[H.A.S.C. No. 117–32]

# HEARING

ON

# NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2022

AND

# OVERSIGHT OF PREVIOUSLY AUTHORIZED PROGRAMS

BEFORE THE

## COMMITTEE ON ARMED SERVICES
## HOUSE OF REPRESENTATIVES
ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

---

SUBCOMMITTEE ON CYBER, INNOVATIVE TECHNOLOGIES, AND INFORMATION SYSTEMS

ON

# OPERATIONS IN CYBERSPACE AND BUILDING CYBER CAPABILITIES ACROSS THE DEPARTMENT OF DEFENSE

---

HEARING HELD
MAY 14, 2021

---

U.S. GOVERNMENT PUBLISHING OFFICE
45–604 WASHINGTON : 2021

SUBCOMMITTEE ON CYBER, INNOVATIVE TECHNOLOGIES, AND INFORMATION SYSTEMS

JAMES R. LANGEVIN, Rhode Island, *Chairman*

RICK LARSEN, Washington
SETH MOULTON, Massachusetts
RO KHANNA, California
WILLIAM R. KEATING, Massachusetts
ANDY KIM, New Jersey
CHRISSY HOULAHAN, Pennsylvania, *Vice Chair*
JASON CROW, Colorado
ELISSA SLOTKIN, Michigan
VERONICA ESCOBAR, Texas
JOSEPH D. MORELLE, New York

ELISE M. STEFANIK, New York
MO BROOKS, Alabama
MIKE GALLAGHER, Wisconsin
MATT GAETZ, Florida
MIKE JOHNSON, Louisiana
STEPHANIE I. BICE, Oklahoma
C. SCOTT FRANKLIN, Florida
BLAKE D. MOORE, Utah
PAT FALLON, Texas

JOSH STIEFEL, *Professional Staff Member*
SARAH MOXLEY, *Professional Staff Member*
CAROLINE KEHRLI, *Clerk*

# CONTENTS

# OPERATIONS IN CYBERSPACE AND BUILDING CYBER CAPABILITIES ACROSS THE DEPARTMENT OF DEFENSE

---

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ARMED SERVICES,
SUBCOMMITTEE ON CYBER, INNOVATIVE
TECHNOLOGIES, AND INFORMATION SYSTEMS,
*Washington, DC, Friday, May 14, 2021.*

The subcommittee met, pursuant to call, at 11:03 a.m., in room 2118, Rayburn House Office Building, Hon. James R. Langevin (chairman of the subcommittee) presiding.

## OPENING STATEMENT OF HON. JAMES R. LANGEVIN, A REPRESENTATIVE FROM RHODE ISLAND, CHAIRMAN, SUBCOMMITTEE ON CYBER, INNOVATIVE TECHNOLOGIES, AND INFORMATION SYSTEMS

Mr. LANGEVIN. The subcommittee will come to order.

Before I begin my opening statement, I want to welcome our witnesses. I am just going to read some technical information since this is a hybrid hearing and some members will be joining us remotely.

Welcome to today's hearing, "Operations in Cyberspace and Building Cyber Capabilities across the Department of Defense." We have convened.

This is a hybrid hearing, and we are joined by members who are participating remotely. Members who are joining remotely must be visible on screen for the purposes of identity verification, establishing and maintaining a quorum, participating in the proceeding, and voting. Those members must continue to use the software platform's video function while in attendance unless they experience connectivity issues or other technical problems that render them unable to participate on camera. If a member experiences difficulties, they should contact the committee staff for assistance.

Video of members' participation will be broadcast in the room and via the television internet feeds. Members participating remotely must seek recognition verbally, and they are asked to mute their microphones when they are not speaking. Members who are participating remotely are reminded to keep the software platform's video function on the entire time they attend the proceeding. Members may leave and rejoin the proceeding. If members depart for a short while for reasons other than joining a different proceeding, they should leave their video function on. If members will be absent for a significant period or depart to join a different proceeding, they should exit the software platform entirely and then rejoin it if they return.

Members may use the software platform's chat feature to communicate with staff regarding technical or logistical support issues only. I have designated a committee staff member to, if necessary, mute unrecognized members' microphones to cancel any inadvertent background noise that may disrupt the proceeding.

So I would like to welcome our witnesses, General Paul Nakasone, the Commander of U.S. Cyber Command and the Director of National Security Agency, and Mieke Eoyang, the Deputy Assistant Secretary of Defense for Cyber Policy. Welcome to you both.

In past hearings, General Nakasone has been joined by the Assistant Secretary of Defense for Homeland Defense and Global Security. However, with the challenges faced in that role, we are thankful that Ms. Eoyang is able to step in, and the committee appreciates your cooperation and collaboration.

So it is truly incredible how much has changed since our last cyber posture hearing on March 4, 2020. The world has been upended by a pandemic, changing the lives of literally every person on the planet. In the realm of cyber matters, the men and women of the Department of Defense, including our soldiers, sailors, airmen, Marines, and guardians, have had no respite, continuing to operate and defend Americans' interests in cyberspace.

Despite the pandemic, our adversaries and competitors have not let up their cyber campaigns. In the last 6 months alone, the media has reported almost nonstop on arguably some of the most significant cyber incidents ever to affect our Nation, from SolarWinds to Hafnium to, just in the last week, the attack against Colonial Pipeline by the DarkSide criminal collective. So if there were any doubters that cyberspace is an active and contested warfighting domain, I would hope that the last year has changed those perspectives.

Yet, incredibly, it still appears to this committee that cyber does not always have the focus for much of the Department's senior uniformed and civilian leadership that it requires, despite our forces engaging adversaries in this domain every single day. I point this out. Recently, the Air Force removed cyber from its mission statement, even though a report from the Office of Secretary of Defense concluded that the inclusion of cyber in the Air Force mission statement is the single reason why Air Force personnel have vastly outpaced other services in pursuing cyber-related certifications.

Candidly, it is frustrating that the people in this room, both members and witnesses, seem to be fighting an uphill battle to put cyber front and center in the Department. Out of five officially recognized warfighting domains, the senior civilian official for air, sea, land, and space domains are military service secretaries. Yet, with all due respect to Ms. Eoyang and her spectacularly overworked team, the senior civilian for cyber is four rungs lower than her counterparts overseeing other domains.

So we also have to account for the ways in which cyberspace operations occur within and affect the information environment. One of the most illustrative examples of how the Department's structure can hinder rather than enable operations is its own organization chart. The DOD's Joint Publication 313 notes that cyberspace is one of many information-related capabilities, designed to affect the information domain alongside psychological operations and

electromagnetic spectrum operations. Yet each of the information-related capabilities is handled by a separate entity and siloed within the Department, ensuring that we cannot leverage our capabilities to the maximum extent possible. This needs to change.

In our current age of great power competition, conflict in the "gray zone" below the level of armed conflict has never been more relevant to our strategic thought. For numerous reasons, challenges with attribution, easily altered payloads, and ease of proliferation, cyber is the ideal tool for the gray zone conflict. The information domain, including cyberspace, is where our forces are engaged against our adversaries daily.

As the Nation comes to realize that this domain is as important as any other, we need the Defense Department to adapt to ensure that any conflict with adversaries remains in the information space as much as possible and never moves into the kinetic realm.

As we push the Department to adapt toward the information environment, congressional oversight has never been more necessary. It is the mechanism by which we monitor the activities of the executive branch and ensure compliance with relevant statute. While I understand that transitions can result in disconnects or misunderstandings, I anticipate hearing from the committee staff that any issues that may have arisen will be quickly resolved to our satisfaction. So I am happy to add detail in private, but we will leave it at that for now.

So, with that, I now want to thank our witnesses again for appearing before us today. As a reminder, after this open session, we will move to the CVC auditorium for a closed, member-only session.

With that, I want to turn now to Ranking Member Gallagher for his remarks.

[The prepared statement of Mr. Langevin can be found in the Appendix on page 33.]

**STATEMENT OF HON. MIKE GALLAGHER, A REPRESENTATIVE FROM WISCONSIN, SUBCOMMITTEE ON CYBER, INNOVATIVE TECHNOLOGIES, AND INFORMATION SYSTEMS**

Mr. GALLAGHER. Thank you, Mr. Chairman. And thank you to General Nakasone and Ms. Eoyang for being here today.

Cyberspace is the ultimate gray zone in which operations often do not fit neatly into either traditional kinetic warfighting or nontraditional activities. Adversaries like China and Russia, as well as nonstate actors, are continuously exploiting the gray zone and probing our networks and exploiting our vulnerabilities in cyberspace. I mean, just in recent months, we have had SolarWinds. We have had Microsoft Exchange. We had Russian cyber actors last week shut down a major U.S. pipeline, highlighting the cyber threat posed to our critical infrastructure from actors anywhere in the world and how actors all over the world can reach out and touch all of our constituents, no matter where our districts are.

I just would say, though our cyber adversaries are diffuse and evolving and they prove time and again that our cyber networks are only as strong as the weakest link, our operations and capabilities have also evolved, in large part due to the work of this subcommittee and the leadership of General Nakasone at U.S. Cyber Command and, in particular, General, the input that you provided

to the Cyberspace Solarium Commission over the last 2 years, which took up a lot of Representative Langevin and my work over the last couple of years.

But as we continue to harden our networks and improve our capabilities, the President's budget must focus on modernizing DOD's [Department of Defense's] platforms. We must consider cutting legacy platforms out of date for modern conflict and investing in emerging technologies in cyber. And I believe I speak for everyone here when I say I hope to see a budget that recognizes the importance of our Cyber Mission Force; invests in necessary cyber infrastructure, including technology and human capital; highlights necessary cyber authorities; and really pushes the Department out of its silos and into a streamlined structure that prioritizes cyber agility and responsiveness.

Our Cyber Mission Force has also matured, but we must continue to identify cyber talent and train, equip, and support our cyber force to improve our capabilities across the cyber continuum and maintain superiority over hostile cyber actors. So we took a lot of pivotal steps in this direction in last year's NDAA [National Defense Authorization Act], and I know we will continue to make progress towards our cyber goals again this year, but the fundamental shift in thinking about cyber will take more than just directives in the NDAA. It will require leaders at DOD and throughout the government and in Congress to think strategically and acknowledge that cyber is now the critical domain to every facet of our national security.

And with that, Mr. Chairman, I look forward to hearing from our witnesses today, and I yield back.

Mr. LANGEVIN. Thank you, Ranking Member Gallagher, for your remarks.

With that, I will now turn it over to Ms. Eoyang and General Nakasone for 5 minutes of remarks each.

Ms. Eoyang, you are recognized. You may proceed.

**STATEMENT OF MIEKE EOYANG, DEPUTY ASSISTANT SECRETARY OF DEFENSE FOR CYBER POLICY, OFFICE OF THE UNDER SECRETARY OF DEFENSE FOR POLICY**

Ms. EOYANG. Thank you, Chairman Langevin, Representative Gallagher, and members of the committee. I am pleased to be here with General Nakasone, the Commander of U.S. Cyber Command, to report the progress that the Department of Defense has made in achieving the Department's objectives in cyberspace.

This afternoon, I am testifying in my role as the Deputy Assistant Secretary of Defense for Cyber Policy. In that role, I am responsible for advising the Secretary and Deputy Secretary on cyberspace policy and the development of the Department's cyber strategy and other cyberspace policy.

Congress has demonstrated that it views cyber defense as a priority through not only its legislative work, but through Member service on the Solarium Commission. And for that, we are grateful for your ongoing support for this crucial issue in a broad and bipartisan manner.

To start, I would like to offer our perspective on the current global strategic context. As you note, 2020 was a year of turmoil, with

a global pandemic drastically altering our day-to-day reality and increasing our dependence on the internet. Our adversaries took notice of our growing reliance on technology. Cyber criminals and nation-state actors alike took advantage of COVID–19 by unleashing ransomware on healthcare facilities, targeting vaccine production and supply chains, exploiting fears to spread disinformation, and even disrupting pipeline companies.

As a result, the cyberspace domain is both more important and more contested than it has been in recent memory. Enhancing the security of cyberspace, both in the United States and around the world, is a top priority as the President's Interim National Security Strategic Guidance prioritizes cybersecurity and pledges to expand investments needed to defend the Nation against malicious cyber activity and cyberattack.

Our competitors are using their cyber capabilities to seek political, economic, information, and military advantages, and to undermine our security by engaging in malicious cyber activity. The DNI [Director of National Intelligence] assesses that cyber threats from nation-states—particularly China, Russia, Iran, and North Korea—and their surrogates will remain acute, both in day-to-day competition and to seek advantage in armed conflict.

As Secretary Austin said at his confirmation hearing in January, China is the pacing threat for the Department, including in cyber operations. China uses cyber operations to erode U.S. military overmatch and economic vitality, stealing U.S. intellectual property and research. Chinese malicious cyber activity continues to this day.

Russia also continues to be a highly sophisticated and capable adversary, integrating malicious cyber activities, including espionage, influence operations, and mutually reinforcing ways to achieve its objectives. They engage in a wide range of malign cyber activities, including attempts to interfere with U.S. elections, spreading ransomware such as NotPetya, efforts to disrupt the postponed Tokyo Olympics, and the most recent SolarWinds attack.

In addition to using cyberspace as an offensive tool, China and Russia view the internet as a mechanism to control and intimidate their own populations. While the United States advocates for an open, interoperable, secure, and reliable internet, China and Russia have created and employed a digital authoritarian model using their technological and cyberspace capabilities to manipulate narratives, repress free speech, surveil their citizens, and quash dissent domestically. China seeks to export digital authoritarianism to other repressive regimes, remaking the internet in its image.

Beyond China and Russia, we remain concerned about the cyber threat posed by Iran and North Korea. And further, nation-state actors, such as criminals, terrorists, and violent extremists, continue to leverage the internet to advance their agendas. The line between nation-state and criminal actors is increasingly blurry as nation-states turn to criminal proxies as a tool of state power, then turn a blind eye to the cyber crime perpetrated by the same malicious actors. This is a common practice for Russia, whose security services leverage cyber criminals while shielding them from prosecution for crimes they commit for personal benefit.

We have also seen some states allow their government hackers to moonlight as cyber criminals. This is not how responsible states

behave in cyberspace, nor can responsible states condone shielding of this criminal behavior.

The President has made clear also the need to strengthen our alliances. The Department is driving new approaches to do that, and we continue hunt forward operations with partners even during pandemic and cyber exercises, such as Cyber Flag, to help our allies prepare for adversary actions.

