely drive the most innovative small businesses away from doing business with the Department.

Finally, any solution must emphasize reducing the attack surface of these companies. I see no reason why, for example, smaller contractors at the base of the supply chain, have substantial amounts of classified or control unclassified data about the larger program. We need to look at implementing concepts that reduce the most common cybersecurity risks and attack vectors.

The fiscal year 2020 NDAA included a comprehensive provision that we led, requiring the Department to develop a Defense Industrial Base cybersecurity framework that includes a wide-ranging set of elements, beyond just CMMC.

I look forward hearing today what the Department is doing to address each of those required elements. I am eager to hear from each of you about the Department's efforts in this area and encourage you to discuss the Department's current and planned efforts. I also am interested in hearing what Congress, this subcommittee in particular, can do to help in these efforts.

Thank you for your willingness to testify today. I look forward to our conversation.

Senator Manchin: Thank you, Senator Rounds.

I will now introduce our witnesses. First, we have, joined today by Mr. Jesse Salazar, who, about 3 months ago, was appointed to so I have as the Deputy Assistant Secretary of Defense for Industrial Policy within the office of the Under Secretary of Defense for acquisition and sustainment. This is Mr. Salazar's first visit to Armed Services Committee, so welcome, Mr. Salazar.

Our other witness is Rear Admiral William Chase, who was recently promoted to two-star rank. Congratulations. Admiral Chase serves as the Deputy Principal Cyber Advisor to the Secretary of Defense and Director of Protecting Critical Technology Task Force. Admiral Chase has testified before the committee multiple times on cybersecurity.

I want to thank both of you for appearing today and for your service to our nation. Mr. Salazar, we will begin with your opening statement.

STATEMNENT OF JESSE SALAZAR, DEPUTY ASSISTANT SECRETARY OF DEFENSE FOR INDUSTRIAL POLICY

Mr. Salazar: Chairman Manchin, Ranking Member Rounds, thank you for the opportunity to testify on the importance of mitigating cybersecurity risk within America's defense industrial base, or DIB.

Because of its sophistication, diversity, and a capacity to innovate for warfighter, the U.S. Defense Industrial Base remains the envy of the world. Every day, people across this country are designing and manufacturing the capabilities that ensure our armed forces have every advantage they need. We must do everything we can to protect these hard-working, entrepreneurial companies and workers.

Increasingly sophisticated cyberattacks, including state-sponsored espionage are threatening the U.S. and the rules-based economic order. That is why DIB cybersecurity is and will remain a top priority for U.S. defense industrial policy. I consider this committee to be a critical partner in these efforts.

Recent examples of malicious cyber activity such as the Colonial Pipeline ransomware attack and SolarWinds espionage campaign have shown that our adversaries continue evolving. The complexity and size of the DIB offers numerous pathways for adversaries for access sensitive systems and

information.

We are in the dawn of the fourth industrial revolution, which will create more than 64 billion IOT devices by 2025. Today, the average American aerospace company has more than 12,000 companies in its supply chain, most of which are small businesses.

Having spent my career in the private sector, I can attest that these small businesses work hard to stay profitable. Few have a full-time IT or cybersecurity professional on staff, increasing the likelihood that predatory cyber actors will target them.

Enabled by recent legislation from Congress, the DOD has designed a multifaceted cybersecurity framework to frustrate, disrupt, and defeat adversaries' efforts to infiltrate DIB companies. I recently assumed oversight of one component of this expansive effort, the Cybersecurity Maturity Model Certification program, which incorporates cybersecurity into the Defense Acquisition System.

The CMMC framework has three broad objectives. The first, to incorporate a unified set of cybersecurity requirements into acquisition processes and contracting language. Second, to hold primes accountable and provide the Department assurance, via external assessment, that contractors and subcontractors meet DOD's security requirements. And, third, to support businesses with

resources, information, and training to improve DIB cyber readiness.

CMMC represents a major leap forward in the Department's approach to cybersecurity and underscores our commitment to accountability in the DIB. That is why we published an interim DFARS rule establishing CMMC in November 2020. The Department has received more than 850 comments in response; in addition, my A.N.S. colleagues have hosted more than a thousand conversations on cybersecurity with Congress, DIB companies, industrial associations, international partners, and allies.

I am grateful to the organizations and individuals who gave such a high volume of feedback on the regulatory and programmatic way forward. In March, A.N.S., under the direction of Deputy Secretary Hicks, initiated an internal assessment of the CMMC, which is common for major programs to help us refine our policy and program implementation.

I want to underscore with this subcommittee that this we are listening to the feedback we are receiving on the CMMC program. The rule-making process around programs such as this typically takes a year. As we adjudicate inputs in the months ahead, the Department is guided by the following policy considerations. First, we are really focused on managing costs of cybersecurity for small businesses.

In my role, I also oversee the Office of Small Business

Programs, so I can say with certainty that small businesses are under immense market pressures. The number of DIB small businesses has shrunk by more than 40 percent over the last decade. After the pandemic, one in seven small businesses within the DIB says that they are unlikely to return to pre-pandemic profitability.

Second, we aim to clarify cybersecurity regulatory policy and contracting requirements. The Department's requirements are complex and challenging to navigate. We want to de-conflict and streamline them to add clarity.

And our third consideration is that we will reenforce trust and confidence in the maturing CMMC assessment ecosystem. The Department is ensuring that we can operationalize our requirements through a sufficient number of assessors. The DOD must also clearly define roles and responsibilities, standards of conduct, and audit mechanisms within the external assessment ecosystem.

And, finally, the DOD is exploring initiatives complementary to CMMC that expand and increase the DIB's access to cyberthreat information sharing programs, cybersecurity as a service program, such as protective DNS, and education and training programs. We seek great value and resources to help small businesses improve their cyber readiness.

