S. HRG. 117–938

RECENT RANSOMWARE ATTACKS

HEARING

BEFORE THE

SUBCOMMITTEE ON
CYBERSECURITY

OF THE

COMMITTEE ON ARMED SERVICES
UNITED STATES SENATE

ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

JUNE 23, 2021

Printed for the use of the Committee on Armed Services

Available via: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
59–562 PDF WASHINGTON : 2025

COMMITTEE ON ARMED SERVICES

JACK REED, Rhode Island, *Chairman*

JEANNE SHAHEEN, New Hampshire
KIRSTEN E. GILLIBRAND, New York
RICHARD BLUMENTHAL, Connecticut
MAZIE K. HIRONO, Hawaii
TIM KAINE, Virginia
ANGUS S. KING, Jr., Maine
ELIZABETH WARREN, Massachusetts
GARY C. PETERS, Michigan
JOE MANCHIN III, West Virginia
TAMMY DUCKWORTH, Illinois
JACKY ROSEN, Nevada
MARK KELLY, Arizona

JAMES M. INHOFE, Oklahoma
ROGER F. WICKER, Mississippi
DEB FISCHER, Nebraska
TOM COTTON, Arkansas
MIKE ROUNDS, South Dakota
JONI ERNST, Iowa
THOM TILLIS, North Carolina
DAN SULLIVAN, Alaska
KEVIN CRAMER, North Dakota
RICK SCOTT, Florida
MARSHA BLACKBURN, Tennessee
JOSH HAWLEY, Missouri
TOMMY TUBERVILLE, Alabama

ELIZABETH L. KING, *Staff Director*
JOHN D. WASON, *Minority Staff Director*

SUBCOMMITTEE ON CYBERSECURITY

JOE MANCHIN III, West Virginia, *Chairman*

KIRSTEN E. GILLIBRAND, New York
RICHARD BLUMENTHAL, Connecticut
JACKY ROSEN, Nevada

MIKE ROUNDS, South Dakota
ROGER F. WICKER, Mississippi
JONI ERNST, Iowa
MARSHA BLACKBURN, Tennessee

CONTENTS

RECENT RANSOMWARE ATTACKS

WEDNESDAY, JUNE 23, 2021

UNITED STATES SENATE,
SUBCOMMITTEE ON CYBERSECURITY,
COMMITTEE ON ARMED SERVICES,
Washington, DC.

The Subcommittee met, pursuant to notice, at 2:00 p.m. in room SR–222, Russell Senate Office Building, Senator Mike Rounds (Ranking Member of the Subcommittee) presiding.

Subcommittee Members present: Senators Rounds, Gillibrand, Ernst, and Blackburn.

OPENING STATEMENT OF SENATOR MIKE ROUNDS

Senator ROUNDS. Good afternoon. On behalf of Senator Manchin, the chairman of our committee, I would like to call this Cyber Subcommittee meeting to order. Senator Manchin has been delayed, but in his usual bipartisan fashion he asked that we get the meeting start and that he will be in as quickly as he can.

I will begin with an opening statement, and then we would love to hear from you, and hopefully by then Senator Manchin will also be able to participate in this open portion of the session.

So I would like to begin by first of all thanking Senator Manchin for the bipartisan effort in which he allows us to begin this process, and second of all, I would like to thank all of our witnesses, Ms. Eoyang, Major General Kennedy, and Rear Admiral Foy.

Our hearing today addresses an issue that has unfortunately been a near-permanent headline over the last year. Ransomware attacks have plagued businesses across the United States, and it seems like no one is immune—not schools, not hospitals, and certainly not government systems. Just in the last few months, several large ransomware attacks of the Colonial Pipeline and the JBS meatpacking company have disrupted the everyday lives of Americans. These attacks shine a spotlight on several areas that we need to pay closer attention to.

First, the capabilities of our adversaries are growing rapidly, and their ability to execute increasingly disruptive attacks is quite worrying. In this case of the Colonial Pipeline attack, a single ransomware attacks was able to disrupt gas availability across a large section of the United States for almost a week.

Second, the ability of private businesses and organizations in the United States to defend their digital infrastructure needs significant improvement.

Third, the Federal Government's capabilities to prevent and respond to these attacks also needs to improve to meet this growing

threat to protect not only the Federal Government system but also the Nation as a whole.

I believe that we need to have a robust national dialogue on the shared responsibilities of the Federal Government and the private sector in addressing these cyber threats. We need to have a public policy debate on the responsibilities of industry, for their own cybersecurity competency, and their enforcement of cyber hygiene within their organizations.

I believe we also need to improve information sharing about cyberattacks. In a hearing in front of our committee earlier this spring, General Nakasone, Commander the United States Cyber Command and the Director of the National Security Agency discussed cyberattacks being conducted against the United States targets by foreign cyber actors by describing that, and I quote, "It is not the fact that we can't connect the dots. We can't see all of the dots," end quote.