President Biden is currently conducting a review of national strategy, which will culminate in the issuance of two key documents: the National Security Strategy and the National Cyber Strategy. The President's guidance will inform our own upcoming defense-level review of the National Defense Strategy and follow on the Department's second ever Cyber Posture Review, which will evaluate our ability to execute national and departmental-level strategies to achieve our goals in cyberspace. We look forward to delivering the strategy and posture review to Congress once they are completed.

Thank you for the opportunity to appear before you today, and I look forward to the members' questions.

[The prepared statement of Ms. Eoyang can be found in the Appendix on page 36.]

Mr. LANGEVIN. Thank you, Ms. Eoyang.

And, General Nakasone, you are now recognized for 5 minutes.

**STATEMENT OF GEN PAUL M. NAKASONE, USA, COMMANDER, U.S. CYBER COMMAND, AND DIRECTOR, NATIONAL SECURITY AGENCY**

General NAKASONE. Chairman Langevin, Ranking Member Gallagher, and distinguished members of the subcommittee, I am honored to be here and testify beside Secretary Eoyang and represent the men and women of U.S. Cyber Command.

Three major incidents over the past 6 months demonstrate the importance of cyber security to our Nation. Well-resourced and sophisticated adversaries are exploiting gaps in the Nation's ability to monitor U.S. cyberspace infrastructure while conducting operations from within the boundaries of the United States.

The SolarWinds incident occurred through the highly skilled means of an adversary against a U.S. company supply chain. At nearly the same time, the server hack associated with Microsoft Exchange showcased the ability of another adversary to exploit vulnerabilities and attack systems around the world. The Colonial Pipeline ransomware attack also demonstrate a growing trend of companies and even government agencies being held hostage by malicious cyber actors. These cases demonstrate the broadening scope, scale, and sophistication employed by some adversaries.

The United States Government, in tandem with industry partners, must improve its defensive posture to prevent and/or minimize the impacts, while contesting and defeating those who would exploit such vulnerabilities and target American companies and citizens. Cybersecurity is national security.

Over the past year, I emphasized the importance of defending the election against foreign interference. We did this through the Election Security Group, a combined team from U.S. Cyber Command and the National Security Agency. We built on lessons from

earlier operations and honed partnerships with the Federal Bureau of Investigation and the Department of Homeland Security Cybersecurity and Infrastructure Security Agency, sharing information with those who needed it as fast as possible. We also worked with the National Guard Bureau to create a mechanism that enabled Guard units to share information about incidents quickly, easily, and uniformly.

U.S. Cyber Command [CYBERCOM] conducted more than two dozen operations to get ahead of foreign threats before they interfered with or influenced our elections in 2020. I am proud of the work the command and the Election Security Group performed as part of a broader government effort to deliver a safe, secure 2020 election.

CYBERCOM is building on recent guidance from the Department, seeking to promote readiness, improve training, and attract high-end talent. The cyberspace environment has changed significantly over the past years. To your point, Chairman, even over the past 14 months, we have seen a tremendous difference in the environment. Adversaries are demonstrating a changed risk calculus. They are undertaking malign activities in cyberspace at greater scope, scale, and sophistication. They desire to take on the U.S. in cyberspace below the level of armed conflict.

To defend our security and our interests in this environment, U.S. Cyber Command must continue to adapt, innovate, partner, and succeed against such adversaries. The men and women at U.S. Cyber Command look forward to working with this committee and are truly grateful for the support Congress has given to our command.

Again, thank you for your support, and I look forward to your questions.

[The prepared statement of General Nakasone can be found in the Appendix on page 54.]

Mr. LANGEVIN. Thank you, General Nakasone, Ms. Eoyang, for your testimony here today. Before we begin procedure questions, I just want to thank you again for your commitment to the national security of the United States. And I wanted to just point out as a matter of personal privilege, we all recognize that our Nation is one giant melting pot, and I think diversity is something to be celebrated. And I think this may be an historic first for this committee in that we have two members of the AAPI [Asian Americans and Pacific Islanders] community testifying before us at the same time. So pretty cool to note. And thank you again.

[Inaudible.]

Mr. LANGEVIN. Very good.

I want to thank you both for being here, again, for your testimony, your commitment to the national security of the United States, and thank you for your remarks.

We are going to now proceed with questions. Each member will be recognized for 5 minutes, beginning with myself.

And, Ms. Eoyang, I want to start with you, if I could. So the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict is responsible for information operations, but the Assistant Secretary of Defense for Homeland Defense and Global Security is responsible for cyberspace operations. Can you explain the

logic as to why two separate chains are established for operations within the same information environments?

Ms. EOYANG. Mr. Chairman, I appreciate the question here. I think—I am not sure that I can give the full history on how that evolved from the Department's perspective in terms of why those two things are in separate silos. Agree that there is a fair amount of overlap there, but as you may know, the PSYOPS [psychological operations]/information ops had traditionally been held in the special operations community. And as cyberspace grew up, it went through a number of evolutions and has found itself within the Homeland Defense and Global Security arena in part because of the focus, I think, on the homeland security aspects of cybersecurity. But, certainly, there are some coordination challenges in the division between the two.

Mr. LANGEVIN. So, to that point, you know, how do you and the Deputy Assistant Secretary of Defense for Special Operations and Counterterrorism, a position that owns the information and operations portfolio for OSD [Office of the Secretary of Defense] Policy, coordinate and collaborate?

Ms. EOYANG. I am in regular communication with my colleagues, and we are collaborating at all levels between our two offices, Mr. Chairman.

Mr. LANGEVIN. That is something that we are going to have to continue to work on, I think too, though.

General Nakasone, one of the Cyberspace Solarium Commission's key outstanding questions was whether the Cyber Mission Force, designed now 9 years ago, was properly sized. You may remember that I asked you about this at last year's hearing. We spoke about this yesterday when you and I met also in my office, but last year, you had replied that you needed more relevant data.

And without discussing the contents of the President's budget before its release, can you tell us about whether you acquired the information necessary to make a decision on the size of the force and what insights you gleaned from this information?

General NAKASONE. Chairman, thank you. We do have the data. And again, to your point, not to get ahead of the budget submission, but in general terms, I would anticipate that as we lay out the case, we have to look at some critical elements that will influence the future size of the Cyber Mission Force, now 133 teams. In the future, we have to account for the growing importance of space. I think we have to account for the importance of what we are seeing with malign cyber actors, whether or not it is Russian cyber actors, Chinese cyber actors, Iranian cyber actors, and their intent.

And I think the last piece is that we are in a period of strategic competition, and I think the word is "competition." So we have to have that balance of, not only what we are going to support our fellow combatant commands if conflict was to break out, but, also, if our adversaries are operating below the level of armed conflict every single day, what type of force do we need to be able to ensure that we can counteract that, much in the same way that we have done in our support to the national elections.

Mr. LANGEVIN. Thank you, General. And, recently, one of your subordinate commands, Army Cyber Command, established an Information Warfare Operations Center. At nearly the exact same

time, U.S. Army Special Operations Command at Fort Bragg separately established an Information Warfare Center. So acknowledging that this is Army specific, it points to a wider issue about lack of clarity on mission sets and an absence of direction inside the Department. How do you distinguish what Cyber Command and its cyber focus subordinate commands do versus what Special Operations Command and its SOF [special operations forces]-centric subordinate elements do?

General NAKASONE. Chairman, I have a very, very close and enduring partnership with U.S. Special Operations Command under the leadership of General Rich Clark. We talk frequently on this.

To provide a bit of perspective on this, I see it as only natural that Special Operations Command, as they operate across all the different domains, also has the capability within cyberspace. I think the delineation is, you know, what is the focus of U.S. Special Operations Command, what is the focus of U.S. Army Cyber Command, what is the overall focus of U.S. Cyber Command. I think we have worked through that.

I think to your point, there is still work to do on our doctrine. We will continue to advocate for that work, but we all realize that it is more than, you know, just conducting one cyberspace operations. It is the entire information domain that we have to understand and be able to operate within.

Mr. LANGEVIN. Thank you, General.

I will hold there and turn to the ranking member for his questions now.

Mr. GALLAGHER. Thank you.

General, you mentioned the challenge in the Colonial Pipeline context of ransomware and criminal groups, and I think it is safe to say that challenge is only going to grow in the short term. Part of the problem that strikes me is an authorities problem. I would be curious, to the extent you can answer in open session, what tools you believe you have in your kit to get at that challenge. Because I believe you also mentioned that as NSA [National Security Agency] Director, you are limited in obviously monitoring domestic U.S. IT [information technology] infrastructure.

Do you think your CYBERCOM forces could be provided under DSCA [Defense Support to Civil Authorities] to DHS [Department of Homeland Security], for example, and used to conduct a sort of monitoring analysis under DHS authorities at least until DHS builds its own capabilities? How do we get at this in the short term while we sort of build out a longer term answer?

General NAKASONE. Ranking Member, I think to your initial point, it is really important to look at this as a broader element and how do we get after this criminal activity. I think this is a whole-of-government effort. In the United States, it is most appropriate that lead Federal agencies, obviously, Department of Homeland Security, Federal Bureau of Investigation. I don't think there is any problem with the authorities in terms of what it's stated out to do.

But as we look at ransomware and as we continue to peel this back, as we see criminal actors that are operating outside the United States, I think what the administration obviously is moving towards is how do we have a whole-of-government approach that

brings together our levers of power that includes diplomacy, and certainly our economic and, if necessary and if authorized, outside the United States, what the Department of Defense might do.

To your last point, Ranking Member, with regards to support for anything like this, well-established processes, as you know, Defense Support to Civil Authorities, and I think that those would be executed if lead Federal agencies needed to have that support.

Mr. GALLAGHER. Well, as we attempt to step back and look at it holistically, I think it is fair, at least with one lens, to look at it as not just as this attack isolated but as a Russia problem, right. And part of the problem is you have, at times, opaque relationships between the Russian Government and criminal groups.

Do we have the sufficient analytical capacity to tease out those relationships, make those distinctions? Is there more regional expertise that we need to apply to this problem? I would be curious to the extent—again, the extent you can answer in this session, how you think about those opaque relationships and our ability to better understand them.

General NAKASONE. Quite simply, I think about it in terms of how do I provide the most intelligence I can as the Director of the National Security Agency or Commander of U.S. Cyber Command that provides both a viewpoint on intent and capability of our adversaries. I think, you know, as any director of a combat support agency would share with you is we need to do more. And we can talk a little bit more in closed session today, but, again, I think that overall, we have work to do across U.S. Cyber Command and the National Security Agency.

Mr. GALLAGHER. And then finally, one of the Cyberspace Solarium Commission recommendations that we are working on right now is this concept of systemically important critical infrastructure, which this case obviously brings up. Do you support the idea of creating a codified relationship between the United States Government and critical functions?

General NAKASONE. Congressman, I would say I support anything that is going to ensure the security of our critical infrastructure and key resources. My experience has been with elections, but there are 16 other sectors. And I think that what the administration has laid out in the 100-day plan initially with regards to energy is a great start where we need to figure out how do we bring the whole parts of the government and, particularly important, how do we bring the private sector into a greater partnership to ensure that we have outcomes that will lead to greater resiliency and obviously security.

Mr. GALLAGHER. Thank you. I guess the clock doesn't count down when you are up this high on the dais, which is interesting. But in the interest of time, I will still yield back.

Mr. LANGEVIN. Well, we follow the lead of the chair and the ranking member on the full committee that the chair and ranking member of the subcommittee are not on the clock. But with that, I want to now thank you for your line of questions, and I also want to commend the ranking member for his leadership as co-chair of the Cyberspace Solarium Commission. I was proud to serve on the Commission with you, and really appreciate your commitment to

our national security. That report went a long way, I think, toward getting us to a stronger place in cyberspace.

With that, I want to recognize now Mr. Larsen for 5 minutes.

Mr. LARSEN. Thank you, Mr. Chair. Ranking Member Gallagher will see the clock ticking now that we are on the others.

General Nakasone——

Mr. LANGEVIN. I am watching it very closely.

Mr. LARSEN. General Nakasone, section 1729 of the NDAA required a conference and evaluation by the SECDEF [Secretary of Defense] basically on how to use the cyber capabilities of the National Guard. Do you have an update on the status of that evaluation?

General NAKASONE. Congressman, I would have to defer to the Secretary if she has one. I personally don't have one, but certainly we can take that for the record, if necessary, Congressman.

[The information referred to can be found in the Appendix on page 65.]

Mr. LARSEN. That is good. Thanks. Perhaps, Secretary?

Ms. EOYANG. Mr. Larsen, I just wanted to clarify. Since we have had a number of congressional interest provisions on National Guard, exactly which of the provisions are we referring to?

Mr. LARSEN. Cyber capabilities and interoperability of the National Guard. It requires a comprehensive evaluation by SECDEF on the mechanisms by which the Department is able to improve the utilization of cyber capabilities resident in the National Guard.

Ms. EOYANG. Our understanding is that we should have an answer for you later this summer on that topic.

Mr. LARSEN. All right. I have a list of questions that are really more appropriate for a different setting, but I do want to ask—where did my question go here? Oh. Perhaps for General Nakasone. Can you highlight, perhaps, how you are leveraging commercial threat information providers, and then how do you share that information?

General NAKASONE. Congressman, we have a number of different relationships with the private sector. Sincerely, in terms of being able to understand better the vulnerabilities that exist in our private—in the same private companies is critical for us. This is obviously sometimes a means upon which we have early alerts to problems that might exist in the private sector.

At the command, I assure you that any type of data is looked at, screened, and carefully evaluated for U.S. persons data. And if by rare occasion that we do have that, we will certainly minimize, and we have processes and procedures upon which to deal with that.

Mr. LARSEN. And then in last year's NDAA, we authorized some language that has CYBERCOM participating and contributing to the Joint Cyber Planning Office at CISA [Cybersecurity and Infrastructure Security Agency]. How will you plan to implement that provision?

General NAKASONE. Congressman, we have had some experience in working very closely with CISA, and it began with the election. One of the things that I directed were a series of planners to go over and to work closely with CISA as we put together our strategy for securing the 2020 election. What we found is that this truly is value added. The way that we do planning operations is something

that I think is very helpful as we take a look at broad-based problems like election security. We are going to continue to support that. That has been an element that the Secretary has emphasized to us, and in very close partnership, obviously, with CISA. So this will be just the first of many steps as we go to work this closely.

Mr. LARSEN. All right. And one final question, and this is kind of related to the operations of NSA. But Congress has just been notified, General, that there was a decision made to close the NSA's onsite childcare center, creating a tough situation for employees or parents. Can you speak a little bit about that decision?