Ultimately, the Department's goal is to ensure that the

DIB embeds cybersecurity into core operational and business practices to build a culture of cybersecurity that keeps pace with rapidly evolving threats. Cyberspace has never been more important than it is today. The United States of America does not get dissuaded by the perseverances of the challenges we face; we always rise to meet any and all threats to the nation. Thank you for your time and I look forward to your questions.

[The statement of Mr. Salazar follows:]

Senator Manchin: Admiral?

STATEMENT OF REAR ADMIRAL WILLIAM CHASE III, DEPUTY PRINCIPAL CYBER ADVISOR TO THE SECRETARY OF DEFENSE, DIRECTOR OF PROTECTING CRITICAL TECHNOLOGY TASK FORCE

Admiral Chase: Thank you, Chairman Manchin, Ranking Member Rounds. Thank you, again, to your invitation to appear, again, before this subcommittee.

I am here today as the Deputy Principal Cyber Advisor to Secretary of Defense representing my civilian senior, the acting principal cyber advisor, who is responsible for driving implementation of the DOD's cyber strategy, oversight of U.S. Cyber Command, manning, training, and equipping issues, and pursuant to Section 1724 of the fiscal year 2021 NDAA, serving as the coordinating authority for the Defense Industrial Base cybersecurity.

My remarks today reflect two complementary imperatives: first, the need to improve the Defense Industrial Base's cybersecurity across the board from small to large and also its scale, and the need to focus protection resources on programs of particular importance.

Neither the Department, nor the Defense Industrial Base may never be able to completely secure industry's networks and controlled information, but our goal must be to complicate and frustrate adversary planning and operations, such that they cannot conduct them with impunity or at scale. To accomplish this objective and address these

imperatives, the Department is taking a multifaceted approach, including holding Defense Industrial Base companies accountable to cybersecurity requirements, rapidly moving out on activities to systematically disrupt cybersecurity espionage and sabotage through partnerships with cybersecurity, IT, and internet communications companies, prioritize and expanding information sharing, exploring direct provisioning of cybersecurity capabilities, and on focused counterintelligence and program protection efforts.

Jesse Salazar spoke to the Cybersecurity Maturity Model Certification program. I will focus on some of the other Defense-wide and pilot efforts that the Department is undertaking, many of which are referenced in Section 1648 of the 2020 NDAA, which laid out a set of potential programs for the Department to implement to protect the Defense Industrial Base.

On partnerships and information sharing, the Department is exploring means to disrupt adversary espionage by leveraging the unique information available to the Government and the Defense Industrial Base, specifically, the Department is working, ensuring threat data with major service providers across the cybersecurity, IT, and internet industries to help these companies detect and disrupt cyber activities before they reach the Defense Industrial Base

networks.

This approach, by bolstering the core services and internet intermediaries will add a layer of protection, not only to the Defense Industrial Base, but to the broader customer base, the American people. The Defense Cyber Crimes Centers threat sharing program, which focuses on Defense Industrial Base companies is also currently under expansion. While this program was originally designed to share indicators of compromise and malware analysis services with clear Defense contractors, meaning those members of the industrial base that have security clearances and access to classified information, the Department of Defense CIO is working to amend relevant regulations so as to allow inclusion of non-cleared Defense contractors, enabling small- and immediate-sized companies to receive the same signatures, indicators of malign IP addresses and threat advisories that the larger, cleared primes receive as part of the program.

The Defense Cyber Crime Center is also expanding other services available to the DIB piloting efforts such as penetration testing to address contractor's external-facing vulnerabilities, as well as about adversary emulation program.

The National Security Agency is conducting a number of pilot, leveraging their authorities to share unique,

actionable threat information and cybersecurity guidance with the members of the DIB and their service providers and to provide unique cybersecurity capabilities to the DIB, among the most promising of which is the provision of free and secured domain system lookup services to the DIB. Domain name systems is colloquially referred to as the phone book of the internet, translating readily remembered website names to IP addresses, appropriate for internet routing.

The NSA is offering a cybersecurity service called protective DNS, or PDNS, in partnership with an advanced commercial DNS provider and is currently enrolling members of its industrial base. This capability combines a commercial DNS sensor architecture with real time analytics to quickly understand malicious activity targeting the DIB and to deploy immediate countermeasures.

Not all of these technical concepts demand the Defense Cyber Crime Center, NSA, or Government providing such services. The primes, through the Defense Industrial Base Sector Coordinating Council, are also piloting a number of concepts that could be applied across their supply chains, including the provisioning the secure messaging, secure cloud environments, and sensors for subcontractor networks.

We must continue to pilot these concepts of operation and capabilities and then scale the successful ones. The direct provisioning of cybersecurity capabilities to

contractors, including the provision of secure environments for development and the storage of controlled, unclassified information is incredibly promising.

The Department of Defense counterintelligence community, specifically, the Defense Counterintelligence Security Agency, and the military Department counterintelligence organizations are also making significant progress in reducing cyber threats to the DIB. Each entity is growing and improving its programs and posturing to counter cyber threat, proactively detect adversary cyber activities and working with partners in the IC to address intelligence gaps, integrating law enforcement, and counterintelligence situational awareness and operations.

I am particularly impressed by the growth of the Defense Counterintelligence Security Agency, which not only runs the National Industrial Security Program, that ensures physical and cybersecurity of our clear defense contractors, but also is leading programs in cyber counterintelligence and supply chain risk identification, including data analysis programs that provide impressive visibility of adversary cyber operations.