I think it is time to explore a requirement for industry to make confidential disclosures of cyberattacks above a certain threshold to the appropriate authorities to strengthen our ability to more quickly find and respond to these cyberattacks.

These topics for debate extend beyond the jurisdiction of the Cyber Subcommittee of the Senate Armed Services Committee, but I believe that we must address these issues holistically, and I look forward to working with my colleagues on the other committees of jurisdiction and with industry to explore the policies necessary to better protect our Nation.

Now in addition to discussing the roles and responsibilities of the private sector in defending themselves against cyberattacks, it is also time to discuss the roles and responsibilities of the Federal Government in responding to ransomware attacks on private industry, and any response must take a whole-of-government approach. In the Fiscal Year 2021 National Defense Authorization Act, our committee included a provision to establish a national cyber director to act as an advisor to the President and coordinate activities like cyber incident response across the Federal Government and with private industry. I urge the President to move quickly to stand up that office in order to improve coordination across the Federal Government in response to the ever-growing number of cyberattacks.

While the Department of Homeland Security and the Department of Energy or the Department of Justice often leads efforts in responding to these attacks, I think it is important for our committee to assess what the appropriate role is for the Department of Defense in defending the Nation from attacks that often are conducted by criminal actors in foreign nations. I am sure that there are many areas where improvements can be made across the entire Federal Government in addressing this growing threat.

Now I want to be clear. The 2018 Department of Defense Cyber Strategy defines three main cyber mission, one of which is to defend the United States and its interests against cyberattacks of significant consequence. I look forward to hearing today about what has been the Department of Defense's role in responding to recent ransomware attacks. However, I would be interested in hearing what additional efforts and capabilities could be provided by the

Department of Defense to deter and counter ransomware attacks as part of a whole-of-government approach. I know that there are many aspects of the cyber capabilities of the Department of Defense that cannot be discussed in public, and I look forward to hearing more in the closed session later this afternoon.

Once again, I want to thank all of you for your willingness to testify today, and I look forward to the conversation here in this open session.

Now I would, at this time, on behalf of Chairman Manchin, like to introduce our briefers here today and ask you to give your testimony, and then when the chairman is able to come back in we will have him give his testimony as well.

We have Ms. Mieke Eoyang, Deputy Assistant Secretary of Defense for Cyber Policy—welcome; Major General Kevin B. Kennedy, Director of Operations for the United States Cyber Command—welcome, sir; and Rear Admiral Ronald A Foy, Deputy Director for Global Operations. You are all here to share your thoughts, and we are here to listen to testimony on ransomware.

With that, Ms. Eoyang, I am not sure if you have a plan sequence or not, but I would invite you to begin if you would like.

STATEMENT OF MIEKE EOYANG, DEPUTY ASSISTANT SECRETARY OF DEFENSE FOR CYBER POLICY

Ms. EOYANG. Thank you, Senator Rounds, Senator Ernst. I am pleased to be here with General Kennedy, Director of Operations for U.S. Cyber Command, and Admiral Foy, the Deputy Director of Global Operations for the Joint Staff, to discuss the Department of Defense's role in addressing the urgent threat of ransomware. I have submitted a joint statement on behalf of all three witnesses and will provide that and then turn to my colleagues for their additional comments.

Senator ROUNDS. Your full written testimony will be included for the record.

Ms. EOYANG. Thank you, Senator. Before I begin, Senator Rounds, as you have noted, we are not able to discuss sensitive military cyber operations in this open, unclassified setting, and we look forward to providing you additional details in the closed session that follows.

I can say this much, however. The Department recognizes the seriousness of this threat to U.S. critical infrastructure. Although the DOD Information Network, known as the DODIN, has not fallen victim to ransomware, we are acutely aware of the threat to private companies that comprise the defense industrial base and operationally critical contractors.

But this is not just a DOD-centric concern. The recent Colonial Pipeline and JBS compromises have demonstrated ransomware's potential to disrupt the lives of everyday Americans. Ransomware is increasingly emerging as a threat to our national, homeland, and economic security, and thwarting ransomware actors effectively requires a whole-of-government response that is coordinated with the private sector and our international partners.

I applaud the members for your bipartisan leadership to ensure that the U.S. Government is able to counter this threat. I understand that each of the states, which you represent, has suffered at

least one ransomware incident involving essential public functions, including those furnished by municipal governments, schools, and airports. As demonstrated by the incidents affecting the Pleasant Valley Hospital in West Virginia and law firms in South Dakota, ransomware hurts people and disrupts lives. These particular ransomware incidents happened recently, but the list of American ransomware victims is long and grows every day, as the threat becomes pervasive. It is not just in the United States. We have seen threats by ransomware to our partners and allies throughout the world, from Ireland to the U.K. to Brazil. This is a truly global problem. I look forward to working with you as we take up the cause of mitigating these disruptions to Americans' daily lives.