General NAKASONE. Congressman, we were alerted several weeks ago by the private company that runs the childcare center that they were intending to close at the end of June. We have spent the past several weeks doing a series of different activities. First of all, working closely with those families that are affected to ensure that they have information and leads to other childcare facilities within the area. Secondly, taking a look at mid- and long-term plans. As you know, we are in the midst of a fairly large construction work at Fort Meade, and so this was, I think, part of the impetus where the private company decided to close at the end of June. But, clearly, it begins with our engagement with the families that are affected, and it has my personal interest, sir.

Mr. LARSEN. Well, I am glad to hear that. Pre-pandemic, we had a childcare crisis in the country. The pandemic has exacerbated that. We have taken action through the American Rescue Plan to try to alleviate some of that, but we don't need to deliberately add to the problems of folks. So thanks for updating me.

I yield back.

Mr. LANGEVIN. Right on time, Larsen. Very good. I thank the gentleman for his line of questions.

Mr. Rogers is now recognized for 5 minutes.

Mr. ROGERS. Thank you, Mr. Chairman.

General Nakasone, the threats that you have described that we face from adversaries in the cyber world, how imminent are they?

General NAKASONE. Well, I think—Congressman, to your point, I think that what we are seeing right now are adversaries that are increasing their scope, scale, and sophistication. What do I mean by that? I mean that it no longer is just a simple guessing of passwords or perhaps a phishing email that our adversaries are starting to use. They are using things like supply chain operations, as we saw in SolarWinds, or they are utilizing zero-day vulnerabilities, those vulnerabilities that the provider doesn't know about but that an adversary can utilize, as we saw with Microsoft.

And so this is the world in which our adversaries are operating below the level of armed conflict trying to do three primary things: They are looking to steal our intellectual property; they are looking to, you know, steal our personal identification, whether or not that is, you know, passwords or that is Social Security numbers or that is email addresses; and they are looking to conduct interference and influence operations either against our electoral processes or within our economy.

Mr. ROGERS. Are they looking to do that in the future or are they looking to do that now?

General NAKASONE. Oh, they are doing that now, Congressman.

Mr. ROGERS. Yeah. So you would urge this committee to act with haste on whatever you are going to recommend for us to do in this year's NDAA?

General NAKASONE. Congressman, I would certainly focus internally, and I am going to be ensuring that whatever we are doing, we are doing at a pace that is accelerated.

Mr. ROGERS. Well, my point is, if you are going to need any additional statutory authority, you need to let us know, because we are ready to act.

I talked to you yesterday about the committee's welcoming of the recommendation from the National Defense Strategy Commission, the suggestion of a Digital Service Academy to help train up personnel to take on this challenge, and you mentioned that you also had a retention issue. Can you talk more to the committee about the challenges you face with retention of quality personnel in this area?

General NAKASONE. So, Congressman, you asked me yesterday about how the services were doing in terms of providing us military and civilian members to outfit our 133 teams, and my response is they do a spectacular job of doing that. It is not the fact that our services don't do a great job in recruiting and the fact that they do a great job in training, and then we develop them at U.S. Cyber Command. At the end of the day, what I think the most about is how do I retain this superior force, particularly those individuals that are so much more capable than their peers. And so retention is something that means a lot to us.

And, you know, one of the things that I continue to work closely with the services is how do we ensure that the best of the best decide to stay with us, or if they are going to leave us, how do they become part of our Reserve Component, our National Guard, our Reserve force, or how do they continue to contribute within the broader U.S. Government.

Mr. ROGERS. Do you think you are going to need some statutory leeway to be able to accommodate that challenge?

General NAKASONE. So this is a point where that we will work closely, obviously, with the Joint Staff and the Office of Secretary of Defense to come back with some recommendations, because I think that we have a growing amount of data that can be helpful here for the Department to make an overall request.

Mr. ROGERS. Great. Well, I look forward to receiving that, and thank you for your service.

I yield back.

Mr. LANGEVIN. Thank you, Mr. Rogers.

I will next go to Mr. Moulton. Welcome back from paternity leave, and congratulations, Seth. And you are now recognized for 5 minutes.

You are on mute.

Mr. MOULTON. How is that?

Mr. LANGEVIN. Go right ahead. You are recognized.

Mr. MOULTON. Sorry. I was unmuted, but I was on the wrong microphone, apparently. My apologies.

Mr. Chairman, thank you for your remarks. It is good to be back.

And to build off some of your comments on the need for coordination between info operations and cyber operations, General Naka-

sone, a few weeks ago the DC police was attacked by the hacking group Babuk, which is reportedly a Russian-speaking group. They accessed and published hundreds of confidential documents, clearly damaging the public's confidence in the police in the process.

In the past year, we have also seen influence operations by Russian entities to undermine confidence in the police and exacerbate societal tensions related to the police, so it is not a stretch to imagine that an adversary could use a combination of cyberattacks, like the one conducted by Babuk, and influence operations to undermine faith in public institutions further. In fact, Russia has clearly tried to do just that in our elections by hacking our electoral organizations while also running disinformation campaigns to undermine the public's faith in the process.

How is your organization posturing itself to defend against that kind of layered attack?

General NAKASONE. Congressman, we are well-postured to ensure that we provide the appropriate support to the lead Federal agencies involved. Let me give you several examples.

So, first of all, I will begin with the elections. Our focus at U.S. Cyber Command, at the National Security Agency, is outside the United States to provide the insights on our adversaries into what they are doing. We are well-practiced at this, and I think we have demonstrated our proficiency in both the 2018 and 2020 elections in doing this.

In terms of the recent concerns about domestic violence, again, our focus is outside the United States for foreign actors that might be doing one of three things: First of all, generating content that might be utilized within the United States; secondly, any type of violent activities that are being called for by a foreign actor; and then thirdly, any type of information that is being passed internally with regards to gathering against the United States in any location. We work closely with the FBI [Federal Bureau of Investigation] on that. We work closely with the Department of Homeland Security. We will continue to do that now and well into the future.

Mr. MOULTON. General, how would you characterize the interagency process and how effectively you are able to work with these different agencies?

It strikes me, as an observer, that the lines of authority are not particularly clear and it is hard to delineate who is responsible for which operations, especially when, even just given the example you just described, it is very easy to see how a foreign actor like Russia can easily have a single operation that goes into the territory of multiple U.S. organizations.

General NAKASONE. Congressman, I think the authorities, at least from my perspective as both the commander and the director, are clearly stated, and I know them very well. And I know that our focus is outside the United States. I know that our focus is enabling our partners within the United States.

And I think—I come back to the elections. There could not have been a closer partnership between U.S. Cyber Command, the National Security Agency, the Federal Bureau of Investigation, and the Department of Homeland Security. To give you an example——

Mr. MOULTON. General, we are just short on time. Just to give you an example of the problem here is that if the rest of us don't see that partnership or understand how it works, then you can have a situation where, you know, you have briefed us that the last election was the most secure in American history, and yet half the people in Washington today, all of one party, are trying to make the case that it wasn't.

So how do we improve that understanding, even if it is just a public understanding, of how these lines of authority work?

General NAKASONE. So, Congressman, in terms of the election, you know, I speak to attempts by foreign adversaries trying to interfere and influence our electoral process, and I am very proud of the work that has been done and in partnership with FBI and DHS on this.

Mr. MOULTON. Yes. But you are not answering my question, General, which is that if public perception does not understand how this interagency coordination works, then it is easy to think that these operations are not successful.

Ms. EOYANG. Mr. Moulton, if I may. Mr. Moulton, if I may.

Mr. MOULTON. Yes, absolutely.

Ms. EOYANG. It is something that the Department works with whole of government to protect our elections, and I think we are very clear with the public about the work that we do in this space. But we do not operate domestically, and so we have to engage with the rest of government to make sure that the American people are resilient to misinformation and disinformation, and we will continue to work with our interagency partners on that.

Mr. MOULTON. Yeah. I mean, that is my point. And I know my time has expired, Mr. Chairman, but I think we clearly need to do work on that. And, you know, if I had time, I was going to ask, you know, when I visit a Marine unit on the ground, are they going to say that they are integrated with Cyber Command. My questions all revolve around this coordination. It is very difficult to do. And I am not trying to suggest that I don't have confidence in your ability to follow your lines of authority, but let's make sure that they work well, not only internally, but that we can communicate them effectively to the American public.

Thank you, Mr. Chairman.

Mr. LANGEVIN. Thank you, Mr. Moulton.

Mr. Gaetz, you are now recognized for 5 minutes.

Mr. GAETZ. Thank you, Mr. Chairman, and thank you for holding this very important and timely hearing.

Millions of our fellow Americans are suffering right now in their quality of life, in their ability to interact with their jobs and their families as a consequence of a lack of resilience to these foreign cyber threats. And, General, I wanted to ask you, in circumstances where this opaqueness exists that Ranking Member Gallagher referenced regarding the connections between malicious cyber actors and state actors, how should we think about the concept of deterrence and our capability to deter against some of these more asymmetric threats?

General NAKASONE. Congressman, I think that in terms of thinking about deterrence, it really is thinking about how do we impose costs, and that is the way we have approached it at U.S. Cyber

Command within the Department. In terms of operating outside the United States, when we see elements that are operating, how do we try to impose the largest cost possible, whether or not that is through being able to expose them, whether or not that is being able to share the information with a series of partners that we have, or whether or not when authorized to conduct operations against them.

Mr. GAETZ. Can our fellow Americans who are dealing with the impact of this last cyberattack assume that the imposition of some cost is what is being contemplated by the Department of Defense now?

General NAKASONE. So while I won't get into, obviously, any of the operations that are being considered, what I would say is that, you know, my role as the Commander of U.S. Cyber Command is to provide a series of operational opportunities or courses of action for the Secretary and the President to consider.

Mr. GAETZ. And I want to, again, delineate the types of options that we would like to task you to develop as they relate to state actors versus nonstate actors. I understand that with governments, exposure and embarrassment can be a high cost. Do you agree that with more asymmetric threats, the costs have to be more direct and economic and kinetic?

General NAKASONE. Congressman, what I would say is my experience is that the type of threats that you have described that are nonstate in nature, our response has to be persistent, that it can't be a one-time effort. It has to be persistently that we are going to enable our partners and to act when authorized.

Mr. GAETZ. I also want to associate myself with the comments of the ranking member of the full committee regarding the workforce and recruitment. We all know why you have retention problems. It is because the private sector pays multiples what we would be able to pay people. And while pay certainly isn't the only thing that motivates folks, it certainly can contribute to a lack of retention of some of this high-end talent.

It used to be the case, you know, not too long ago that the brightest minds in Silicon Valley were working on cyber and munitions and lasers, and the Department of Defense was the most important customer and often the most important investor. And now I am concerned that the brightest minds in America are working on likes and shares and memes and other activities that don't directly connect to the mission of the Department. And so I think it is essentially critical for us to follow the thread that Ranking Member Rogers laid out to actually develop more of that pipeline earlier, understanding that there will be some attrition. But a Digital Service Academy seems to be an inspirational, patriotic, nationalist thing for us to be able to do. I think it would inspire a great deal of confidence, both in the public and the private sector.

Is there any advice you would give us going forward to perhaps flesh out that idea from Ranking Member Rogers?

General NAKASONE. So I think—I couldn't agree more in terms of just the spirit of what both you and Congressman Rogers has described with regards to opportunities future for talent. I would only add, what we have to do collectively as, obviously, the Department and the government, is to make it as easy as possible for people

to go from the private sector into the public sector. And I think we still have work to do there.

Mr. GAETZ. Yeah. I mean, I recall even from our first orientation, the challenges presented by some of the limitations and exclusions that the Department puts on people for decisions or recreation that they engaged in that then could disqualify them, and I would hope we would want to cast a wide net for high-quality talent that can make that contribution.

And, again, the earlier you get started with—you know, we get to nominate these great patriots to service academies now, and we see how in the 9th and 10th grade, they are already making choices to try to earn those nominations and those appointments. And so I think that building that pipeline sooner would certainly be very helpful.

I thank the chairman, and I yield back.

Mr. LANGEVIN. Thank you, Mr. Gaetz.

Ms. Houlahan is now recognized for 5 minutes.

Ms. HOULAHAN. Thank you, Chairman. I really appreciate the chance to ask questions.

This one is for General Nakasone, and it is nice to see you again. I am really interested in digital citizenship and digital literacy. I think it is incredibly important, especially in this time when we are, frankly, as a nation and as a world, unclear on where the truth lies. I am wondering if you could tell us how you, frankly both of you, are ensuring that your cyber professionals are trained on how to identify and root out disinformation. And if there is any specific training that you are using for your own team, is there anything that we could leverage or take advantage of to expand to all of the DOD employees to be able to educate them in sussing out the truth as well?

General NAKASONE. So, Congresswoman, I will begin, and if the Secretary wants to jump in. So I begin in terms of our work, we have a very, very structured analytic development program at U.S. Cyber Command that walks our analysts through being able to understand the information that is presented.

I think, to your point, this is a dynamic environment, and so our training continues to evolve. We continue to see our adversaries utilize new means upon which they are trying to influence, and that is one of the areas that we have focused on is being able to have that ability to meter our training fairly rapidly.

Ms. HOULAHAN. And is there anything that you can think of that would be applicable to the broader DOD at large?

Ms. EOYANG. If I may, Congresswoman. I know that this is a priority for the Secretary, increasing the resilience of the DOD workforce, and it is something that he has been working on as we have gone through and responded to the events of January 6.

And I think, to echo General Nakasone's comments about the analytic work force, not just at NSA, but at all of DOD's intelligence elements, we do teach a fair amount of critical thinking to large parts of our workforce.

Ms. HOULAHAN. I would love to follow up with you both on whether there is any applicability to the larger workforce and not just the analytical aspects of our DOD workforce but the body as a whole.

The next question. I would like to very much associate myself with the remarks of Mr. Gaetz, and I know Mr. Rogers as well, are interested in this concept of the Digital Service Academy. I as well am very keen on exploring that and advancing that as well. But in the meantime, highly skilled STEM [science, technology, engineering, and mathematics] professionals are definitely something that we are competing with with the civilian economy. And I was wondering if you could speak a little bit about the Cyber Excepted Service and how it has either positively or negatively impacted DOD's cyber missions, and what we can do in this space more to enhance our workforce capabilities. Maybe General Nakasone speaks first.

General NAKASONE. Thank you, Congresswoman. I am a huge supporter of Cyber Excepted Service. What are we seeing with it? We are seeing that it is an avenue for us to be able to go to recruiting fairs and offer final job opportunities and opportunities for young people to come and consider a career with U.S. Cyber Command.