Progress in the Defense Industrial Base cybersecurity is also being driven through program protection efforts and from acquisition program offices in industry. The

Department the currently refining its supply chain risk management and program protection efforts, including leverage available to program managers to shape prime and subcontractor behavior in protecting their programs. The prime contractors, in addition to conducting the pilots mentioned earlier, have been key partners in reenforcing their own supply chain security programs, standing up resources, such as secured messaging, and making them available to their subcontractors.

The Department relies on the primes to ensure the sanctity and operational security of critical information germane to its programs through close coordination, cyber conscious program management, and the establishment of appropriate incentives.

Thank you for providing me the opportunity to testify before you today and we look forward to your questions.

[The statement of Admiral Chase follows:]

Senator Manchin: Thank you, Admiral Chase.

Now we will start our questions. Mr. Salazar, you have been in your position for only a few months, but expect you are aware of my longstanding interest and that of the subcommittee in seeing DOD hold prime contractors responsible and accountable for ensuring that their subcontractors are protecting DOD technology and confidential information. My reason for that is we understand that most of our sabotage is done through the backdoor of the smaller subcontractors and going in from that end.

So, my question, what does the Department currently do to hold prime contractors accountable for the cybersecurity of their subcontractors?

Mr. Salazar: Thank you, Senator.

The Department should never shy away from requiring contractors to safeguard the information that we entrust to them and, in turn, if they are going to subcontract with other companies, they should be sure that they have the same assurances that they have given to us. We hold them accountable through our contracts and we have a number of ways to ensure that they are meeting those responsibilities, like performance reviews and contract actions.

The essence of the CMMC model is that primes have a special place in the Defense ecosystem that involves helping

others to mature their capabilities and we have been impressed by the way in which a number of the primes have lent their expertise to our efforts, shared information through my office through the Office of Small Business Programs. We have a program called the Mentor Protege where the primes actually coach the subcontractors and small businesses in the responsibilities of handling this kind of information. And, similarly, we have a new platform called Project Spectrum where primes are sharing what they know in real time with small businesses that could be 5 people or it could be 50 employees.

Senator Manchin: Yeah, but let me ask you this, the primes right now, is there any penalty or any fines or any cost or reprisal of losing, maybe their contract, if they don't secure? Are you making the primes secure that the subcontractors or subprimes are being protected hardened?

Mr. Salazar: Yes, Senator. Through our contracts process, through our requirements process. I have had a number of --

Senator Manchin: They have to prove to you that their subs are secured? Do you all go into it in that depth?

Mr. Salazar: So, when we entrust specific types of information of a national security interest to the primes, we also require that they mark and identify that information and that they ensure that the subcontractors are trained and

capable of handling that information.

Senator Manchin: But if you find out they haven't done it, what is the penalty? If you find out they haven't done it, do they lose --

Mr. Salazar: We have a number of possible answers. Usually, the PMO office will identify the opportunity to improve. We will also hold them accountable through the contracts and we can use a number of acquisition levers to --

Senator Manchin: Do you know if that has ever been enforced or implemented? Well, you have only been there a couple of months.

Mr. Salazar: I would have to take that for the record and see what recent actions there are.

Senator Manchin: If you could get back to me on that once you get your feet wet a little bit more and find out to my staff and find out if they have implemented any type of actions against them. We are finding out that doesn't happen.

But, anyway, Admiral, if you would, several provisions of the fiscal year 2021 NDAA are directly pertinent to this hearing and involve the principal cyber advisor, for whom you work. So, my question, Section 1724, designated the principal cyber advisor to be responsible for coordinating DOD and DIB cybersecurity efforts.

How are you finding that role?

Admiral Chase: Sir, as the deputy principal cyber advisor, this is a working group I host regularly as one of our lines of effort in partnership. We have had two of these meetings at the flag level to understand all the stakeholder roles and responsibilities. These include also some of, and one of my other hats as protecting critical technologies task force, making sure that we understand all of the objectives that that entity and task force has been stood up to exercise to include protecting the critical programs and technologies list, making sure we understand where those efforts are specific. That list has been tiered and looking to be more granular in order to provide a smaller attack surface for the broader DIB.

Senator Manchin: If you could answer this, this is two parts. Section 1736, okay, I will go over it with you. 1736, the director of the principal cyber advisor assesses the feasibility of working with the DIB to place sense source inside and outside DIB companies to help detect intrusion compromises.

So, on that one there, if you could answer that, is this work now underway that you know of?

Admiral Chase: Yes, sir, it.

Senator Manchin: It is.

Section 1737 requires DOD to assess the practicality of

a comprehensive threat intelligence sharing program with DIB companies. What is the status of that program?

Admiral Chase: That one is also, we have several efforts that have been piloted. The adversary emulation is one of those. Another is called, this is through the Defense Cyber Crime Center, another called Crystal Ball, which is an outside looking in. They have partnered with, to identify the vulnerabilities and threats inbound, and those were used to identify and notify 13 DIB partners of a Chinese malicious actors, attacks on the Microsoft Exchange server vulnerabilities. On the previous adversary emulation, that one was also used in this effort. DIB vulnerability program disclosures, that is a 12-month pilot that is ongoing to help with, broadly, the cyber hygiene. And then looking to expand these into non-cleared pilots for the non-cleared actors to go from 800 clear Defense contractors up to the broader DIB, overall.

Senator Manchin: Thank you.

Senator Rounds?

Senator Rounds: Thank you, Mr. Chairman.

Mr. Salazar, recognizing that you have only been on the job for a few months, I am not going to burden you with a lot of the questions on this, and I mean no disrespect, but I think will focus on the Admiral.

Admiral Chase, let's start by talking about

communications and the availability. If there is an incursion by an outside source into one of our contractors, are they required to report the incursion if it is on a project that isn't DOD-oriented?