President Biden has made it a priority to address the ransomware threat. This made clear the U.S. position that attacks on, and disruption of, our critical infrastructure, through the use of ransomware or any other cyber means, in not acceptable. In May, after the Colonial Pipeline incident, the President signed an Executive order to improve our Nation's cybersecurity. The order calls for Federal agencies to work more closely with the private sector to share information, to strengthen cybersecurity practices, and to deploy technologies that increase resilience.

Addressing the threat of ransomware will be a challenge. Part of this challenge is the increasingly blurry line between nation-state and criminal actors. We have seen some governments let government-employed hackers "moonlight" as cybercriminals for personal benefit, which is not how responsible states behave in cyberspace. Our adversaries have also created permissive environments for criminal ransomware gangs, providing them safe haven within their borders and shielding them from prosecution as long as they avoid targeting the host country's businesses and government systems. This scourge, again, is affecting countries all throughout the world.

This is sometimes evident in ransomware code, as gangs operating in Russia design their malware to avoid infecting computers where Russian is the default language. The administration has been clear that this is not acceptable, and that responsible countries must take action against criminals who conduct ransomware activities from within their soil.

We cannot, however, expect these financially motivated crimes to cease in the immediate term. The Department currently works to counter ransomware threat as part of our mission to defend the Nation in cyberspace. We do this as part of whole-of-government efforts, but the DOD has several distinct roles in this effort.

First, the Department gains insights about hostile cyber actors through Hunt Forward Operations on allied and partner nation networks. We use those insights to improve our own security posture and to enable appropriate actions by our partners, domestically and internationally. We are also prepared to take authorized actions to stop or degrade activity.

Second, we take actions to increase the security and resiliency of the defense industrial base and operationally critical contractors. The DOD Cyber Crime Center and its Defense Industrial Base Collaborative Information Sharing Environment, have prioritized ransomware reporting and content briefings in support of DOD's

DIB Cybersecurity Program Partners, emphasizing impacts, implications, and threat mitigations.

Third, the Department continuously defends the DODIN from all malware, including ransomware. Our cyber forces regularly hunt for adversaries on the DODIN, and, as I mentioned previously, we continue to leverage the insights gained by operating on foreign networks to improve our defenses, and we continue to strengthen our partnerships with the Federal Bureau of Investigation and the Department of Homeland Security in order to improve those cyber defenses of Federal, State, and local level, as well as those of the private sector.

The Department has the capability and capacity to ensure the security and resiliency of its own networks and to conduct operations in support of the Joint Force. Thus far, ransomware perpetrators appear to be financially motivated and therefore to have targeted private industry for financial gain. These are crimes.

The Department stands ready to support our colleagues at the Federal Bureau of Investigations (FBI) in their pursuit of these criminal actors. Further, the Department may provide assistance, where requested, to the Department of Homeland Security, which has the lead for protecting domestic critical infrastructure.

In closing, I would like to thank the members once again for your bipartisan leadership to enable the U.S. Government to counter these threats and as we work with our interagency partners in defending the Nation against ransomware. We know that Congress is a strong and willing ally in this fight, and as Senator Rounds noted, a whole-of-government response is necessary to address this threat effectively. As the majority of U.S. critical infrastructure is privately owned, combatting ransomware requires a whole-of-nation response.

Thank you, and I will turn to my colleagues for their remarks.

Senator ROUNDS. Thank you, Secretary Eoyang, and on behalf of the chairman I would recognize Major General Kevin Kennedy.

STATEMENT OF MAJOR GENERAL KEVIN B. KENNEDY, USAF, DIRECTOR OF OPERATIONS, UNITED STATES CYBER COMMAND

General KENNEDY. Thank you, Senator Rounds. Ranking Member Rounds, Senator Ernst, members of the Cyber Subcommittee, I am Major General Kevin Kennedy, Director of Operations at U.S. Cyber Command. I am pleased to be here today with Deputy Assistant Secretary of Defense Eoyang and Rear Admiral Foy, and honored to represent the men and women of U.S. Cyber Command, as we discuss this urgent threat of ransomware.

As the action arm for the Department of Defense in cyberspace, U.S. Cyber Command recognizes the serious nature of the growing ransomware threat to our critical infrastructure and military capabilities. Increasingly, capable, organized criminal groups and opportunistic criminals are exploiting victim data to extort and deny access to crucial information and critical systems. The growing list of municipalities, corporations, and private citizens around the world who have been preyed upon by these criminal demonstrates the broadening scope, scale, and sophistication of this malicious cyber activity.

The number and size of ransomware incidents represents a growing trend by cyber criminals to threaten companies and government agencies. These malicious actors conduct their criminal operations from within the boundaries of the United States, exploiting gaps in our defenders' ability to see malign activity in U.S. cyberspace infrastructure.