The other element is, is that I think it takes into account that we have to hire differently, and so we are seeing a dramatic drop in the number of processing days for those that are hired under Cyber Excepted Service. Let me give you an example. Traditionally, it has taken about 110 days to bring someone into our civilian workforce. Under Cyber Excepted Service, we are seeing that drop to somewhere in the 60-day range, so that is a tremendous drop for us. That means that we get people into our workforce much quicker. It is a much better sign for those that are coming into U.S. Cyber Command that we are serious about talent as our number one priority.

Ms. HOULAHAN. Ms. Eoyang, do you have anything further to contribute to that?

Ms. EOYANG. I think that General Nakasone is right, and building a strong and vibrant cyber workforce is certainly a priority, and we have been working with our colleagues in personnel and readiness to try and improve that.

Thank you.

Ms. HOULAHAN. And with the last couple minutes or couple seconds of my time, is there anything further that we could be doing in addition to things like the Digital Service Academy and programs such as these that we can make sure that we are including in this round of the NDAA? Ms. Eoyang.

General NAKASONE. So, Congresswoman, if I might, let me highlight DreamPort, which is an initiative that this committee has supported. I think you will recall that DreamPort in 2018 was stood up. It is an unclassified facility just outside of Fort Meade that we utilize for a number of different initiatives, initiatives such as bringing young people in, a series of high school interns for the summer, an ability to bring together commercial industry with U.S. Cyber Command to talk about key topics like, you know, new architectures for our networks.

But what I have seen when I have gone over to a place like DreamPort, a very small investment can have tremendous impact on young people in terms of exciting them about coming into and thinking about cyber as a career.

Ms. HOULAHAN. Thank you. As a former high school——

Ms. EOYANG. The only other thing that I would add that——

Ms. HOULAHAN. Go ahead.

Ms. EOYANG. I am sorry. The only other thing that I would add to what General Nakasone says is that many of the people in our workforce, they come to us because they are motivated by the mission, that money is not their primary motivator. And so the Congress' continued support for the ways in which we can bolster the training and education of our workforce to help them deepen their support to the mission, we appreciate the support that you have given us so far, and we hope that that would continue in the future.

Thank you.

Ms. HOULAHAN. Thank you, ma'am. And I yield back.

Mr. LANGEVIN. Thank you, Ms. Houlahan.

Mr. Franklin is now recognized for 5 minutes.

Mr. FRANKLIN. Thank you, Mr. Chairman.

And my first question would be for Ms. Eoyang and it is a follow-up, really, to what Mr. Gaetz was referring to before, asking about regarding the attacks we are seeing that are coming from both nation-states and nonstate actors. Specifically, with the nonstate actors that are being financially backed by these states, do our tactics differ on how we attack or how we deter those attacks, depending on whether they are coming from the nation-states or nonstate actors?

Ms. EOYANG. Certainly, nonstate actors who are engaging in financially motivated crimes, the lead for responding to those actors are the FBI and DOJ [Department of Justice]. The challenge, I think, that we have is that when those attacks first come across the networks and impact us, when we see that malicious activity, it is always a challenge of attribution to be able to pull it apart and figure out who are the state actors and who are the nonstate actors. Which elements of government would then be tasked with the lead to disrupt that activity varies based on location and whether or not they are criminal or not. But certainly it is clear that for nation-states who are playing in this hybrid space, we consider that irresponsible state behavior and would continue to call it out where we see it.

Mr. FRANKLIN. All right. Thank you.

In both of your testimonies, you make clear that the U.S. can't go it alone here and we have this great need to work with our allies when it comes to cyber specifically. In what ways can you see that we can strengthen our current relationships? And then, how do we go about building out new ones? And with some of our tactics like, you know, hunt forward, has that position changed over time, depending on which partner country we are referring to?

Ms. EOYANG. Congressman, I would just say that as the President has indicated, strengthening and reinforcing our relationships with our alliances and partners is a very high priority for him. We have demonstrated our commitment to working with allies and partners in the face of the threat. We have expanded our participation in Cyber Flag, and the President continues to maintain a high interest and support for hunt forward operations. I will let General

Nakasone speak to the specifics of that, but we continue to build relationships with partners and allies.

General NAKASONE. Congressman, I would just add, hunt forward operations, where we are obviously coming at the request of a foreign government, worked through the Department of Defense and the Department of State, has been, I think, a tremendous ability for us to show our commitment to partnerships. And, you know, just during the defense of the 2020 elections, 11 different missions in 9 different countries, you can see the importance that the Department places on this.

Mr. FRANKLIN. Great. Thank you. That is all I have, Mr. Chairman. I yield back.

Mr. LANGEVIN. Thank you, Mr. Franklin.

Ms. Slotkin is now recognized for 5 minutes.

Ms. SLOTKIN. Great. Thank you, Mr. Chairman. And thank you to our witnesses for showing up here. You guys have such an important mission.

I want to associate myself with the comments that Representative Gallagher said at the top of the session here. I think it would be so important to really present a truly transformational budget on cyber, you know, whenever you guys submit it. I think that this committee is crying out for it. I think that the country is crying out for it.

And we know that that will come at the expense of older systems, legacy systems, pork, and that Congress has a responsibility to help you with that, which we don't always live up to. But I just want to encourage you to be bold and provide something that really helps move us into the 21st century so we can maintain our military edge.

I guess the question I have for both of you is, I am running this task force, along with Mr. Gallagher, on the Defense Department's supply chains and our vulnerabilities. And cyber has come up at every single session that we have had 8 weeks in a row.

So can you tell us, particularly in the wake of SolarWinds, kind of what CYBERCOM is doing to look at supply chain vulnerabilities, either access by foreigners or just, you know, whether it is intentional or benign? Can you talk to me about supply chain issues?

General NAKASONE. Congresswoman, what we have done in the wake of SolarWinds is, again, taken apart and better understand exactly what the adversary was able to do, and from that, working with the National Security Agency and the Department of Defense, have looked at the defense industrial base to be able to share that information.

I would offer to you, however, that we are also getting a tremendous amount of support and information from defense industrial base companies that provide us kind of an indicator, and I would be more than happy to follow up with that in a future session.

Ms. SLOTKIN. Okay. The other thing I guess I would ask is, you know, in Michigan, we host a multi-domain exercise that is Army, Air Force, and has now been integrating cyber into, you know, the giant exercise. Tell me about what you have done to try and encourage the cyber component of multi-domain exercises all over world.

General NAKASONE. Congresswoman, what we have done is two-fold. One is to try to encourage and support the Guard, not only in exercises, but in real world. And so we created a capability called the Cyber 9-Line, which allows any element within the Guard, Air or Army, to be able to access our big data platform, to share information at an unclassified level with the simple use of a common access card, which is your ID card. Every single element within the United States, the 54 elements of the Guard in our States and territories, has utilized that.

The second piece is, is continuing to support, not only within our exercises, Cyber Flag, as the Secretary mentioned, but also within Guard exercises to have robust cyber play.

Ms. SLOTKIN. Okay. And I guess, you know, this is more of a comment than it is a question. But along the lines of what Representative Moulton was saying, it is so hard to explain to the American public what we are doing to respond when they see these very visible attacks, whether they are from a foreign entity, ransomware, or whatnot.

Our constituents, they are on the front lines of these attacks, and yet they can't feel—they don't know what their country is doing to respond. And I know that that is a difficult position for you all. What you do should be under the radar, but I would just note that there is a real sense that there is just no deterrence on a cyberattack, that a Russian group, a Chinese group can just attack us with impunity. They can steal a million records, you know, the SF–86 forms of a million Federal workers, and we put out a strongly worded press release.

So we are going to need to figure out how to not just do it in the shadows but communicate to the American people that we are not leaving ourselves open as this becomes kind of the primary form of attack on the average American citizen. So I will leave it at that.

Thanks very much, and I yield back.

Mr. LANGEVIN. Thank you, Ms. Slotkin.

Mr. Fallon is now recognized for 5 minutes. Mr. Fallon, are you with us?

Mr. FALLON. Yes. Sorry, Mr. Chairman. Can you hear me?

Mr. LANGEVIN. We can hear you now, yeah.

Mr. FALLON. Oh, wonderful, thank you.

Well, my colleagues have asked some very good questions, excellent questions. And I wanted to ask Secretary Eoyang, the Cyber Mission Force has only reached full operational capacity by 2018. And given that personal computers and the internet have been a part of our daily lives for 30-plus years, why do you think it took so long to gain this capability and capacity?

Ms. EOYANG. Congressman, I think—while I wasn't here in the Department in 2018, I think that it is a growing recognition of the importance that cyber plays.

Prior to this, many of the cyber response capabilities for the Department were resident in the services, but as we realized the need to integrate and think about those things more broadly, the Cyber National Mission Force was stood up. And I am happy to let General Nakasone speak to what the evolution of that has been and the capability that they have developed.

I think we are at the beginning of being able to see the role of the Cyber Mission Force and its integration into the rest of DOD's responses, but I think that its role will continue to grow for us in the Department.

General NAKASONE. Congressman, I would say, we began building the force in 2014 based upon a decision at the Department. The command stood up in 2010. Twenty-eighteen was a pivotal year for us. It is not just the fact that we achieved full operational capability. With the help of this committee, with the help of Congress, we received the right authorities within the NDAA that identified cyber as a traditional military activity, and that was instrumental for the work that we did in the 2018 midterm elections.

The force is mature, it is moving on, it is getting better, it is innovating, it is improving. You know, I can't speak to the length of time to why it took us until 2018 to finish it, but what I can speak to is, is that I am very proud of the work that it has done and where we are headed.

Mr. FALLON. Well, General, I would say, thank you for your answer. But I would be little bit more concerned not so much that we finished the beginning really, or we had the end of the beginning in 2018, but we didn't start till 2014. I think this is something that probably should have been done back when you were a company grade officer in the 1990s, and it is unfortunate that it hasn't happened. It seems like we are playing a little catch-up.

Since 2018, General, what do you see as the notable accomplishments that have been achieved by your command?

General NAKASONE. Congressman, I would begin with security of the elections in 2018 and 2020, a much different result that came about based upon, again, the authorities that came to us from both the legislative and the executive branch.

There are other series of operations that have been conducted since then, that I would welcome to be able to comment this afternoon in a different forum. But I think I would close with just the ability for the services and the Department to evolve pretty quickly in terms of, not only the fact that we stood up a force, but the fact that the services now have established cyber services and cyber branches, and then being able to move quickly to react to how we need to outfit those forces.

Mr. FALLON. General, what kind of collaboration exists between CYBERCOM and DHS's CISA?

General NAKASONE. Daily collaboration, Congressman. As I mentioned, we have a series of planners that are there. We have worked such initiatives as, you know, the protection of the vaccines within this country. We have also looked at a series of exercises to posture ourselves for support to DHS in the event of a crisis. So it is an ongoing, robust relationship with CISA.

Mr. FALLON. Thank you, General, Secretary. And thank you, Mr. Chairman. I yield back.

Mr. LANGEVIN. Thank you, Mr. Fallon.

Ms. Escobar is recognized for 5 minutes.

Ms. ESCOBAR. Thank you, Mr. Chairman. Really appreciate the opportunity. Many thanks also to our witnesses for their service to our country, as well as for bringing their expertise to this subcommittee.

You know, as our daily lives and as more of our security and the utilities that we depend on migrate toward the web, and as we see recent attacks like what we saw with Colonial Pipeline, the urgency of this issue could not be more pressing for our committee.

I am very interested in exploring innovation. And, General, you mentioned innovation and, Secretary Eoyang, you did as well. But, Secretary Eoyang, I would like to explore a little bit more the Department's initiatives to engage institutions of higher learning, not just for recruitment when it comes to cyberspace, but also as partners for this badly needed innovation.

The University of Texas at El Paso in my home district is a National Center of Academic Excellence in cyber operations. And so I am curious about just how much the Department prioritizes collaboration with universities, you know, as you described DOD's key partners outside the U.S. Government. And I want to give you a chance to elaborate on this and, again, not just in terms of recruitment, but also as a key partner.

Ms. EOYANG. Yes, absolutely, Congresswoman. Research universities like UTEP [University of Texas at El Paso] and others, who have a focus on cyber, do provide tremendous benefit to the Nation. Universities, as part of our research and engineering efforts in the Department, are a key source of ideas and innovation for us, and we have prioritized funding to those institutions.

We will have to—we can reengage with you when the President's budget is submitted about specifics related to that.

General NAKASONE. Congresswoman, if I might just add to the Secretary's comments. As you well know, the National Security Agency sponsors over 300 Centers of Academic Excellence in the United States, of which I believe UTEP, as you indicated, is one of them.

We will continue to do that as an agency. It is critical, not only in the sense, as you noted, with regards to the development of our young people, but also in the development of curriculum that changes and matters to what our universities are working on. So I think this is a rich partnership that we will certainly continue well into the future.

Ms. ESCOBAR. General, I really appreciate that. And, you know, one of the things that I would add, in addition to bringing that innovation that universities and institutions of higher learning can bring, an institution, as you know, like UTEP, which is a Hispanic-serving institution, brings badly needed diversity to the way that we operate as a country, as a government. And so I appreciate that, and I look forward to continuing to work with you all on ways to expand opportunities for institutions like UTEP, but also to really rely on that innovation that I think will help get us out from being behind the curve and to being more in front of it.

Secretary Eoyang, one last thing. I want to explore the Pathfinder program. You said you partner with DHS on this, in which you assist private companies by enhancing their ability to protect their own networks. Can you describe the results of the Pathfinder initiatives?

Ms. EOYANG. So I believe we owe Congress a more fulsome answer on our analysis of the Pathfinder program, but as we see today with the interruption of Colonial Pipeline, the Department's

ability to partner with private sector in order to be able to help them identify threats on their networks is an important defensive step that we can take to help secure the whole of nation. And I think perhaps General Nakasone has some thoughts on additional public-private partnerships in that area.

General NAKASONE. So, Congresswoman, I think my experience has been, we have worked closely with both the financial and the energy sectors on that. If we might have—if I can take that for the record, though, to provide you a more fulsome answer.

[The information referred to can be found in the Appendix on page 65.]

Ms. ESCOBAR. That would be great. I appreciate it. Thank you both. Mr. Chairman, I yield back.

Mr. LANGEVIN. Thank you, Ms. Escobar.

Mrs. Bice is now recognized for 5 minutes.

Mrs. BICE. Thank you, Mr. Chairman, for holding this very important hearing. And thank you to both the witnesses for joining us today to share your perspectives.

I appreciated your comment, General, in the beginning that cybersecurity is national security, and I think that the things that we have seen over the last, you know, week or two especially, have highlighted the importance and the swiftness at which this issue needs to be addressed.