Admiral Chase: Yeah, there are mandatory reporting criteria that the DIB contractors have to report to the defense cybercrime entity. In things like SolarWinds, the Department specifically asked for the number of intrusions and reports that we had on that. I believe we had 37 companies that reported specific, 44 different reports.

Senator Rounds: So, if it is a private entity and they are doing DOD contract work and there is a discovered security leak through cyber means, they do have to report today to the appropriate office within DOD?

Admiral Chase: Yes, sir. There is mandatory reporting criteria and then there is voluntary reporting is certainly encouraged for attempted attacks, not necessarily successful, but we welcome those. We believe that we will get their faster if we can get to voluntary reporting, which should really be led by information sharing of the threat. And so, the partnerships with industry really go much farther when the Government has something to share, timely, relevant, threat-intelligence information, malicious signatures, things that we can put into virus total, using our unique insights through NSA, CYBERCOM's hunt forward

operations that generate insights, et cetera.

Senator Rounds: That is the part that I wanted to follow-up with. Once there is a notification of an incursion or a leak and it has been reported to the Department of Defense, what happens in terms of trying to stop it from happening again or assisting that contractor in dealing with it, which office is responsible for that?

Admiral Chase: The Defense Cyber Crime Center is the first point of report and that will get sent out to law enforcement officials, as well. The counterintelligence community would be brought to bear from the Department's standpoint, but largely, that is viewed as a private crime until such time as we give more.

Senator Rounds: You have been there long enough to where you have seen this occur already, fair statement?

Admiral Chase: Fair statement.

Senator Rounds: Okay. Let's take a look at an organization now such as what just happened with the pipeline. Granted, not in this particular case, I am assuming that it is not a DOD contractor. In this particular case, there is no evidence that they reported this to anyone, they are a private entity, and, you know, at the same time, it has a national consequence to it.

Is there, at some point, the need in order to address this type of an issue, the need for some sort of a

communication or an expectation of a communication between a private business and either Homeland Security, the Department of Justice, the FBI, and thus back into the appropriate level at the Department of Defense, who really is the only source who can work outside of the United States to try to stop the attack from happening in the future. I ask it only because your role is not just with regard to the Defense Industrial Base, but because you also carry the titles of 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 and the Director of Protecting Critical Technology Task Force.

I am looking for advice.

Admiral Chase: So, Senator, malicious cyber campaigns absolutely threaten the public sector, the private sector, and individuals. So, we, the Federal Government, have to improve our own cybersecurity and this is of critical importance, but it does extend down all the way to the private sector and we have to do that on premises, on cloud, IT systems, or operational technology systems like you see in the pipeline attack. We have to do this and the Government Government's undertaking Zero Trust is a best practice for cybersecurity. We are clearly in the latest executive order on improving the Nation's cybersecurity. These things are all called out as we need standards of

these across the Federal Government.

Senator Rounds: And I appreciate the comments, but I think what we are talking here is we have silos. We have silos between the different agencies and those silos need to be coordinated; in other words, at some point, we need to recognize that we need to, at a national level, coordinate between Homeland Security, the Department of Justice, specifically, the FBI, and the Department of Defense, if we are going to have a coordinated effort to not just defend, but then to go out and then to stop these attacks from occurring again in the future. And it is not just within DOD, but it is a matter of on the national level coordinating all of the different, very capable entities that make up our cybersecurity defense within the nation to protect those individuals who may not be subcontractors or contractors to the Department of Defense, but who I suspect would most certainly appreciate the ability to appreciate and benefit from the capabilities that the Department of Defense has in stopping the attacks in the future. So, that is the reason for my --

Admiral Chase: No, Senator, I think you bring up a great point. We need to remove barriers to information sharing to dispel all of those silos. That probably does need to start with the threat, because in the world of cybersecurity, if you don't have the threat information, the

best you ever do is break even. So, we should start there, making sure we that we can get some tipping and queueing and bring the whole DIB up.

Senator Rounds: Thank you.

Thank you, Mr. Chairman.

Senator Manchin: Senator Gillibrand, via Webex.

Senator Gillibrand: Thank you, Mr. Chairman.

Let's start with Admiral Chase. Okay. As you know, DOD's announcement to move towards Zero Trust policy not only applies to cybersecurity but also to buying microelectronics and other national security essentials technology. The shift towards Zero Trust policy will be demanding and the volume of microelectronics required security measures is outpacing that shift.

How do we ensure that the pace of Zero Trust implementation matches the pace of the growth with microelectronics?

Admiral Chase: Thank you for the question, Senator.

I think first and foremost, we understand that Zero Trust is really about that we don't give privileges to person or non-person entities in the cybersecurity world. So, at its core, this is about access control and making sure that everyone doesn't have access to everything. We would move from an enclave-based world where once you get in the doors, you are free to move about. I think probably a

better description would be banking where I have access to my account. We may have the same bank, but I can't see yours. And even my children, I may have access to their accounts, but they can only do certain things with it. So, it is not just access, but what can you do with each level of privilege to be able to see what needs to be done with it, and those need to be baked in from the start.

So, as microelectronics, their purpose is known, we need to make sure that they have the ability to control access and that we have the ability to reconfigure on the fly, the configuration controls required to protect that end use appropriately.

Senator Gillibrand: Okay. In her past testimony, Deputy Assistant Secretary Eoyang noted that there can be a lot of ambiguity when it comes to attributing who is responsible for cyber intrusions, cyberattacks, especially when it comes to organizations working as proxies of nation states. In the case of financial cybercrimes where the FBI or the DOJ may have jurisdiction over investigating a cybercrime or intrusion, how well and how quickly is DOD working with other agencies to attribute these open-ended intrusions that can either be criminals or state adversaries, what could be improved?