For U.S. Cyber Command to meet this threat, our special partnership with the National Security Agency is paramount. The intelligence and insights produce by the National Security Agency are critical enablers for the law enforcement community and U.S. Cyber Command to prevent, blunt, and respond to malign activity with the speed and agility required in cybersecurity. When authorized, U.S. Cyber Command acts to disrupt, degrade, and defeat foreign malicious cyber actors, to include organized criminal groups. We also work with National Guard units to rapidly share information about malicious cyber activity, thereby enhancing their support to state and local incident response.

U.S. Cyber Command is fully engaged with our interagency partners. We provide critical threat information and insights to the Federal Bureau of Investigation and the Department of Homeland Security's Cybersecurity Infrastructure Security Agency, enabling each to act under their respective authorities.

Finally, we work with our industry partners to enhance our shared understanding of the cyberspace environment so that together we can increase the resilience of our Nation's information systems, both public and private.

Cyberspace affords our adversaries, to include cyber criminals, many opportunities and means to threaten U.S. interests. Our adversaries have proven to be creative and adaptive. Ransomware is indicative of the evolving threat. However, U.S. Cyber Command, in close partnership with the National Security Agency, is adapting too. We persistently engage these threats, as close as practical, to the source. With our partners and allies at home and abroad, we are proactively contesting these threats, posturing to respond when necessary, and continuously seeking opportunities to disrupt, deny, degrade, and defeat malign activity beyond our shores.

The men and women of U.S. Cyber Command are grateful for the support of this committee and Congress as we execute our mission on behalf of the Nation, and I now look forward to your questions.

Senator ROUNDS. Thank you, General, and on behalf of the chairman, Chairman Manchin, I would ask Rear Admiral Ron Foy for your comments, sir.

STATEMENT OF REAR ADMIRAL RONALD A. FOY, USN, DEPUTY DIRECTOR FOR GLOBAL OPERATIONS, JOINT STAFF

Admiral FOY. Thank you, sir. Chairman Manchin, Ranking Member Rounds, Senator Ernst, and distinguished members of the subcommittee, thank you for the opportunity to appear before you today with Deputy Assistant Secretary of Defense for Cyber Policy Eoyang and Major General Kennedy.

On behalf of the Joint Staff, the J–39, which I run, focuses on enabling the DOD, with the requisite authorities and processes, to conduct cyber effects operations. I facilitate the interagency approval process for cyber effects campaign plans, required under

NSPM–13, to enable USCYBERCOM to execute authorized missions against adversaries outlined in the 2018 National Defense Strategy.

Since 2018, the Secretary of Defense has approved multiple campaign plans that address adversaries noted in the 2018 National Defense Strategy, and as a result of your ongoing support the Department is postured with the requisite authorities and interagency coordination procedures to respond to and preemptively address malicious cyber activities.

Again, thank you. I am honored to be here today, and I look forward to a thorough and continued dialogue, and welcome your questions.

[The joint prepared statement of Ms. Eoyang, General Kennedy, and Admiral Foy follows:]

JOINT PREPARED STATEMENT BY MIEKE EOYANG, MAJOR GENERAL KEVIN B. KENNEDY, REAR ADMIRAL FOY

Thank you Chairman Manchin, Ranking Member Rounds, and Members of the Committee. I am pleased to be here with Major General Kennedy, Director of Operations, U.S. Cyber Command (USCYBERCOM), and Rear Admiral Foy, Deputy Director for Global Operations, Joint Staff, to discuss the Department of Defense (DOD) role in addressing the urgent threat of ransomware. I have submitted this joint statement for the record on behalf of all Department witnesses. Before I begin, I would like to remind the Members that we are not able to discuss sensitive military cyber operations in an unclassified setting. We look forward to providing you with additional information in the closed session.

I can say this much, however. The Department recognizes the seriousness of this threat to U.S. critical infrastructure. Although the DOD Information Network (DODIN) has not fallen victim to ransomware, we are acutely aware of the threat to the private companies that comprise the defense industrial base (DIB) and operationally critical contractors. This is also not just a DOD-centric concern. The recent Colonial Pipeline and JBS compromises have demonstrated ransomware's potential to disrupt the everyday lives of Americans. Ransomware is a threat to our national security, and thwarting ransomware actors effectively requires a whole-of-government response that is coordinated with the private sector and our international partners.

I applaud the Members for your bipartisan leadership to ensure that the U.S. Government is able to counter this threat. I understand that each of the States, which you represent, has suffered at least one ransomware incident involving essential public functions, including those furnished by municipal governments, schools, and airports. As demonstrated by the incidents affecting the Pleasant Valley Hospital in West Virginia and small law firms in South Dakota, ransomware hurts people and disrupts lives. These particular ransomware incidents happened recently, but the list of American ransomware victims is long and grows each day, as the threat becomes more pervasive. I look forward to working with you as we take up the cause of mitigating these disruptions to Americans' daily lives.