As both of you know, the DOD currently relies on thousands of data centers that are often stovepiped, disconnected, and in many cases, have reached their limits of life service. They can no longer be upgraded to meet current cyber threats our Nation is facing.

I understand there is a directive for DOD agencies to migrate to milCloud 2.0, but the adoption has been slow. For both of the witnesses, but specifically to Secretary Eoyang, could you provide me with your perspective on the migration to milCloud 2.0 and the degree to which the migration can help address DOD's current cyber vulnerabilities?

Ms. EOYANG. So as you know, the Department takes a number of steps to defend its networks and its data, but as to the specifics of migration, I will have to take that for the record. I want to make sure that I have coordinated that with my CIO [Department of Defense Chief Information Officer] colleagues.

Thank you.

[The information referred to can be found in the Appendix on page 65.]

General NAKASONE. What I would add to that, Congresswoman, is, what we have learned over the past 6 to 12 months is that we have to think about defense differently. In terms of as we move to, you know, cloud-based capabilities to secure our data, many people think that we will just put it into the cloud. It doesn't work quite that way.

And so ensuring we have the right contracts written, ensuring that we have our defensive forces trained to a higher degree in terms of their abilities, ensuring we have the big data capabilities that are necessary, that is what I would add to it.

Mrs. BICE. Follow-up question specific to that topic, and that is, do you believe that we are investing enough in cybersecurity?

And I will elaborate on that. I feel like we tend to focus when we are looking at budgets, on people and, you know, equipment, but we are not looking at that cyberspace as much as I believe maybe we should be, and maybe some of the things that we are seeing now are highlighting some of that.

Ms. EOYANG. Certainly, we have tremendous risk in cyberspace, and we are facing persistent adversaries in this space. I think that the questions of the resourcing are things that we have to take into consideration in light of the other demands that are placed upon the Department and the Nation. While we certainly could make use of additional funds, whether or not—how that all works out, we are happy to engage the committee when the President's budget is released.

General NAKASONE. Congresswoman, I am at a bit of a disadvantage because you are asking the combatant commander in charge of cyber to comment on a question like that. Here is what I would say: We have to use every single dollar that is provided to us by Congress in probably a much more efficient way.

And the way I would characterize that is that, working very, very closely with the DOD Chief Information Officer, where do we prioritize our last dollar of defense. He has done a tremendous job, John Sherman, in laying that out. We have clear guidance from the Secretary that accountability means something with regards to cybersecurity.

So it is not just the fact that we need more money. We need to be able to use the money that we have to the most efficient benefit of our Department.

Mrs. BICE. On that note, do you believe that flexibility in making those acquisitions in a timely fashion would be of benefit to you? Because one of the concerns I have is that we spend a lot of time planning, developing, and then procuring, but it could be 2 years by the time that actually takes place, and at that point, the technology that we are acquiring is no longer, you know, of use in many cases.

How do we address the timeliness of making sure that we are keeping up with these cybersecurity challenges?

Ms. EOYANG. I do think this is one of those areas where we have to think differently, given the speed of the threat. The traditional acquisition models that the Department has used for concrete weapons systems may not be applicable to cyber, given the speed of things, but that is something that we need to work out with our colleagues in Acquisition and Sustainment, and happy to come back to you guys with some additional thoughts on that.

General NAKASONE. I appreciate the committee's elimination of the $75 million cap on acquisition, in the last NDAA. That was incredibly important for us, because we are starting to now grow this ability to do acquisition at the command. We need to go faster on that, but that is an example of something that helped us tremendously.

Mrs. BICE. Thank you for your time today. Mr. Chair, I yield back.

Mr. LANGEVIN. Thank you, Mrs. Bice.

Mr. Morelle is now recognized for 5 minutes.

Mr. MORELLE. Thanks very much, Mr. Chair, for this important hearing. And I want to not only thank you but thank the witnesses for their considerable contributions to the country.

And, General, it is nice to see you. I had an opportunity with the freshman class in 2019 to visit with you at Fort Meade and was very impressed with the operation, and I know how critical this is.

I want to just—and these may have been questions, as I am thinking about it, may have been asked in one form, but maybe you could just drill down a little.

I have some questions about how private industry, the private sector innovation can help CYBERCOM address increased cyber-attacks, whether they can, whether, in your opinion, some of those [inaudible] I know the private sector is working on it.

Secondly is whether or not the command is well-positioned to implement cutting-edge technology from the private sector. So is it available? Is there help out there that you think you could use? Are you positioned to be able to implement help and resources and innovation in the private sector?

And finally, are there obstacles preventing you from acquiring and implementing technology that we need to address, that we need to help you, you know, through the NDAA or other means to help you with a greater collaboration?

And I would ask of both witnesses.

General NAKASONE. Congressman, just to start out, I would say that, is there initiatives in the private sector that could certainly help us? Yes, most definitely. And we see that. We are working with the Defense Innovation Unit. We are working through a series of partnerships that have been established.

And then we are bringing it to, you know, a common location like our DreamPort facility where it is unclassified. We can have a discussion. They can understand in the private sector what our priorities are. That is among the most important things that we have to do at the command, is list each of the challenges that we need assistance on. Private sector is seeing that. They understand that.

The other piece is that I think that perhaps what we have to do even more prevalently is be able to have the culture that sometimes we don't have to develop it, that it has been developed in the private sector. So when we talk about new architectures for our network, there is a lot of networks in the United States, a lot of really well-run networks in the United States; we should be able to leverage that quite rapidly, and that is what we are doing.

The last piece, in terms of obstacles, if I might, again, just working through our folks and then back to the Department, if I can provide some thoughts on that as well.

Mr. MORELLE. Thank you, General.

Madam Secretary, do you have any additional thoughts?

Ms. EOYANG. I think that obviously the private sector has been——

Mr. MORELLE. I am sorry. I can't hear the Secretary.

Ms. EOYANG. Sorry. The private sector has a tremendous amount of capability and innovation. I think the Department is looking for innovative ways to be able to bring that innovation in to benefit our mission. The challenge, I think, is while the private sector may move fast and break things, we, in the Department, can't afford to

have things break. We need to move fast and fix things. So we welcome private sector partnership to work on that.

Thank you.

Mr. MORELLE. Very good.

Mr. Chair, I think this is an important subject. I would love to continue to be a part of the conversation and be helpful to both the Secretary and the General as they meet what are emerging and obviously very serious threats. With that, I will yield back, Mr. Chair.

Mr. LANGEVIN. Thank you, Mr. Morelle.

Mr. Moore is now recognized for 5 minutes.

Mr. MOORE. Thank you, Chairman. Obviously, a very pertinent and important conversation today, so I am glad and appreciate having the time and the witnesses for being here.

I think the American public would be able to categorize this as these things—these issues keep happening. We have got Colonial, we have got SolarWinds.

My two questions are for General Nakasone. They are about deterrence and talent. So let me jump into the first one.

We have now set a precedent, we are naming Russia as the culprit in a couple of these situations, in these attacks. Is that a plan going forward? Is it meant to be a deterrent for future hacks? Will it be a deterrent? Could you provide some context on our approach to that and even more broadly with respect to deterrence?

General NAKASONE. If I might start, and then I am certain that the Secretary may have some comments on that as well.

Mr. MOORE. Please.

General NAKASONE. So with regards to what we are seeing by adversaries operating against us in cyberspace, this is going to continue. And so the Department's position in terms of defend forward, operating outside the United States, and U.S. Cyber Command's ability to do persistent engagement is what we are doing, and we need to do more of it. We need to be able to enable our partners better, and we need to act, when authorized, more effectively, and I think that this will be certainly where we are headed.

In terms of specific options regarding any of the adversaries, I would defer that until this afternoon. But there are, from my vantage point, a series of options that we continue to develop and provide when necessary for a number and a range of opportunities for the Secretary and the President's determination.

Mr. MOORE. Excellent.

Ms. EOYANG. Congressman, thank you for that very important question. I think deterrence is certainly the Department's goal when it comes to cyberspace, but I think we need to be specific about what kinds of deterrents and against which types of adversaries.

Since some of the activity that you referenced is what we would consider cyber espionage, and while we would expect that there is nothing that an adversary could do to deter U.S. intelligence-gathering efforts, there is likewise, we may not be able to deter adversary activity in that space to zero. That is not to say we can't impose costs, both by calling it out and making their lives harder, and engaging through other means to try and limit the scope of that activity. And I think that there are other ways that we can think about deterrence by denial.

I would just note that in terms of cyberattacks that would rise to the level of an armed attack, we have not seen that type of attack from the adversary on the U.S., from a nation-state adversary on the U.S. And we would, I think, continue to maintain a strong deterrence posture against any type of attack of that nature.

Mr. MOORE. Excellent. Thank you. And I look forward to discussing more through our closed briefing.

Quickly, just with respect to the pool of cyber talent in the DOD, how, ultimately, are we going to be competitive with the commercial industry? How can we better avoid the attrition that we oftentimes see within the DOD that is both an expense and, you know, a dearth of talent that exists?

General NAKASONE. So, Congressman, I would begin. Our number one competitive advantage in this space is our mission. There is nowhere you can do some of the things that you can do at U.S. Cyber Command, legally, in the United States. And so that is something that we continue to obviously reinforce with our members.

The second is that we have world-class facilities. Whether or not you are in Fort Meade or Georgia, Texas, Hawaii, Colorado, anyplace that we are operating, one of the things that we have been the beneficiaries of is a very, very high standard of facility that we operate.

And thirdly, one of the things that we continue to obviously leverage are a series of financial incentives that the service's Cyber Excepted Service has provided to us. But it will never be about money. It needs to be about what we are doing in the mission and the folks that they are working with.

Mr. MOORE. Excellent. Welcome any other thoughts, Secretary.

Ms. EOYANG. Thank you, Congressman. We really appreciate the committee's focus on this. And while we seek to retain the best possible cyber talent for the Department, we do have the benefit of, as we train cyber personnel, General Nakasone's personnel complete their military service and return to the private sector, we are also helping to fill a shortage of cyber talent across the Nation.

So while we need to make sure that we can meet our retention requirements and readiness requirements, it is not a complete loss for the Nation because we send more people out there to defend in the private sector space as well.

Mr. MOORE. Excellent. Looking forward to discussing more.

I will yield back. Thank you.

Mr. LANGEVIN. Very good. Thank you, Mr. Moore.

And with that, I want to thank our witnesses for their testimony, the members for their questions. To our witnesses, I know that members had some questions that required follow-up and members may have additional questions. I ask that you respond in writing at the earliest opportunity.

And with that, we are going to close out the open session of this hearing, and we will move now to CVC–200 for the classified portion.

With that, the hearing stands adjourned. Thank you.

[Whereupon, at 12:32 p.m., the subcommittee proceeded in closed session.]

# A P P E N D I X

MAY 14, 2021

**PREPARED STATEMENTS SUBMITTED FOR THE RECORD**

MAY 14, 2021

**Chairman James R. Langevin**
**Cyber, Innovative Technologies, and Information Systems Subcommittee**
**Operations in Cyberspace and Building Cyber Capabilities Across the Department of Defense**
**May 14th, 2021**

The subcommittee will come to order. Welcome to today's hearing, "Operations in Cyberspace and Building Cyber Capabilities Across the Department of Defense". We have convened this as a hybrid hearing and are joined by members who are participating remotely. Members who are joining remotely must be visible onscreen for the purposes of identity verification, establishing and maintaining a quorum, participating in the proceeding, and voting. Those Members must continue to use the software platform's video function while in attendance, unless they experience connectivity issues or other technical problems that render them unable to participate on camera. If a Member experiences technical difficulties, they should contact the committee's staff for assistance.

Video of Members' participation will be broadcast in the room and via the television/internet feeds. Members participating remotely must seek recognition verbally, and they are asked to mute their microphones when they are not speaking.

Members who are participating remotely are reminded to keep the software platform's video function on the entire time they attend the proceeding. Members may leave and rejoin the proceeding. If Members depart for a short while, for reasons other than joining a different proceeding, they should leave the video function on. If Members will be absent for a significant period, or depart to join a different proceeding, they should exit the software platform entirely and then re-join it if they return. Members may use the software platform's chat feature to communicate with staff regarding technical or logistical support issues only.

I have designated a committee staff member to, if necessary, mute unrecognized Members' microphones to cancel any inadvertent background noise that may disrupt the proceeding.

I'd like to welcome our witnesses General Paul Nakasone, the Commander of U.S. Cyber Command and the Director of the National Security Agency, and Mieke Eoyang, the Deputy Assistant Secretary of Defense for Cyber Policy. In past hearings, General Nakasone has been joined by the Assistant Secretary of Defense for Homeland Defense & Global Security; however with the challenges faced in that role, we are thankful that Ms. Eoyang is able to step in, and the committee appreciates her cooperation and collaboration.

It's truly incredible how much has changed since our last Cyber Posture Hearing on March 4th 2020. The world has been upended by a pandemic, changing the lives of literally every person on this planet. In the realm of cyber matters, the men and women of the Department of Defense, including our soldiers, sailors, airmen, marines, and guardians, have had no respite, continuing to operate and defend Americans' interests in cyberspace.

Despite the pandemic, our adversaries and competitors have not let up their cyber campaigns. In the last six months alone, the media has reported almost non-stop on arguably some of the most significant cyber incidents ever to affect our nation, from SolarWinds, to Hafnium, to just in the last week, the attack against Colonial Pipeline by the DarkSide criminal collective.

If there were ever doubters that cyberspace is an active and contested warfighting domain, I'd hope that the last year has changed those perspectives. Yet incredibly, it still appears to this Committee that cyber does not have the focus from much of the Department's senior uniformed and civilian leadership that it requires, despite our forces engaging adversaries in this domain every single day. Recently, the Air Force removed cyber from its mission statement even though a report from the Office of the Secretary of Defense concluded that the inclusion of cyber in the Air Force mission statement is the single reason why Air Force personnel have vastly outpaced the other services in pursuing cyber-related certifications.

Candidly, it is frustrating that the people in this room, both members and witnesses, are fighting an uphill battle to put cyber front and center in the Department. Out of five officially recognized warfighting domains, the senior civilian official for the air, sea, land, and space domains are military service secretaries. Yet - and with all due respect to Ms. Eoyang and her spectacularly overworked team - the senior civilian for cyber is four rungs lower than her counterparts overseeing the other domains.