Admiral Chase: I will start with the first part of that. There is quite a bit of sharing going on throughout

the intelligence community and cybersecurity specifically, that begins with CYBERCOM defending forward, gaining insights as to where some of our adversaries are attacking our partner nations and taking those insights, bringing them back, and sharing them broadly within the intelligence community, as well as within industry, where appropriate. Then, as you come back within the Federal Government, that threat information sharing is robust and really begins with tactics, techniques, procedures, sometimes down in the malware itself, requiring forensics experts to take a look at that. You get lots of hints from what language it is written in, where there are other places we have seen it, and where it has been attributed in those aspects.

So, I think within the Federal Government, the sharing is high. It gets more challenging and we have not had a good track record, history with sharing that with the broader Defense Industrial Base, and so I think there is significant effort going into pilots now to do that.

Senator Gillibrand: Given the recent Colonial Pipeline hack, I am especially concerned about ransomware attacks that can paralyze some of our important industrial partners. Are you confident in DOD's ability to respond and be helpful if an important DIB entity, industrial partner or business, was hit with a ransomware attack and required DOD assistance?

Admiral Chase: Well, I think first pass at that would go to the law enforcement agencies. If asked, the Department is prepared to assist there, but only in rare cases would that likely happen in national emergencies, but it would go through the same defense support system requested that any other request of the Department would go to.

Senator Gillibrand: Thank you, Mr. Chairman. Thank you.

Senator Manchin: Thank you, Senator.

And now Senator Wicker. Senator Wicker? Not there.

Senator Ernst?

Senator Ernst: Thank you, Mr. Chair. And thank you, gentlemen, as well, for your service and for being here today to share some thoughts on safeguarding our industries. I really appreciate that.

Cyberspace has been a growing conflict domain for quite a while now, but the American people have really seen over the past several months, that cyberattacks are striking ever-increasingly close to home. Of course, we have seen a variety of adversaries attacking water-treatment systems, oil pipelines, and our cloud computing infrastructure. And we know that they will continue targeting our Defense Industrial Base in years to come, as well, so I would like to focus on that a little bit.

The Defense Industrial Base's development and protection process are linked with the DOD beginning at the earliest stages of development. While this is necessary, I am concerned about the burden of cost the Government's required security measures levy on our smaller companies. We have a lot of small businesses that engage with DOD.

From your perspective, when it comes to cybersecurity, how do we strike the right balance between our private and public responsibility for cyber protection, especially as it applies to those smaller businesses? And Mr. Salazar, if we could start with you and then, Admiral, if you would like to add any thoughts.

Mr. Salazar: Within the Defense Industrial Base, we see small businesses really as the engines of innovation and vitality that make our capabilities possible. And we want to make sure, as a policy matter, that we are doing everything we can to maintain a thriving small business segment. And the recent state of supply chain attacks and disruptions have shown that many adversaries are viewing these small businesses as a weak link, that they recognize that they might not have the same cyber resilience.

Now, that said, every day, I am thinking about the challenges that these small businesses are facing and there are ways that we can, as a Department, be driving down the cost for cyber hygiene. Many of the things these companies

can do to ensure that they have good cyber hygiene, good cyber resilience are low-cost. When it comes to building systems, the Department reimburses the costs for increasing cyber resilience, but as part of our adjudication process of the CMMC system, one of the things we have heard over and over again from industry is that the barriers are quite high to ensure that these companies are meeting our requirements.

So, we are looking at this very closely and thinking about, one, how can we reduce the costs for reaching a level of cyber maturity to meet our requirements and, two, what tools and resources can we make available today to make sure that these businesses are more resilient?

So, we have actually stood up a website called ProjectSpectrum.IO, which actually had been very helpful. We have had more than 500,000 views, 10,000 trainings disseminated on cyber hygiene. Small businesses can go and says where they currently stand today. These are the kinds of resources that we are trying to make available so that we can drive down the cost and start protecting these companies today.

Senator Ernst: Thank you very much.

Admiral?

Admiral Chase: Certainly. The Defense Cyber Crime Center has also a tool if you go to their website. It is free and downloadable to the DIB, a cyber resilience

analysis tool, and this is something that covers 300 different security areas of a company across 10 different domains. These map directly to five maturity levels that are in CMMC to help understand where you are, so you don't have to go and spend a lot of money for it, so you can understand what your posture is and understand where it needs to be shored up. That is really important because the requirements are set based on adversary and threats, not what the government believes we need. So, as part of the Defense Industrial Base, they are more likely to become attacked than the more hardened Federal Government aspects are, so we want them to be successful, and this is why we believe that increasing Defense Industrial Base cybersecurity is superbly important. And we can also scale this at low cost, for things like the protective DNS system, where if you go into every query that goes out to the internet that is now enriched with potentially malicious site names so you don't get back and bring that traffic back in. It is an incredibly low-cost way to scale cybersecurity for the entirety of the DIB on a per-person, or so smaller companies wouldn't have to pay as much as, say, the large primes.

Senator Ernst: Exceptional.

And I am glad that you are so well tied into the small business community and understanding low-cost, yet effective

is certainly something that we need to enable they'd them to do.

I am running out of time, so I will leave it there and maybe submit some questions for the record. Thank you very much, gentlemen.

Senator Manchin: Thank you, Senator.

Senator Blumenthal?

Senator Blumenthal: Thanks, Mr. Chairman, and thank you to and the ranking member for having this hearing. Thank you for being back.

Have there been any cyberattacks on the Defense Industrial Base since we were here during the last hearing?

Admiral Chase: I am absolutely certain of it, I am just not sure which ones and where they are, Senator.

Senator Blumenthal: Have there been any successful ones?

Admiral Chase: I think that probably sadly falls into the same category.

Senator Blumenthal: Let me ask you about the SolarWinds and the Microsoft Exchange attacks. I think at the last hearing, you reported that neither was successful in penetrating our Department of Defense, correct?