President Biden has made it a priority to address the ransomware threat. This made clear the U.S. position that attacks on, and disruption of, our critical infrastructure, through the use of ransomware or other cyber means, are not acceptable. In May, after the Colonial Pipeline incident, the President signed an executive order to improve our Nation's cybersecurity. The order calls for Federal agencies to work more closely with the private sector to share information, to strengthen cybersecurity practices, and to deploy technologies that increase resilience.

Addressing the threat of ransomware will be a challenge. Part of this challenge is the increasingly blurry line between nation-state and criminal actors. We have seen some governments let government-employed hackers "moonlight" as cybercriminals for personal benefit, which is not how responsible States behave in cyberspace. Our adversaries have also created permissive environments for criminal ransomware gangs, allowing them to operate from within their borders and shielding them from prosecution so long as they avoid targeting the host country's businesses and government systems. This is sometimes evident in ransomware code, as gangs operating in Russia design their malware to avoid infecting computers where Russian is the default language. The administration has been clear that this is not

acceptable, and that responsible countries must take action against criminals who conduct ransomware activities from within their territory.

We cannot, however, expect these financially motived crimes to cease in the immediate term. The Department currently works to counter the ransomware threat as part of our mission to defend the Nation in cyberspace. We do this as part of whole-of-government efforts, but DOD has several distinct roles in this effort.

First, the Department gains insights about hostile cyber actors through Hunt Forward Operations on allied and partner nation networks. We use those insights to improve our own security posture and to enable appropriate actions by our partners, domestically and internationally. We are also prepared to take authorized actions to stop or degrade adversary activity.

Second, we take actions to increase the security and resiliency of the DIB and operationally critical contractors. The DOD Cyber Crime Center (DC3) and its DOD–Defense Industrial Base Collaborative Information Sharing Environment (DCISE) have prioritized ransomware reporting and content briefings in support of DOD's DIB Cybersecurity Program Partners—emphasizing impacts, implications, and threat mitigations.

Third, the Department continuously defends the DODIN from all malware, including ransomware. Our cyber forces regularly hunt for adversaries on the DODIN. As I mentioned previously, we continue to leverage the insights gained by operating on foreign networks to improve our cyber defenses, and we continue to strengthen our partnerships with the Federal Bureau of Investigation and the Department of Homeland Security in order to improve the cyber defenses of Federal, State, and local governments, as well as those of the private sector.

The Department has the capability and capacity to ensure the security and resiliency of its own networks and to conduct operations in support of the Joint Force. Thus far, ransomware perpetrators appear to be financially motivated and therefore to have targeted private industry for financial gain. These are crimes.

The Department stands ready to support our colleagues in the Federal Bureau of Investigation in their pursuit of these criminal actors. Further, the Department may provide assistance, when requested, to the Department of Homeland Security (DHS), which has the lead for protecting domestic critical infrastructure.

In closing, I would like to thank the Members once again for your bipartisan leadership to enable the U.S. Government to counter cyber threats to our national security. As the Department works to support its interagency partners in defending the Nation against ransomware, we know that Congress is a strong and willing ally in this fight. A whole-of-government response is necessary to address the ransomware threat effectively, but as the majority of U.S. critical infrastructure is privately owned, combatting ransomware also requires a whole-of-nation response. Thank you for your time today, and I look forward to your questions.

Senator ROUNDS. Thank you, Admiral, and look, on behalf of the Chairman once again I want to thank all of you for your comments and for participating in this open session. We are in a position to where we will be able to do a closed session as well.

Senator Ernst, I know that you have got questions as well. Since I will be here for the hearing, I would defer, if you would like to ask questions first. On behalf of the chairman I would ask you if you would like to ask your questions, and then we will move from there.

Senator ERNST. Thank you, Ranking Member Rounds. I appreciate that very much. I will have another committee to attend here in a moment. So again, thank you all for appearing in front of us today, and specifically for stepping up to the ransomware challenge.

Cyberspace has been a growing conflict domain now for many years, but the American people have seen, over the past several months, that ransomware has the capacity to strike closed and closer to home. The Department of Defense should not sit on the sidelines of this conflict, and this discussion of how the DOD may be able to lend additional aid to the fight against cyberattacks is a very productive start. So once again thank you so much.

Ms. Eoyang, what challenges does DOD face as it aims to prevent and retaliate against ransomware attacks on government contractors support DOD installations and key defense industrial base capabilities?

Ms. EOYANG. Thank you, Senator. This is indeed a challenge, and we have been very fortunate in the Department that our own systems have not been affected by this, but we do very much worry for our industrial base, and we have seen some incidents where they have been targeted.