We also have to account for the way in which cyberspace operations occur within and affect the information environment. One of the most illustrative examples of how the Department's structure can hinder rather than enable operations is its own organization chart. DoD's Joint Publication 3-13 notes that cyberspace is one of many information related capabilities designed to affect the information domain, alongside psychological operations and electromagnetic spectrum operations. Yet, each of the information related capabilities is handled by a separate entity and siloed within the Department, ensuring that we cannot leverage our capabilities to the maximum extent possible.

In our current age of great power competition, conflict in the "gray zone" below the level of armed conflict has never been more relevant to our strategic thought. For numerous reasons – challenges with attribution, easily altered payloads, and ease of proliferation – cyber is the ideal tool for gray zone conflict. The information domain, including cyberspace, is where our forces are engaged against our adversaries daily. As the nation comes to realize that this domain is as important as any other, we need the Defense Department to adapt to ensure any conflict with adversaries remains in the information space as much as possible and never moves into the kinetic realm.

As we push the Department to adapt toward the information environment, congressional oversight has never been more necessary. It is the mechanism by which we monitor the activities of the Executive Branch and ensure compliance with relevant statute. While I understand that transitions can result in disconnects

or misunderstandings, I anticipate hearing from the Committee staff that any issues that may have arisen will be quickly resolved to our satisfaction. I am happy to add detail in private but will leave it at that for now.

With that, I want to thank our witnesses for appearing before us today. As a reminder, after this open session, we will move to the CVC auditorium for a closed member-only session.

I'll now turn to Ranking Member Gallagher for his remarks.

STATEMENT OF

MIEKE EOYANG

DEPUTY ASSISTANT SECRETARY OF DEFENSE FOR CYBER POLICY

TESTIMONY BEFORE THE

HOUSE ARMED SERVICES COMMITTEE

SUBCOMMITTEE ON CYBERSECURITY, INNOVATIVE TECHNOLOGIES,

AND INFORMATION SYSTEMS

MAY 14, 2021

Thank you Chairman Langevin, Ranking Member Stefanik, and Members of the Committee. I am pleased to be here with General Nakasone, Commander of U.S. Cyber Command (USCYBERCOM), to report on the progress the Department of Defense (DoD) has made in achieving the Department's objectives in cyberspace. This afternoon, I am testifying in my role as Deputy Assistant Secretary of Defense for Cyber Policy. I am responsible for advising the Secretary and the Deputy Secretary on cyberspace policy and the development of the Department's cyber strategy and cyberspace policy, leading our interagency partnerships and coordination of our participation in whole-of-government cyber efforts; engaging with our allies and partners on cyber matters; and ensuring the coordination of cyber capabilities across the Joint Force in support of objectives established by the President and Secretary of Defense.

The Congress has demonstrated that it views cyber defense as a priority, for which I would like to express the Department's thanks. I note that Chairman Langevin and Representative Gallagher served on the Cyberspace Solarium Commission, in which the Department played a role, and that many of the Commission's recommendations were included as provisions in the National Defense Authorization Act for Fiscal Year 2021. The very existence of this newly formed subcommittee on Cyber, Innovative Technologies, and Information

Systems demonstrates your dedication to our enterprise. We are grateful for your ongoing support.

**Strategic Context**

To start, I would like to offer our perspective on the current strategic context. 2020 was a year of turmoil, with a global pandemic drastically altering our day-to-day reality. Americans had been moving more aspects of their lives online for years prior to the pandemic, but COVID-19 accelerated that trend and increased our dependency on the Internet. Suddenly, many of us found ourselves working, studying, and socializing almost exclusively in virtual environments.

Our adversaries took notice of our growing reliance on technology as Americans began teleworking and turning to online services in greater numbers than ever before. The increase in network traffic presented nefarious actors with additional opportunities to cause mayhem. This led to an uptick in the volume and breadth of disruptive activity online. Cyber criminals and nation-state hackers alike took advantage of COVID-19 by unleashing ransomware on healthcare facilities, targeting vaccine production and supply chains, exploiting fears to spread disinformation—and even hijacking the virtual meetings upon which we had come to rely.

As a result, the cyberspace domain is both more important and more contested than it has been in recent memory. Enhancing the security of cyberspace, both in the United States and around the world, is a top priority for the President and, by extension, for me and the Department. The President's Interim National Security Strategic Guidance makes cybersecurity an imperative across the government and pledges to expand the investments needed to defend the Nation effectively against malicious cyber activity and cyber attack. I am confident that this focus will allow the Department to continue to defend the Nation against the myriad challenges we face in the cyberspace domain.

**Current Threat Environment**

Increased malign activity in cyberspace reflects greater geopolitical trends. The distribution of power across the world is changing, and our competitors are using their cyber capabilities to seek political, economic, information, and military advantages, and to undermine our security by taking more sophisticated and concerning actions below the threshold of armed conflict. In its unclassified threat assessment for 2021, the Office of the Director for National Intelligence (ODNI) assesses that cyber threats from nation states—particularly China, Russia, Iran, and North Korea—and their surrogates will remain acute, as they increasingly use cyber operations as a tool of national power, in some cases attempting to pre-

posture capabilities to achieve a decisive military advantage in the event of a conflict.

As Secretary Austin said at his confirmation hearing in January, China is the pacing challenge for the Department and looks to compete with us along a spectrum of activities, including cyber operations. China uses cyber operations to erode U.S. military overmatch and economic vitality. Its operations include stealing U.S. intellectual property and research from the defense industrial base and other segments of the private sector. And, despite President Obama and Chinese President Xi Jinping's 2015 joint commitment not to conduct or knowingly support cyber-enabled intellectual property theft, Chinese malicious cyber activity continues unabated.

Russia continues to be a highly sophisticated and capable adversary, integrating malicious cyber activities, including cyber espionage and influence operations, in mutually reinforcing ways to achieve political, economic, and military objectives. SolarWinds, the broad-scope cyber espionage campaign perpetrated by the Russian Foreign Intelligence Service (SVR), demonstrates the formidable threat that Russian state actors pose to U.S. interests in cyberspace. Russia has also engaged in a myriad of other malign cyber activities, including its attempts to interfere with U.S. elections, spreading ransomware such as NotPetya, and efforts to disrupt the postponed Tokyo Olympics.

In addition to using cyberspace as a tool of power outside their borders, China and Russia view the Internet as a mechanism to control and intimidate their own populations. While the United States advocates for an open, interoperable, secure, and reliable Internet, China and Russia have created and employed a digital authoritarian model, using their technological and cyberspace capabilities to manipulate narratives, repress free speech, surveil their citizens, and quash dissent domestically. China seeks to export digital authoritarianism to other repressive regimes, remaking the Internet in its image.

Although China and Russia remain our two primary strategic competitors, the threats to the United States in cyberspace include a diverse set of additional actors. Iran and North Korea continue to employ their cyber capabilities to conduct espionage, and they remain a threat to public and private U.S. critical infrastructure. Non-state actors, including criminals, terrorists, and violent extremists, continue to leverage the digital domain to advance their agendas, and the growing availability and use of open source cyber tools is increasing the overall volume of unattributed cyber activity around the world. The line between state and non-state actor activity is increasingly blurry as states turn to criminal proxies as a tool of state power and then turn a blind eye to cybercrime perpetrated by the same malicious actors. This is a common practice for Russia, whose security services

leverage cybercriminals while shielding them from prosecution for crimes they commit for personal benefit.

We have also seen states allowing their government hackers to "moonlight" as cybercriminals. In December 2020, the Department of Justice charged three hackers employed by North Korea's General Reconnaissance Bureau with attempting to steal or extort more than $1.3 billion from financial institutions around the world. The hackers sought mostly to benefit the North Korean regime, but at times, they sought to enrich themselves, using state hacking tools for private financial gain. This is not how responsible states behave in cyberspace, nor can responsible states condone states shielding such criminal behavior.

The ubiquity of digital technologies in all aspects of U.S. society means that the average American is far more exposed to malicious activity in cyberspace than they are to aggression in other domains. Nation-state digital threats are not constrained to nation-state targets, they also harm American families and businesses, distort our social interactions, and disrupt commerce. One particularly concerning example of cybercrime is ransomware, which has disrupted municipal governments, forced schools to close, forced many businesses in the Defense Industrial Base to close and, perhaps most egregiously during a pandemic, has disrupted healthcare facilities and hospitals straining to cope with COVID-19. The Secretary of Homeland Security recently described ransomware as an epidemic

spreading through cyberspace and highlighted the danger posed by the growing sophistication of cybercriminals and the increasing frequency of ransomware attacks.

Finally, as our defenses improve, our adversaries evolve, growing more sophisticated in their attempts to circumvent our protections. Spear phishing and other simple exploits are no longer the only threats we face—we must now counter much more complex and insidious actions such as malicious activity targeting our supply chains. The SolarWinds incident demonstrates that as our adversaries dig further down in the software supply chain, more organizations will be adversely affected. This highlights the criticality of our interagency partnerships, and of working with the private sector and our international allies, with whom we must collaborate to address these sophisticated actors and the intricate threats they pose.

The threats I've outlined above, which span the spectrum from high-end conflict to day-to-day cybercrime, are what we in the Department must contend with as we work to advance U.S. objectives in cyberspace.

**DoD's Approach to Cyberspace**

The Department must be postured and prepared to advance U.S. national security in cyberspace in day-to-day competition, crisis, and conflict. As President Biden has stated, a powerful military matched to the security environment is a decisive American advantage.

The Department also seeks to disrupt, degrade, and defeat cyber threats before they harm U.S. national interests. We accomplish this by understanding and countering adversary activity in cyberspace outside the United States in the same way we stop threats outside our borders on land, in the air, at sea, and in space. Through operations on foreign digital networks, what we call "defending forward," we gain insights about hostile cyber actors we can use to improve our own security posture and to enable appropriate actions by our partners, domestically and internationally. We are also prepared, if directed, to take actions to stop adversary activity.

A few examples illustrate how the Department puts these ideas into action. The most tangible examples of defending forward are hunt forward operations. The Cyber National Mission Force deploys defensive cyber teams globally at the invitation of allies and partners to conduct combined operations that look for, and gain insights into, malicious cyber activity. These operations also provide the Department with enhanced warning of adversary actions, enabling us to defend government and civilian networks, data, and platforms more effectively.

The Department also defends forward to protect the integrity of U.S. elections. This is one of our enduring missions. In 2018 and 2020, we operated beyond our borders to generate insight into adversary intentions and activities and, when appropriate, took action to disrupt, degrade, and defeat malicious actors'

attempts to interfere with or covertly influence our elections. This approach complemented our interagency partners' efforts to enhance the security of this segment of our domestic critical infrastructure.

In addition to defending forward, the Department is called upon to defend the homeland, and we embrace this mission as a critical enabler of whole-of-government efforts to counter threats to our national security. To protect our elections, the Department stood ready to support our interagency partners directly, at their request. In 2018 and 2020, we ensured that we had policies and agreements in place that would allow us to spring into action immediately if our colleagues at the Department of Homeland Security (DHS) requested assistance. DHS was ultimately able to accomplish its missions without direct support from the Department, but with this streamlined framework for collaboration in place, we are ready to assist during the 2022 elections and beyond.

The Department also supports our interagency partners in responding to crises, including COVID-19 and the recently discovered SolarWinds Orion platform vulnerability. We paved the way for the Department to provide technical expertise to DHS to support OPERATION WARP SPEED security, enhancing the cybersecurity and supply chain security of this HHS-DoD joint effort to deliver COVID-19 vaccines to the American people. We provided DoD personnel to DHS to enhance collaborative cybersecurity planning and to assist with incident

response, including synchronization of Cybersecurity and Infrastructure Security Agency and USCYBERCOM efforts in response to SolarWinds. The latter example was made possible by our implementation of the pilot program established by section 1650 of the National Defense Authorization Act for Fiscal Year 2019, which authorizes DoD to provide DHS with cybersecurity technical personnel, on a non-reimbursable basis, to enhance cybersecurity cooperation, collaboration, and unity-of-government efforts.

**DoD's Key Partners Outside the United States Government**

The Interim National Security Strategic Guidance directs us to "renew our commitment to international engagement on cyber issues, working alongside our allies and partners to uphold existing and shape new global norms in cyberspace." With international partners, the Department is driving new approaches to expand and strengthen traditional security cooperation tools in support of these important relationships.

COVID-19 has temporarily complicated these efforts, but international partnerships and capacity building remain important to us, and we have found ways to work together in this new environment to meet our shared objectives. For example, the Institute for Security Governance, a component of the Defense Security Cooperation Agency, quickly transitioned to virtual engagements to continue sharing tools for capacity building with foreign partners. We have been

able to continue Hunt Forward operations by following appropriate safety protocols. USCYBERCOM hosted CYBER FLAG, its annual joint cyberspace training exercise fusing attack and defense across the full spectrum of operations against a realistic and thinking enemy via a virtual cyber training range in 2020. We look forward to the next iteration of CYBER FLAG, which will incorporate allies, including the UK, France, Denmark, and Estonia, and aims to improve the overall capability of the United States and allies to respond in unison to defend against malicious cyberspace activities targeting our critical infrastructure and key resources. This exercise demonstrates the United States' commitment to its international partners and will be critical as we work with those partners to increase resiliency in the wake of SolarWinds.

I would like to thank the Congress for including a new, enumerated mission area within 10 U.S. Code Section 333 in the last National Defense Authorization Act (NDAA). The addition of a new authority—specifically, for "Cyberspace Security and Defensive Cyber Operations"—will bring much-needed clarity and emphasis to our efforts to build partner capacity in cyberspace. Building on this new authority, and informed by the Secretary's revalidation of DoD's International Cyberspace Security Cooperation Guidance, the Department aims to leverage and advance our existing cyber-related capacity-building engagements overseas and,

over the coming year, will look to expand DoD cyber cooperation with select international partners in line with our strategic interests.

Collaboration between the private sector and the government is crucial to building a safer and more secure environment—both online and off—for all Americans. To that end, the Department has undertaken a number of "Pathfinder" pilot programs through which we partner, in coordination with the Department of Homeland Security, with private companies in critical sectors, such as energy and finance, to enhance their ability to protect their own networks and improve information sharing. The ultimate goal is not only to ensure that the Department can carry out its mission but broadly to defend the Nation. We recently concluded an assessment of our ongoing private sector collaborations pursuant to section 1728 of the National Defense Authorization Act for Fiscal Year 2021. The assessment includes recommendations to strengthen our enduring initiatives.