Admiral Chase: Yes, Senator.

Senator Blumenthal: Were they successful in penetrating any of the subcontractors or contractors?

Admiral Chase: So, we had exposure of the DIB was 37 companies made 44 reports on SolarWinds exposure.

Senator Blumenthal: Those are the 44 reports of targeting or of successful intrusion?

Admiral Chase: A mixture. Those were 44 reports on exposure, the level of which I am not prepared to go into here today. I can take that one for the record.

Senator Blumenthal: But the word "exposure" refers to?

Admiral Chase: The SolarWinds attack, in particular, a supply chain attack where the SolarWinds software itself, adversaries, malicious actors compromised the software patch, itself, and so when companies normally downloaded patches as part of good cyber maintenance practice, they downloaded the malware. That malware led to command and control signals going outbound. At a minimum, this is probably where those reports would start, generically speaking. I don't have access to those at the moment, but just to understand what I say exposure, that is the exposure we are talking about.

Details of successful attacks or when that malware, that command and control call-out was brought back in additional malware and other details.

Senator Blumenthal: Would the security controls required under the CMMC have stopped those intrusions?

Admiral Chase: They would not guarantee it, but they

would have enabled them to see, possibly. Probably the best example is FireEye very publicly reported they caught the SolarWinds from observing lateral movement and privilege escalation within their own environment. If say, a level 5 CMMC would have probably had sufficient tools to give them a shot at seeing this similar lateral movement, provided they had the tipping and queueing in place. So, it would certainly enable, but it would not guarantee it.

Senator Blumenthal: And what procedures are you taking to assure that contractors actually adopt these controls? I know you have, I think you have mentioned some of the reporting requirements, but what kind of additional scrutiny and oversight are you taking just to make sure that they are doing what they are saying they are doing?

Admiral Chase: So, there are a number of innovative pilots outside of the CMMC proper that would enable to see CMMC things. There are, we have talked about one of the them, adversary emulation on the outside would show what the threats are exposing. The Crystal Ball is an outside-in looking program. There is another that is an in-line program that would allow traffic coming in see, if adopted, would send it back to a centralized repository and give us more of a, both, the Government and other entities, some idea of what threats are being presented and be able to advise on next steps, playbooks, those sorts of things.

Senator Blumenthal: Do you need more staff or more resources to do your work?

Admiral Chase: We certainly stay busy all the time, sir.

Senator Blumenthal: Thank you.

Thanks, Mr. Chairman.

Senator Manchin: Senator Blackburn?

Senator Blackburn: Thank you, Mr. Chairman.

Admiral Chase, I want to come to you and talk about the SMMs. And as we have looked at some of these cyberattacks, we have begun to talk with some of our suppliers that are such an important part of our supply chain, but, of course, they do not have the financial, the technical, or the cybersecurity support systems for their equipment and these DIB companies across Tennessee really are interested to see what is going to happen with operational cybersecurity for the U.S. manufacturing supply chain.

We know that this would be a cost-effective way not only to protect them, but to protect ourselves. So, if you would walk me through what you see as the necessary actions in the short-form and then also the longer term for DOD to take to improve that cybersecurity posture for these SMMs.

Admiral Chase: So, for small business, the single, and really for any enterprise undertaking cybersecurity, the most important thing is getting visibility of the things you

own. So, making sure that you have both, the sensing and the ability to understand what it is that you are looking at. And these are becoming available as a service, so I am excited about that. Security as a service platform as a service for companies that do their businesses as cloud. These are increasingly prevalent, so we are excited about that.

You mentioned operational technology. This is probably the, in cybersecurity at large, the least understood, because operational technology is aware, cybersecurity is meaning controlling of machines and many times, those are not even under the same internet protocols that we see under traditional cybersecurity, so it requires a unique workforce. So, whether we put a cyber wrapper around that to understand the flows that are going in so we can look at that in Zero Trust and make sure that are the right people controlling this, does this order coming from the right, the place that orders to this piece of machinery should normally come from, these are the sorts of things that a control system company would want to know and make sure that they could see happening and be able to intervene.

Senator Blackburn: Do you all have sufficient authority to work with these SMMs, and to improve their, or help them harden their systems and properly integrate their systems with yours?

Admiral Chase: I certainly believe the Department has enough to be able to share what we know about the threat and we have our own operational control systems, operational technology systems and we can share, certainly share the best practices. I would say as the executive order is tasked with a lot of these same topics to make a lot of progress and share those out, work with NIST to develop standards for all of the above, I think those are areas where we can bring the Department of Defense to bear.

Senator Blackburn: What about Zero Trust architecture, how does that inform your efforts as you look at cybersecurity and hardening for the supply chain?

Admiral Chase: So, Zero Trust principles include at their core, access control and configuration management, and these are common cybersecurity principles, however, doing so at a much more granular level is the knack here. So, understanding your flows, who should have access to data inside even a small company network. For small businesses, that is a relatively straightforward task. As you start to move up in scale, these need to be able to be done at an enterprise level, so are probably more challenging.

Senator Blackburn: Let me ask you this, do you all have any training or best practice protocols that you are sharing with or training your providing to some of the SMMs, so they know how to assess vulnerabilities and they know

what is going to be a preferred platform for integrating their work with yours?

Admiral Chase: So, the Defense Cyber Crime Center, I think has a number of pilot programs. They do a significant amount of training and so does the counterintelligence community; however, those are not DIB and widely exported to the DIB and I think that is probably an area as we come to learn more internally, we can share that, but that is an area for growth, not something we have today.

Senator Blackburn: Okay. Well, you know, in Tennessee, the Y12 complex is co-leading the supply chain cybersecurity initiative and we are really proud of the work that they have doing and I will submit a question to you in that regard. I see that I have run out of time. Thank you.