It is a challenge in that these are criminal acts occurring on U.S. soil against U.S. contractors, and the Department's focus has been largely to focus on the nation state actors outside of our borders. So we work closely with the FBI and the Department of Justice and our own law enforcement agencies internal to the Department to be able to identify the perpetrators and try and mitigate the impact of any such incident.

Senator ERNST. Taking that just a little bit deeper dive, what role is appropriate for the DOD as we play a role in this arena in supporting the government's response to those ransomware attacks on our critical infrastructure or with those defense contractors? What is appropriate for us?

Ms. EOYANG. So, Senator, one of the challenges—well, the Department has three main missions in cyberspace: defending the DODIN, preparing to fight and win the nation's wars, and defending the nation. We will not be able to stop every attack from coming in—the volume is just too much—but the Department can play a critical role in enabling other departments and agencies, based on the insights that we can generate overseas against these actors to help them identify these individuals.

I will turn to General Kennedy to give some more specifics on how that works.

Senator ERNST. Thank you.

General KENNEDY. Yes, Senator. So, Senator, I can talk as far as the policy of what it should be. I can talk about what we do do, and so right now there are kind of two primary phases. The first one is any attack that we want to see how we can prevent that from coming to fruition, and so if we see indications of compromise or malware present in the environment outside of the nation we take that information and we provide those indicators of compromise to our partners in the interagency, primarily through Cybersecurity and Infrastructure Security Agency (CISA) and through the FBI. They then would be able to share with industry partners.

With respect to the defense industrial base and our DIB contractors, DOD has the Defense Cyber Crime Center, and we would share that information with them, and they have information-sharing agreements in place that enables them to help provide them that awareness.

After the fact, any kind of ransomware, malware present that has an effect on our DIB partners, in this case, then again, it would be information sharing of indication of compromise with the incident response through those primary organizations, and also emphasizing with our partners as we continue to operate in cyberspace what was emphasized in the National Security Council memo on the 2nd of June, of treating this type of threat, it is more than

information loss. This is a continuity of business operations threat. And if you approach it from that perspective, I think then our corporations and our partners in industry would then have a different mental model as they approach their defense.

Senator ERNST. Thank you for that. And, General Kennedy, while you have the floor, there are a number of high- and low-tech common operating platforms like Windows, Amazon Web Services, where government, military, and civilian industries all conduct business. So how do we improve the DOD's capability to integrate our defense capabilities or simply conduct information sharing and coordination across these common operating platforms and industrial networks?

General KENNEDY. Senator, the approach that we are taking within the Department is an approach of looking at how we move from boundary defense primarily to one of a zero-trust type of environment, so we have more of a layered defense. And the critical aspects of that are how we encrypt our data at rest so that we can have access, how we understand the identity of the people that have access to the information within the networks, and also then how do you determine who is the data layer type of data responses that you put in place on your information, in addition to a level of resilience and boundary defense. Just as I lock my windows and doors on my house, although I know that is not going to keep out a persistent adversary if they truly want to come in, but then inside we have other types of active defense and persistence that I have. The same holds true in the information space.

Senator ERNST. Okay. And would that be then what we call cyber hygiene and just making sure that those services are enabled, or those defenses are enabled?

General KENNEDY. Yes, ma'am. There are some core practices of cyber hygiene that we practice in the Department that we emphasize with our DIB partners as well.

Senator ERNST. Okay. Yeah, I appreciate that, and my time has expired. Thank you, Ranking Member.

Senator ROUNDS. Thank you, and on behalf of the chairman, and once again, we do this on a bipartisan basis, and I really do appreciate the chairman allowing us to proceed with this process. He is in the middle of an infrastructure meeting right now and he is going to be here as soon as he can, but I will ask my questions and then we will move from there.

I want to begin by just kind of fleshing out a little bit about the role of the Department of Defense with regard to cyberattacks, and recognizing that the actual damage being done is in the forms of, in the case of the demand for a ransom to be paid, that occurs in the United States. But the actual attack itself originates, in many cases, in most cases, overseas.

We will have organizations, sometimes they are criminal organizations that are not part of a government, but may very well have found a safe harbor, so to speak, in another country. They will perpetrate a crime using computer systems, not only in their own country but in other countries, that the other owners of those other computers may not even know that their computers are being used. In doing so, finding and directing and attributing, really, the location of where the beginning of the attack is a challenge, but it is

one that we have become very good at. But in the meantime, the damage being done is the demand of ransomware being paid in the United States.

In an open, unclassified setting such as this, I wanted to explore a little bit the public policy side and the understanding that the Department of Defense really does play a role. I would ask you to comment on this scenario. In the beginning years of our country, we made it very clear that when pirates would attack shipping that was vital to the United States we actually created the Marine Corps, in a way, to actually go on out and find these private citizens who were acting as pirates, and we basically took them out, even though they had found a safe harbor in other sovereign countries. In doing so, we had extended and recognized that the defense of our country included the defense of our assets. We did this using our, at that time, Department of the Navy and the Marines, I am going to say the Department of Defense today.