**Looking to the Future**

Through defending forward and extensive cooperation with our U.S. interagency, international, and private sector partners, the Department is able to advance the high-level objectives articulated in the Interim National Security Strategic Guidance, the 2018 National Defense Strategy, and the 2018 DoD Cyber Strategy. The 2018 National Defense and DoD Cyber strategies have served the Department well, allowing us to make great strides toward advancing our national

objectives in cyberspace. But even the best strategies must be periodically revisited and revised to address an ever-evolving threat landscape and account for new priorities; this is especially true in the cyberspace domain.

President Biden is currently conducting a review of national strategy, which will culminate in the issuance of two key documents: the National Security Strategy and the National Cyber Strategy. The President's guidance will inform our own review of the Department-level National Defense Strategy (NDS), which will take place over the coming months. The next NDS will describe how the Department plans to support the objectives articulated in the President's National Security Strategy, in addition to providing amplifying direction to the Department on a range of issues, to help ensure the Department can implement this guidance. Then, once we have national and Department-level direction in place, we will issue updated defense-focused cyber-specific guidance to align with, and nest under, the National Security Strategy, the National Cyber Strategy, and the National Defense Strategy.

The final step in the strategic review process will be the Department's second-ever Cyber Posture Review (CPR). The CPR will evaluate how the Department is positioned to execute the national and Department-level strategies and achieve our goals in cyberspace. We look forward to delivering the next CPR to Congress once it is completed.

These new strategies will come at a time when the United States faces emerging challenges in the cyberspace domain. To name a few: the propagation of ransomware holds essential services such as hospitals at risk, as I alluded to earlier in my testimony. Covertly disseminated misinformation and disinformation are proliferating and have threatened to shake Americans' confidence in elections and in COVID-19 vaccines. Our adversaries seek to use social media platforms to mine data on members of our military. Some of these activities are perpetrated by nation-state actors and some by cyber criminals; none are confined by borders.

In the near future, we will have to contend with these and other unforeseen challenges as bad actors use cyberspace to their advantage with greater creativity. We may see a confluence of the Department's responsibilities and equities with those of law enforcement, particularly when new cyber threats emanate from criminal enterprises or from within the United States. We must tread carefully as we consider how the Department can leverage its capabilities to protect the American people from novel threats while respecting their rights and remaining within the bounds of the law.

We look forward to working with the Congress to address these challenges. However, as I have noted throughout this testimony, the Department of Defense is not the only Federal department or agency with cyber equities, and the NDAA is not the only vehicle for providing the authorities we need to defend the American

people in cyberspace. When we think of the Department and its authorizing legislation as the primary vehicle for achieving our goals in the cyberspace domain, we risk over-militarizing our approach. Cyberspace is not solely a domain of warfare, but it is a place in which Americans live much of their daily lives. Although the Department has unique capabilities and capacities to bring to bear, our civilian departments and agencies lead the defense of the civilian networks on which we work, connect with our loved ones, pay our bills, and register to vote. We are postured to support our civilian interagency partners in defending those networks when called upon to do so.

**Conclusion**

Thank you once again for the opportunity to appear before you today. With the Biden Administration's Interim National Security Guidance and the 2018 DoD Cyber Strategy in place, we are confident that the Department has the right policy and guidance to support the defense of our Nation in cyberspace. We were able to use that guidance and resourcing during the past year to meet the unique cyber challenges presented by COVID-19, and while those challenges are not yet behind us, there are brighter days ahead.

We anticipate adjustments to our national and Department-level strategies in the coming months, but there is one thing we can be certain those strategies will include: a return to the world stage. As President Biden has said, America is back.

Cyber is a team sport, and I look forward to building and strengthening our alliances and partnerships to drive toward a safer, more secure cyberspace for all.

We may face many challenges in the cyberspace domain, but I am confident that by working with the Congress and our critical stakeholders inside and outside the U.S. Government, the Department is equipped to ensure that the U.S. military continues to compete, deter, and win in cyberspace.

**Mieke Eoyang**
**Deputy Assistant Secretary of Defense for Cyber Policy**

Ms. Mieke Eoyang is the Deputy Assistant Secretary of Defense for Cyber Policy. The Cyber Policy office is responsible for establishing DoD cyberspace policy and strategy, providing guidance and oversight on DoD cyberspace activities, and managing DoD's primary external relationships across the U.S. government, key domestic stakeholders, and our allies and partners.

Prior to that she was the Senior Vice President for the National Security Program at the think tank, Third Way, where she led their work on a wide range of national security issues including on foreign policy, Congress' role in the national security policymaking process, non-proliferation, intelligence oversight, electronic surveillance, cybersecurity. She was the founder of the organization's Cyber Enforcement Initiative which focused on improving the government's efforts to impose consequences on the human behind malicious cyber activity.

Before joining Third Way, she was the Chief of Staff to Rep. Anna G. Eshoo (D-CA) having previously served as the Subcommittee Staff Director for Intelligence Community Management on the House Permanent Select Committee on Intelligence. While there, she was the committee's lead for cybersecurity, personnel management and worked on electronic surveillance reform, among other issues.

Prior to that, she served as the Defense Policy Advisor to Senator Edward M. Kennedy, advising him on all matters related to the Senate Armed Services Committee and Defense Appropriations during the Iraq War. Earlier in her career, she served as the lead Democratic Professional Staff Member on the House Armed Services Committee for the Military Personnel Subcommittee. Ms. Eoyang received her Juris Doctor from the University of California, Hastings College of the Law, and her Bachelor's Degree from Wellesley College.

POSTURE STATEMENT OF

GENERAL PAUL M. NAKASONE

COMMANDER, UNITED STATES CYBER COMMAND

BEFORE THE 117TH CONGRESS

HOUSE COMMITTEE ON ARMED SERVICES

SUBCOMMITTEE ON CYBER, INNOVATIVE TECHNOLOGIES
AND INFORMATION SYSTEMS

14 MAY 2021

Chairman Langevin, Ranking Member Stefanik and distinguished members of the Committee, I am honored to appear before you today and to represent the men and women of United States Cyber Command (USCYBERCOM). 2020 presented some unique challenges to USCYBERCOM that will inform our actions over the next year. Indeed, 2021 is offering opportunities for USCYBERCOM to build upon.

USCYBERCOM was established in 2010 and became a unified combatant command in 2018. Our mission is to plan and execute global cyberspace operations, activities, and missions to defend and advance national interests in collaboration with domestic and international partners across the full spectrum of competition and conflict. We direct, synchronize, and coordinate cyber planning and operations. Our three enduring lines of operation include:

- Provide mission assurance for the Department of Defense (DoD) by directing the operation and defense of the Department of Defense Information Networks (i.e. the DoDIN) and its key terrain and capabilities;

- Defeat strategic threats to the United States and its national interests; and

- Assist Combatant Commanders to achieve their missions in and through cyberspace.

In January 2021, our Cyber Mission Force (CMF) comprised roughly 6,000 service members and civilians out of an authorized total of 6,187 positions. This includes Guard and Reserve personnel on active duty serving at our headquarters and on our CMF teams. For comparison, the 2018 DoD *Cyber Posture Review* counted about 238,000 personnel in the Department's cyberspace operations forces, including the CMF, USCYBERCOM's subordinate command elements, cybersecurity service providers (CSSPs), special capability providers, and specialty units.

The DoD depends on USCYBERCOM and its performance. Every operational plan and every mission across the Department builds from the assumption that we will be able to assure that the bandwidth and data that military forces require will be accessible and trustworthy.

*A Look Back at 2020*

In 2020 USCYBERCOM made progress in the face of significant challenges. Operationally, we helped to lead the successful defense of the 2020 elections and played a key role in the Government-wide response to the SolarWinds, Microsoft Office 365, and related breaches. We also gained Departmental commitments to enhanced resources and a better alignment of cyber responsibilities and authorities for the Command (including the FY21 NDAA elimination of the $75 million cap on funds available for acquisition activities).

We saw increasingly capable cyber adversaries target the United States via influence operations, efforts to compromise sensitive data, and attempts to gain access to our weapons systems. Adversaries still seek to exploit gaps and seams between our organizations and authorities:

- China is a sophisticated cyber adversary. Beijing conducts effective cyber espionage and other operations and has integrated cyber activities into its military and national strategy. China remains focused on shaping the global narrative and exploiting American networks and cyber systems.

- Russia is a sophisticated cyber adversary. It has demonstrated its ability to conduct power influence campaigns utilizing the medium of social media. Moscow conducts effective cyber espionage and other operations and has integrated cyber activities into its military and national strategy. Russia remains focused on shaping the global narrative and exploiting American networks and cyber systems.

- North Korea has demonstrated the capability and intent to impact the United States in cyberspace. Its regime sponsors cyber exploitation of international finance via cyber means to evade United Nations sanctions.

- Iran has demonstrated both the capability and intent to impact the U.S. in cyberspace. Iranian cyber actors are growing adept at exploiting systems as well as delivering disruptive and destructive attacks and have attempted to execute a series of influence campaigns.

- Finally, non-state actors and criminal cartels remain threats to us and our interests, whether by financing, recruiting, and advertising violent extremist tactics, or through the exploitation of data for theft or ransom.

All of these actors felt the effects of the COVID-19 pandemic – as did we. Fortunately, we saw their operational tempo briefly diminish at roughly the same time that we had to restrict access to our facilities. COVID-19 mitigations remain in full effect across our enterprise, and we are vaccinating our personnel as fast as vaccine supplies and local conditions allow. Overall, I was pleased that the pandemic has not limited the force's readiness or posture to fulfill its missions.

Last year, I emphasized the importance of defending the election against foreign interference, in part through the Election Security Group (ESG), a combined team from USCYBERCOM and the National Security Agency (NSA). The ESG ensured that intelligence informed whole-of-nation efforts to harden defenses and prevent or disrupt threats to the U.S. elections. We built on lessons from earlier operations and honed partnerships with the Federal Bureau of Investigation (FBI) and the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, sharing information with those who needed it as fast as possible. We also worked with the National Guard Bureau to create a mechanism that enabled Guard units to share information about incidents quickly, easily, and uniformly. We called it the Cyber 9-line, given the nine lines of information a reporting entity would complete. As the election approached, every state had joined this program. I am proud of the work the Command and the ESG performed, as part of a broader government effort, to deliver a safe and secure 2020 election.

USCYBERCOM conducted more than two dozen operations to outpace foreign threats before they interfered with or influenced our elections in 2020. Three points stand out for me:

- First, USCYBERCOM must be ready and able to act. Threats can arise rapidly, and opportunities can be fleeting. Our ability to operate successfully in cyberspace is a function of streamlined processes, mission readiness, and the trust of our various mission partners.

- Second, USCYBERCOM's partnership with NSA remains the foundation of our success. Working together under one leader again demonstrated the ability of both organizations to operate with speed and agility to achieve outcomes for the nation.

- Third, we enable our foreign allies and partners, just as they remain crucial to our ability to act. Operating with allies and partners allows each to magnify each other's unique strengths. Our efforts over the last year highlight the value of not only operating but training together as well.

USCYBERCOM supported the combatant commands with a wide range of other operational accomplishments over the last year. Counterterrorism operations in cyberspace are continuous, helping to protect the force and prosecute targets in Afghanistan and other regions on behalf of USCENTCOM and USSOCOM. We are also shifting JTF-Ares' focus (though not all of its missions) from counterterrorism toward heightened support to strategic competition, particularly in USINDOPACOM's area of responsibility.

In recent months our priority has been mitigating the threat to federal systems from malicious cyber actors compromising widely-used SolarWinds software and Microsoft Cloud resources, and exposing thousands of public and private systems to targeted exploitation. The U.S. government learned of the compromise in December 2020. As an immediate response to this threat, I directed the creation of a combined USCYBERCOM-NSA team in support of the U.S. government's efforts, through the Unified Coordination Group, to mitigate the compromise. To date, we have yet to identify any compromise of DoD information networks in the unclassified or classified domains.

My teams have provided more than 100 days of continuous support to the whole-of-government mitigation effort. I have organized our efforts across three lines of effort:

1. *Bound the Problem*. Using both automated and manual processes, we worked to determine the scope of SolarWinds Orion software products employed across the DoDIN. Each instance was immediately isolated and disconnected from DoD networks. Meanwhile, NSA worked to understand the adversary's intent and illuminate additional tradecraft and infrastructure to inform threat detection and asset response activities. Finally, we prepared to support and assist other federal departments and the Defense Industrial Base in bounding their respective problems.

2. *Expel the Adversary*. This is a continuous process driven by USCYBERCOM's Joint Force Headquarters-Department of Defense Information Networks (JFHQ-DoDIN),

which has directed network administrators to enumerate, isolate, and remediate all affected systems before they are reconnected to the DoDIN. We have yet to find any adversary presence on the DoDIN as a result of the SolarWinds compromise. We continue to work with federal partners to share best practices and expertise to expel the adversary from affected systems.

3. *Impose Cost.* USCYBERCOM and NSA are both planning and informing the whole-of-government response options to the SolarWinds supply-chain and Microsoft Office 365 compromises and the adversary's associated campaign. Policymakers are considering a range of options, including costs that might be imposed by other elements of our government.

Two recent incidents show well-resourced and sophisticated adversaries exploiting a gap in the nation's ability to monitor U.S. cyberspace infrastructure while conducting operations from within the boundaries of the United States. The SolarWinds incident occurred through the highly skilled means of an adversary against a US company's supply chain. Malicious code was inserted in software and was then propagated when other users downloaded this update. At nearly the same time, the server hack associated with Microsoft Exchange showcased the ability of another adversary to exploit vulnerabilities and attack systems around the world. These two cases demonstrate the broadening scope, scale and sophistication employed by some adversaries—they reinforce the imperative and importance for government and industry to collaborate in detecting and responding to malicious cyber activity. The United States Government, in tandem with industry partners, must improve its defensive posture to prevent and/or minimize the impacts and impose cost in time and money on those who exploit such vulnerabilities and target American companies and citizens.

*Our Focus for 2021*

My focus for the coming year is to broaden the foundation for operational progress. In particular, we are building on recent guidance from the Department, seeking to promote sustainable readiness; to improve training; and to attract and retain high-end talent across our military, civilian, active duty, and Reserve workforces.

Cybersecurity and defensive cyberspace operations mean mission assurance for the DoD and thus are integral to our nation's security. For 2021 and the years ahead, there are several areas where USCYBERCOM plans to improve. Our growth to date has highlighted certain misalignments between the responsibilities I have as Commander and the resources and authorities to execute those responsibilities. The following initiatives reflect the Department's guidance to align mission, responsibility, and accountability for the Command:

Accountability: The Secretary of Defense in late 2020 issued a directive emphasizing accountability by aligning cybersecurity efforts with operational risk decisions. USCYBERCOM will improve risk management while also holding commanders and directors accountable for their risk decisions.