Thanks, Mr. Chairman.

Senator Manchin: Thank you, Senator.

Senator Rosen? Not here?

Admiral Chase, the whole thing of what happened, first, the United States Government, Department of Defense, do we pay ransoms?

Admiral Chase: No, sir, we do not.

Senator Manchin: Do we counter attack?

Admiral Chase: That would be a whole-of-government approach, based on a preponderance of other factors and national policy.

Senator Manchin: The reason I am saying that, knowing that we do not pay ransoms, but the private sector, there is no rule or law against the private sector paying them, as we just Colonial pay.

Admiral Chase: A true statement. And I believe one of the other challenges I have seen in popular reporting, depending on who you look at, somewhere between a 15 and 22 percent rate, even if you pay the ransom, that you will actually get your decrypted data back.

Senator Manchin: I think --

Admiral Chase: That is what I am reading in open press.

Senator Manchin: Sure. Sure.

Well, I am just saying, it sets up, you know, this illegal, criminal activity that will continue to grow, knowing that the American public or that the American businesses will pay, or thinking they will if Colonial sets the standard. That is probably the highest profile I have heard of, of paying that type of a ransom, what, 4.9 million in crypto? I believe that was the amount.

Admiral Chase: I believe that is what I heard was asked.

Senator Manchin: Yeah, that is what we heard.

Admiral Chase: I don't have any knowledge of what was paid.

Senator Manchin: The thing I am trying to say is, we have so many different cyber agencies and different, I mean cyber departments and different agencies, but there is only one, I think, that would have the ability to hit back and hit it pretty good would be you all.

Admiral Chase: Senator, I think one of the challenges, at cybersecurity level, you are left with two things: espionage and sabotage. So, depending on how those are, one is a crime and the other would be, if done by foreign actors, and this is one of the challenges of attribution even from some of the latest ones, is with the commoditization of malware becomes, it may have been developed by one entity and used by another and employed by a far-less sophisticated actor in the case of an unprotected customer. So, I think that is --

Senator Manchin: I think we were able to detect where it came from and who did it. It didn't seem like it took that long for them to identify.

Admiral Chase: We know that the malware was written in some Russian code or pro -- to not attack certain Russian actors, but I am not seen any attribution of who actually did the act.

Senator Manchin: I am just saying there has to be something that we, as a country and our Government, is going to use to deter this from happening again or continuing to

happen.

Admiral Chase: Absolutely, Senator. I mean, I think the most recent one with the dark side shows that this is effectively organized crime and the international community has to come to terms with how we are going to deal with this. Not just the United States, but it is a worldwide problem.

Senator Manchin: Is there discussions going on?

Admiral Chase: I believe that there is certainly a recognition that this is a problem. I tend to spend more of my time on the cybersecurity side than on the policy side.

Senator Manchin: Okay. Thank you.

Senator Rounds?

Senator Rounds: Thank you, Mr. Chairman.

Mr. Salazar, I want to come back to you for just a minute. In your opening statement, you indicated that the CMMC rules were being vetted at this time and that it would probably be at, I think you said about 10 months yet or close to a year from the beginning until the end.

Would you except that the finals on the CMMC rules would be in place by the end of this year?

Mr. Salazar: As I mentioned, it typically takes about a year to adjudicate comments for this kind of DFARS rule. Eight hundred and fifty comments is what we would consider a very high volume of comments and on top of that, we have the

recommendations from our internal policy review. So, about half of the comments that we received to the DFARS rule were not about the rule itself, but about the program and so that is why, as part of our look, we are trying to assess how we bring clarity to the requirements that we are asking, looking at the barriers to small businesses and then making sure that we have trust in this assessment ecosystem.

Senator Rounds: Thank you. You know, during that time period until CMMC is implemented, we are going to find, you know, we are still going to have those openings and the risk that CMMC is trying to address is still there. So, I am going to come back over to Admiral Chase.

And I think where the Chairman is going with regard to his line on this in terms of how do we coordinate to be able to protect not just the DOD, but all of the different entities that the American public rely on from cyberattack is so critical, and I think it would surprise a lot of the folks out there to realize that the Department of Defense really doesn't have a role to play today in defending against cyberattacks coming in from overseas, at least directly and that they have to be invited in from Homeland Security in order to respond.

It seems to me that part of the responsibility that we have here is to be able to coordinate between the different, as we call them, silos or offices. A lot of that has got to

start in the White House and within the top ends of the Executive Branch of the government. We wanted, and I think the Cyber Solarium this last time around, laid out clearly the need for a principal cyber advisor. And when we laid out the principal cyber advisor to the President, we also, and that would be the national cyber director, we modeled that in many ways along the same lines as we wanted to have a principal cyber advisor for the Secretary of Defense and for each of the separate branches within the Department of Defense.

And I think that is still critical that we have someone there to provide advice to look at integrating those cybersecurity needs and a sense of how critical cybersecurity is in all of the things that we do within the DOD. And I sense that there is almost a blowback to that in terms of we are not seeing the principal cyber advisors being identified and we are not seeing the national cyber advisor necessarily being sent in for approval by the United States Senate.

So, my question, Admiral Chase, and I am just going to offer this, what does that do in your role here, and as you hear us asking the questions of you today, do you find a challenge in terms of just your role to try to respond to the demands that are out there, with regard to protecting DOD from the attacks that are ongoing. As you indicated to

Senator Blumenthal, the attacks are ongoing and they are always there and there are people that are incurring right now.

Is it simply a matter that we haven't lit a fire yet or is it a matter of we don't have the technical expertise or is it simply a matter that the bad guys are, the numbers are so large in numbers that we are going to have a tough time getting ahead of this whole program. What is it that seems to slow down our ability to respond quickly, with regard to the cyberattacks that are going on?