I think it still holds true with regard to cyberattacks, and I think the Department of Defense clearly has a role to play in extending, and in protecting, and I think most citizens in the country believe that if someone from out of the country is going to be attack us, either critical infrastructure or, in the case of ransomware, if there is a way for our Department of Defense to either stop the incoming attacks or to respond accordingly, outside of our country to those incoming attacks, it would seem to be appropriate to do so, recognizing that this is not normal just stealing of information and espionage. This is a demand for payment or this is a direct attack on property within the United States.

Secretary Eoyang, would you care to comment and share your thoughts on whether or not you would agree with my assessment or my analogy today?

Ms. EOYANG. Senator Rounds, a very much appreciate your analogy to piracy because I have actually been thinking a lot about the development of international law and piracy as it relates to cybersecurity, and I think it is a very instructive one for us, as a nation.

One of the challenges that we saw with piracy is that territories at that time were either unwilling or unable to do anything about the threats that emanated from their territory. I think this is a very important question for us to be asking now, as we see these cyber actors who are operating outside the United States. Are they operating from territory where the host nation is unable to be able to do anything about it, in which case we need to focus on how we build capacity, how we build relationships with allies and partners, how we ensure that they understand the severity of the problem and are willing to cooperate with us in bringing those perpetrators to justice as part of a whole-of-government effort, or in those cases where there are nations that are unwilling—unable is one thing, unwilling is another—and when they are unwilling, then that poses a diplomatic challenge, and a national security challenge, and we have seen the President ask that question directly of a territory where we have seen a number of malicious cyber actors using a safe haven for their activity to victimize countries around the world, and to make very clear that they have a choice to make about whether or not they are willing to do anything about this, and that they will be held accountable for being unwilling to do so.

So I think it is an apt analogy in this space. I do think international law has evolved somewhat since the days of piracy, or at least I hope so, and we need to be able to think about that analogy in the context of technology and the complicated legal issues that arise.

Senator ROUNDS. Thank you. We do have with us, by Webex, Senator Blackburn, and at this time I would ask Senator Blackburn, on behalf of Chairman Manchin, if she would like to ask questions.

Senator BLACKBURN. Yes indeed, Senator Rounds. Thank you so much for that.

Ms. Eoyang, a couple of things that I wanted to ask you about. I agree with you when you talk about our allies and the way we focus on that. Let me bring that back home just a touch.

Senator Rosen and I have introduced a bipartisan Civilian Cyber Security Reserve Act, and this would establish a pilot that you would see between DOD and DHS that would have some cybersecurity-trained civilian personnel to ensure that we have the talent that we are going to need for rapid response and to address some of these vulnerabilities that currently exist.

So from your perspective, do you feel like that we have enough in the Federal Government, do you think we have enough of a cyber-literate workforce? Then secondly, would a civilian cybersecurity reserve force multiply the capacity that we have currently at DOD and DHS when it comes to responding to these attacks, or either being able to forestall some of those attacks?

Ms. EOYANG. Senator Blackburn, thank you for that, and I think you are certainly onto something when it comes to the capacity of the workforce. Certainly this is a national challenge. We have a cybersecurity literacy challenge not just for the Department but for the Nation, and so focusing on training, focusing on developing that workforce I think is very important. I cannot speak to the specifics of the particular legislation, but that is certainly something we would want to take a look at, and we thank you for thinking creatively about how we can solve this problem for the nation.

Senator BLACKBURN. Do you feel like that you have the authorities that are necessary for you there at DOD, do you have what you need to require or to push, or even support a whole-of-government response when it comes to ransomware attacks, or are there additional authorities that you would need in order to have a rapid response?

Ms. EOYANG. Senator, the Department, at this time, has all the authorities that it needs, and we really appreciate some of the legislative fixes that Congress has provided to us previously, and I am happy to address the ways in which we use those authorities in the closed session.

Senator BLACKBURN. Okay. Thank you. Another area that Senator Rosen and I have decided to tackle is to look at developing an emerging technology qualification program, because our warfighters are not going to change the way they fight unless we change the way they think and the way they approach problem-solving, and the way they pull technology into that. We really see this as we are looking at artificial intelligence, as we are looking at autonomous vehicles, as we are looking at the more widespread

utilization of 5G, and how you integrate that into modern-day warfare.

So would an emerging technology qualification that helps to identify talent to build a force, would that be helpful to you all?