Budget Control: USCYBERCOM's FY21 budget is roughly $605 million, which covers the headquarters staff and the Cyber National Mission Force. Meanwhile, 27 different components shape the Department's overall Cyber Activities Budget, which averages about $10 billion a year. USCYBERCOM is working with the Services and the Office of the Secretary of Defense to direct CMF funding in a more collaborative effort while allowing for informed tradeoffs (across the Services) based on operational needs.

Team Realignment: The CMF's original force structure was set in 2012, and several teams were originally aligned to support the counter-terrorism fight. With the advent of strategic competition, USCYBERCOM is realigning some teams to focus on key nations.

Force Growth: Recent demand across the DoD has demonstrated that the original 133 teams in the CMF are not enough. The strategic environment has changed since the original CMF was designated in 2012. Added forces will ensure USCYBERCOM can fulfill its responsibility as both a supported and a supporting command.

Training: USCYBERCOM is centralizing the provision of advanced training. The Army will serve as the executive agent for advanced cyberspace training. This will ensure that each Service presents well-trained personnel to USCYBERCOM who can contribute to our missions as soon as they arrive in the Command.

Sustainable Readiness: We are improving our ability to monitor the status of forces down to the team, mission element, and even individual levels in order to identify and remedy challenges to gaining and maintaining necessary readiness. We are working to better provide commanders with the situational awareness they require to assess risks and make informed decisions, not just in operations but also in maintaining the force as a whole. I am pleased with the progress here, but more needs to be done.

Domestic and International Partnerships: Such ties collectively are a force multiplier when it comes to cyber operations. USCYBERCOM is enhancing its existing relationships and forging new ones based on U.S. Government priorities. We have been sending teams to "hunt forward" at the invitation of foreign governments, helping them find adversary malware on their governmental systems. Such persistent engagement in cyberspace lets the Command deliver outcomes in competition with adversaries, both by enabling our partners and by acting when called upon.

Realigning Cyber Protection Teams: USCYBERCOM is working with the combatant commands to ensure they have dependable defensive support for their missions while we retain forces to deal with global challenges to the DoDIN.

USCYBERCOM executes its operations employing the Joint Cyber Warfighting Architecture (JCWA), which is a cyber capabilities architecture that enables us to act against our adversaries in competition, crisis, and conflict in cyberspace. When fully realized, JCWA will provide unified capabilities for Cyberspace Operations Forces, integrating the data from offensive and defensive cyberspace operations in ways that help commanders gauge risk, make timely decisions, and act.

To help drive operational needs and capability development, USCYBERCOM activated a JCWA Capability Management Office (JCMO). This promoted unity of effort across the Command, the Services, and Department in building the many and varied components that together comprise the JCWA. Those components include:

- Improved operational architectures that give our forces the ability to operate at scale from multiple locations;

- Data sharing and analytics (the Unified Platform) that provide insight for offensive and defensive operations;

- Command and control features that display the readiness of our forces as well as operational status. One tool in this suite, Project IKE (soon to be Joint Cyber Command and Control), has ensured we can measure readiness down to the individual level while informing exercises, training, recruiting, and even retention;

- Tool development capabilities that are responsive to operational needs and increasingly able to focus talents and innovations when and where they are needed most;

- Realistic collective training (via the Persistent Cyber Training Environment, or PCTE) that lets us rehearse missions and even exercise with Reserve Component and foreign partners.

Last year's operational successes would not have been possible without the Department's Total Force, which includes the National Guard and the Reserves. Before the 2020 elections, the Guard provided local connectivity and insight on key events like Super Tuesday. They also played vital roles during the pandemic. For example, the National Guard and Reserve provided cyber forces in response to a Defense Support to Civil Authorities (DSCA) request from the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency in support of Operation Warp Speed, providing cybersecurity support to the pharmaceutical industry as it developed COVID-19 vaccines in record time.

Finally, the Reserve Component's ability to hire qualified cyber warriors who decide to leave active duty upon completion of their service commitment has proved invaluable. Members of the National Guard and Reserve have relevant private-sector experience in fields of strong interest to the Department, and many of them work for some of the nation's top-tier technology companies. The Air National Guard, for example, has built both offensive and defensive cyber units in which members departing active duty can transfer to part-time status while they pursue careers in the civilian sector.

As the trailblazer for the DoD's Cyber Excepted Service (CES) personnel authority, the Command benefits from flexible hiring authorities in filling civilian vacancies and recruiting top cyber talent. Even with COVID-19 impacts and security clearance timelines that continue to challenge the whole Department, USCYBERCOM offered competitive compensation and incentives to our best candidates. We are also partnering with the National Security Innovation

Network (NSIN), a Defense Innovation Unit program office, to conduct a virtual hire-a-thon that runs through this month. The most recent hire-a-thon garnered more than 260 resumes from people eager to join our team, and similar events are planned for the future. Civilians continue to play an important role for USCYBERCOM, providing vital continuity in several areas.

*Conclusion*

USCYBERCOM is actively engaged in addressing the nation's challenges from sophisticated and evolving adversaries in cyberspace. The Command supports other combatant commanders in every geographic and functional area of responsibility, while implementing the Department's Defend Forward strategy and enhancing our capabilities.

For the year to come our priorities are set. We will focus on strategic competition through persistent engagement, especially in support of USINDOPACOM, and particularly through improving the efficiency and effectiveness of DoDIN operations and defensive cyberspace missions. To prepare for the approved growth in the CMF, we will enhance our control over resources for the force, improve its readiness (including the metrics we require in doing so), and consolidate CMF training. We will integrate the development efforts ongoing in support of the JCWA. We will also improve recruitment and retention of top military and civilian performers. All of these measures will enhance the proficiency of USCYBERCOM and boost its ability to provide defensive security assurance and options for policymakers and commanders at the senior levels of the government and the Department of Defense.

The men and women at USCYBERCOM are grateful for the support this Committee and Congress in these efforts. I thank you for that support in the important work that we have undertaken together. And now I look forward to your questions.

**General Paul M. Nakasone**
**Commander, U.S. Cyber Command and**
**Director, National Security Agency/Chief, Central Security Service**

General Paul M. Nakasone assumed his present duties as Commander, U.S. Cyber Command and Director, National Security Agency/Chief, Central Security Service in May 2018.

He previously commanded U.S. Army Cyber Command from October 2016 - April 2018.

A native of White Bear Lake, Minnesota, GEN Nakasone is a graduate of Saint John's University in Collegeville, Minnesota, where he received his commission through the Reserve Officers' Training Corps.

GEN Nakasone has held command and staff positions across all levels of the Army with assignments in the United States, the Republic of Korea, Iraq, and Afghanistan.

GEN Nakasone commanded the Cyber National Mission Force at U.S. Cyber Command. He has also commanded a company, battalion, and brigade, and served as the senior intelligence officer at the battalion, division and corps levels.

GEN Nakasone has served in Joint and Army assignments in the United States, the Republic of Korea, Iraq, and Afghanistan. His most recent overseas posting was as the Director of Intelligence, J2, International Security Assistance Force Joint Command in Kabul, Afghanistan.

GEN Nakasone has also served on two occasions as a staff officer on the Joint Chiefs of Staff.

GEN Nakasone is a graduate of the U.S. Army War College, the Command and General Staff College, and Defense Intelligence College. He holds graduate degrees from the U.S. Army War College, the National Defense Intelligence College, and the University of Southern California.

GEN Nakasone's awards and decorations include the Distinguished Service Medal (with oak leaf cluster), the Defense Superior Service Medal (with three oak leaf clusters), Legion of Merit, Bronze Star, Defense Meritorious Service Medal (with oak leaf cluster), Army Commendation Medal, Joint Service Achievement Medal (with oak leaf cluster), Army Achievement Medal (with four oak leaf clusters), Joint Meritorious Unit Award, Iraq Campaign Medal, Afghanistan Campaign Medal, Combat Action Badge, and the Joint Chiefs of Staff Identification Badge.

GEN Nakasone and his wife are the proud parents of four children, who form the nucleus of "Team Nakasone."

**WITNESS RESPONSES TO QUESTIONS ASKED DURING THE HEARING**

MAY 14, 2021

## RESPONSE TO QUESTION SUBMITTED BY MR. LARSEN

General NAKASONE. USCYBERCOM defers to Office of Secretary of Defense. [See page 11.]

---

## RESPONSE TO QUESTION SUBMITTED BY MS. ESCOBAR

General NAKASONE. Cyber Command participated in two Pathfinder initiatives with Department of Homeland Security (DHS).

The first was with DHS, the Treasury, and the Financial Systemic Analysis & Resilience Center (recently renamed to simply the Analysis & Resilience Center) to look at vulnerabilities in one of the financial sector's most critical systems, the Wholesale Payment System. The results of this collaboration over a 15 month period were collaborative analysis, mitigation development, and information sharing to provide better threat identification and early warning to improve security of critical financial infrastructure.

For the second, USCYBERCOM partnered with DHS, Energy, and a private energy sector reliability coordinator in order to evaluate ICS/SCADA vulnerabilities highlighted by Energy's Cybersecurity Risk Information Sharing Program (CRISP) and DHS's Automated Indicator Sharing (AIS) System. This effort demonstrated the usefulness of CRISP and AIS to utility companies, reliability coordinators, Treasury and DHS, and underscored the requirements that remain for USCYBERCOM to derive impactful information from these sharing initiatives to drive military cyber operations.

Perhaps the most important outcome from these Pathfinder efforts was the acknowledgement and increasing understanding of how USCYBERCOM must interoperate with DHS as the lead federal agency for CIKR cybersecurity. We have demonstrated this understanding successfully, on a small scale, through efforts enabled by legislation like Sec. 1650 of the 2019 NDAA. As a result of this legislation, USCYBERCOM continues to support DHS with personnel that provide a critical and sustained link between our Departments. Additionally, it is important to note, the Pathfinder efforts are not the only venues or conduits for collaboration but have been important in testing new processes and developing useful routines and habits, which CYBERCOM has found valuable. [See page 24.]

---

## RESPONSE TO QUESTION SUBMITTED BY MRS. BICE

Ms. EOYANG. DOD-authorized commercial cloud services, such as milCloud 2.0, provide a computing infrastructure that can be more secure than the legacy computing infrastructure. However, milCloud 2.0 infrastructure alone may be insufficient to address potential vulnerabilities in the software components and IT operations that compose the complete system. This is because Cloud computing generally consists of three layers: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). MilCloud 2.0 only targets the IaaS layer, and thus it is still necessary to redesign legacy applications to take full advantage of the Cloud, including updating any out-of-date software components. Fully addressing the range of potential application vulnerabilities often necessitates adopting strong access management tools and policies for access to cloud resources, implementing effective security automation, and improving the application's cybersecurity controls. [See page 24.]

## QUESTIONS SUBMITTED BY MEMBERS POST HEARING

MAY 14, 2021

## QUESTIONS SUBMITTED BY MR. KIM

Mr. KIM. Section 1729 of the FY21 NDAA requires the Secretary of Defense to conduct an evaluation of the statutes, rules, regulations and standards that pertain to the use of the National Guard for the response to and recovery from significant cyber incidents. This evaluation is due to be submitted to Congress no later than June 29. Can you provide an update on this study, including when Congress should expect to see the results and any preliminary findings?

Ms. EOYANG. DOD completed the evaluation and intends to deliver its results no later than June 29, 2021, as required by section 1729 of the National Defense Authorization Act for Fiscal Year 2021 (NDAA for FY 2021).

Mr. KIM. Recently, NSA purchased a cybersecurity curriculum for use in its educational programs to build talents within DOD to address future workforce needs in the critical cyberspace field. However, it is my understanding that DHS's Cybersecurity and Infrastructure Security Agency (CISA) already owns and operates a more comprehensive curriculum for cybersecurity through Cyber.org that achieves the same goals and is available to NSA for use. Can you explain why the purchase of this additional curriculum was necessary and assess the level of information sharing and cooperation between various agencies when it comes to workforce development programming in the cyberspace field?

General NAKASONE. NSA did not purchase the referenced cybersecurity curriculum to use in its educational programs; the National Cryptologic Foundation (formerly Museum), a private entity separate from NSA, procured this product for use in its Center for Cyber Education and Innovation.

CISA's Cyber.org program focuses on K–12 curriculum, whereas NSA's cyber education programs focus on college-prep curriculum for the pipeline into Centers of Academic Excellence. That said, NSA is a partner with CISA, and all efforts are fully coordinated to achieve complementary programs for cyber education, with collaboration on informational materials to provide clarity to government partners and educators on the attributes and recommended usage of their programs, and how to access materials and resources. For instance, NSA's GenCyber Program uses the Cyber.org curriculum.

---

## QUESTIONS SUBMITTED BY MR. MOORE

Mr. MOORE. The DOD currently relies on over 2,500 data centers that in many cases have reached the limits of their service life and can no longer be upgraded to meet current cyber threats. How will migration to the cloud address these shortcomings?

Ms. EOYANG. Cloud environments enable data center consolidation by allowing organizations to focus less on servers and storage and more on software applications and the data environment. DOD has used its Data Center Optimization Initiative (DCOI), a Department-wide effort to optimize data centers for greater efficiency, performance, security, and affordability, as an opportunity to evaluate which applications should be retired, consolidated, or replaced, and to migrate needed applications to the Department's cloud services. By 2025, this will allow the Department to close a projected 2,100 data centers that have reached the end of their service lives.

The reduced and re-ordered data center inventory has also enabled DOD to manage cyber vulnerabilities more effectively and to focus investments in cyber security in its enterprise data centers. The DOD's DCOI end-state is projected to have approximately 1,500 data centers Department wide.

Mr. MOORE. The DOD's Cloud Strategy identifies three clouds: milCloud 2.0, the Defense Enterprise Office Solution (DEOS), and the JEDI general purpose cloud. 4th estate agencies were directed to move to new systems, but adoption has been slow. Will the DOD enforce the 2018 mandate directing cloud migration by the 4th estate?

Ms. EOYANG. Yes. DOD is enforcing the 2018 mandate by directing the 14 Fourth Estate agencies to migrate to cloud services through the Cloud and Data Center Optimization Initiative, a subset of the Department's DCOI.

Mr. MOORE. The DOD's Cloud Strategy identifies three clouds: milCloud 2.0, the Defense Enterprise Office Solution (DEOS), and the JEDI general purpose cloud. 4th estate agencies were directed to move to new systems, but adoption has been slow. Will the DOD enforce the 2018 mandate directing cloud migration by the 4th estate?

General NAKASONE. USCYBERCOM defers to the office of the DOD CIO within OSD.

○