Admiral Chase: For the Department, I mean, I think we spend a fair bit of our time making sure that we don't have stove pipes and that is to your point, exactly what I believe Congress stood up the principal cyber advisor to do and I think we, on a day-in day-out basis, we run up to 10 or 11 cross-functional teams kind of by subject matter, covering broadly four areas: one, the DOD; two, the DIB; three, mission assurance and weapons systems critical infrastructure that are not traditionally cyber things, but were created before those thoughts were prevalent and yet, we still have some of the older weapon systems, so how do we deal with those, and this is where the strategic cybersecurity program, mission assurance pieces come in; and then we have workforce to work across all of those, as well.

So, we spend a lot of time in those cross-functional

areas with others as the lead and just making sure doing introductions, hey, do we have this particular aspect cover done. So, I find that our organization is most successful by asking questions, rather than by trying to be forceful at certain pieces, because seldom are we the lead, except for areas like in DIB coordination, but again, that is making sure left and right and know who is coordinating which part.

So, I think you are absolutely right about breaking down barriers. Minimizing the barrier to entry is a principle I think we all want for improving cybersecurity, whether or not we are talking about the DIB, the DOD, or areas of weapons systems and critical infrastructure.

Senator Rounds: You know, Mr. Chairman, I think that is one of the things here that as we challenge these leaders within cybersecurity, it is really the public policy part of this that we have yet to fix, in my opinion, and that is, that we have folks from outside of the United States that are clearly interested in reading our intellectual properties at all levels and yet we have the multiple silos within the whole-of-government that because of our public policy, we don't want to inflict the DOD onto the public here and we don't want the DOD directly involved in the day-to-day lives or within the Defense Industrial Base or any of the other industries in the country, and yet I think the public has this expectation that we have the capability to

defend them, and yet because of our own public policy, even if we know about it, Homeland Security can't reach out and stop the guy who is throwing the systems in or the weapons in and the Department of Defense, who really have a lot of great capabilities really can't go out and get them until they find out about the attacks themselves.

And so, we find ourselves at a point in which we have to coordinate it and we are not doing a good job of that yet.

Senator Manchin: Senator, you know, and this is a discussion for you all and for us too, but the Department of Defense is going to intervene to prevent something from happening once they identify it. I am just looking at the Colonial. I have been concerned about this because I know of our infrastructure has so much. We know what Mother Nature did to Texas and how that shut down and the lives were at danger and everything that happened. We know what happened with the Colonial Pipeline, what it did to the economic. I mean, all up and down the East Coast, just about, especially in the South, it just destroyed it for that period of time, about a week. So, that is an attack to me, as far as on our country.

Admiral Chase: Yes, sir. The threat is very real. It is not just cybersecurity. It is to the reality of the DIB's business and the private sector at large is under the

same attack. We think the fastest way we can bring that to bear and not be completely reactive is to share the threat information we have at the cybersecurity level, the tactics, techniques, and procedures. After we saw AB, the next thing that is going to happen is C, and we can --

Senator Manchin: Well, we have had SolarWinds. We have had so many different things happening back and forth and we are still trying to, but do you know, did we have any knowledge at all of this Colonial Pipeline that you know of? Did we see anything?

Admiral Chase: We do not. I believe even the history of that particular actor only goes back about a year, if you look in public internet, it will tell you that it springs up. And this is what I spoke to earlier about the commoditization of malware and actors, it has been made relatively straightforward and easy for criminals to do so. What is unique about this one is they seemed to have a network of subordinate actors to do some of the work after packaging up the malware. So, I think that is a sad statement on the sign of our times, but it is also the reality that every member of the private sector is under as well.

Senator Rounds: But with regard to that particular one, if my knowledge is correct, and I will ask the Admiral if he could confirm it for us, number one, there is no rule

that says that the private company needs to notify either Homeland Security or the FBI or the Department of Justice and then second of all, even if they did notify the FBI, the Department of Justice, and so forth, there is no established ongoing process in which to gather that information and then deliver it to the Department of Defense to respond to those threats coming in from overseas unless they specifically request. And to the best of my knowledge, number one, we are not aware that Homeland Security was even advised of what occurred and second of all, to the best of our knowledge, and I will ask you to confirm this part, I don't think the Department of Defense was ever asked to intervene or to assist in this particular case, were you?

Admiral Chase: I am not aware of it and if we are, I will take that one for the record and come back and tell you.

Senator Rounds: Thank you.

Senator Manchin: If you could, any information you can.

The other thing, you know, with crypto coming in, the way it is coming on, all over the world, it makes it much more difficult for us to follow as we could with currency and that has been the problem that we have had. Have you all been looking at the crypto and how we might be able to have better tabs on that or be able to have identity and

follow that?

Admiral Chase: Are you talking about cryptocurrency as a means of payment?

Senator Manchin: Yeah.

Admiral Chase: That is not something my office has particularly studied. We have been on the other side of cryptography, protecting our weapons systems and critical infrastructure.

Senator Manchin: Gotcha. Well, we are going to have to use all of our expertise we have, I think, to defend our country.

Mr. Salazar, do you have anything you want to add to the conversation? It is kind of random here.

Mr. Salazar: Only that across the [inaudible].

[Audio Malfunction.]

Senator Manchin: Admiral, anything else?

Admiral Chase: No, Senator, thank you.

Senator Manchin: Senator Rounds?

Well, if not, let me thank you both for coming. It was very enlightening and we appreciate very much your service to our country. I really do appreciate that very much. I know that Senator Rounds feels very strongly about that, too.

So, with that, we are adjourned.

[Whereupon, at 3:37 p.m., the hearing was adjourned.]