Ms. EOYANG. Senator, again you are prescient in thinking about the ways the Department needs to incorporate technology into the way that we operate. I think we see this as two different challenge. One is how do we make sure that people generally are aware of technology and how it needs to be used for the Department, but then there is the separate track of how we think about those who operate technology and operate in that domain, and those are two different levels of expertise and education.

We are in the process right now of reviewing education and training requirements for cyber, for the Department, and we would be happy to look at how this might fit into that plan. Thank you.

Senator BLACKBURN. Well, that would be helpful to us. I honestly believe if we can begin to make some of these changes of how we are going to use this data, how we are going to crunch these data sets, and how they are going to help us with doing predictive analysis and then bringing that to bear, that it is going to help you all with the way you approach this and the way we deal with our allies and the way we defeat our enemies. So thank you very much for being with us today.

[Pause.]

Senator ROUNDS. (Mic was off). Second of all, I would simply say that I would look forward to a closed session discussion as well, and the chairman has indicated that he will meet us there for that.

So at this time, unless you have any further comments that you would like to make to the committee, if there are any I would accept them at this time.

[No response.]

Senator ROUNDS. If not, we will close. On behalf of Chairman Manchin we will close the open session and we will meet you in the SCIF for the closed portion of the session. This subcommittee meeting is adjourned.

[Whereupon, at 2:42 p.m., the Committee adjourned.]

[Questions for the record with answers supplied follow:]

QUESTIONS SUBMITTED BY SENATOR JACKY ROSEN

CYBER WORKFORCE AND READINESS

1. Senator ROSEN. Ms. Eoyang, in the midst of unprecedented ransomware attacks like those on Colonial Pipeline and JBS meatpacking, the United States is expected to face a shortage of 3.4 million skilled technical workers by next year, with particularly large gaps in cybersecurity. What are you doing to ensure Department of Defense (DOD) has the available workforce to strengthen our nation's ability to withstand and respond to cyber-attacks?

Ms. EOYANG. [Deleted.]

2. Senator ROSEN. General Kennedy, could you outline CYBERCOM's current and future workforce needs? And could you tell us how you work with the services to standardize the type of cyber personnel hired, how they are trained, and the equipment used to sustain DOD's cyber readiness?

General KENNEDY. [Deleted.]

3. Senator ROSEN. General Kennedy, how might having a surge capacity of trained personnel available support your ability to execute the CYBERCOM mission?
General KENNEDY. [Deleted.]

CRIMINAL CYBER THREATS

4. Senator ROSEN. Ms. Eoyang, as the recent ransomware attacks on Colonial Pipeline and JBS meatpacking demonstrate, the line between nation-states and criminal enterprises seeking to do us harm is increasingly blurry and complicates our ability to attribute attacks. How does DOD distinguish between state actors and government-linked criminal enterprise actors capable of conducting cyber-attacks on U.S. critical infrastructure?
Ms. EOYANG. [Deleted.]

5. Senator ROSEN. Ms. Eoyang, should DOD conduct offensive cyber operations against foreign criminal enterprises targeting our critical infrastructure? How do you delineate between DOD and Department of Justice (DOJ) when deciding who is responsible for pursing foreign-based cyber criminals?
Ms. EOYANG. [Deleted.]

6. Senator ROSEN. General Kennedy, do you have the authorities and capacity necessary to quickly adapt to the evolving cyber threat environment, as that line between nation-states and criminal enterprises becomes increasingly blurred?
General KENNEDY. [Deleted.]

INTERAGENCY CYBER COORDINATION

7. Senator ROSEN. General Kennedy, since CYBERCOM doesn't have the authority to operate in domestic cyberspace, how is DOD coordinating with Department of Homeland Security (DHS) to specifically track and respond to malicious ransomware activity?
General KENNEDY. [Deleted.]

8. Senator ROSEN. Ms. Eoyang, as you know in 2018, DHS and DOD signed a memorandum of agreement to spell out how the two departments will work together to secure America's cyber networks. Is the agreement enabling adequate joint operational planning and mission coordination in light of recent ransomware attacks?
Ms. EOYANG. [Deleted.]

QUESTIONS SUBMITTED BY SENATOR MARSHA BLACKBURN

CIVILIAN CYBER RESERVE

9. Senator BLACKBURN. Ms. Eoyang, would a civilian cybersecurity reserve force have the potential to provide the U.S. with a sufficiently large enough cyber-literate workforce to address ransomware and other cyber security concerns? What would be an appropriate size and scope for such a force?
Ms. EOYANG. [Deleted.]

10. Senator BLACKBURN. Ms. Eoyang, would a civilian cybersecurity reserve force multiply the capacity for agencies like DOD and DHS to address ransomware attacks?
Ms. EOYANG. [Deleted.]

11. Senator BLACKBURN. Ms. Eoyang, would an emerging technology qualification program help identify the talent necessary to build a force that can respond more rapidly and resiliently to ransomware attacks?
Ms. EOYANG. [Deleted.]