[H.A.S.C. No. 116–14]

HEARING

ON

NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2020

AND

OVERSIGHT OF PREVIOUSLY AUTHORIZED PROGRAMS

BEFORE THE

COMMITTEE ON ARMED SERVICES
HOUSE OF REPRESENTATIVES
ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

SUBCOMMITTEE ON INTELLIGENCE AND EMERGING THREATS AND CAPABILITIES HEARING

ON

FISCAL YEAR 2020 BUDGET REQUEST FOR U.S. CYBER COMMAND AND OPERATIONS IN CYBERSPACE

HEARING HELD
MARCH 13, 2019

U.S. GOVERNMENT PUBLISHING OFFICE
36–300 WASHINGTON : 2019

SUBCOMMITTEE ON INTELLIGENCE AND EMERGING THREATS AND CAPABILITIES

JAMES R. LANGEVIN, Rhode Island, *Chairman*

RICK LARSEN, Washington
JIM COOPER, Tennessee
TULSI GABBARD, Hawaii
ANTHONY G. BROWN, Maryland
RO KHANNA, California
WILLIAM R. KEATING, Massachusetts
ANDY KIM, New Jersey
CHRISSY HOULAHAN, Pennsylvania
JASON CROW, Colorado, *Vice Chair*
ELISSA SLOTKIN, Michigan
LORI TRAHAN, Massachusetts

ELISE M. STEFANIK, New York
SAM GRAVES, Missouri
RALPH LEE ABRAHAM, Louisiana
K. MICHAEL CONAWAY, Texas
AUSTIN SCOTT, Georgia
SCOTT DESJARLAIS, Tennessee
MIKE GALLAGHER, Wisconsin
MICHAEL WALTZ, Florida
DON BACON, Nebraska
JIM BANKS, Indiana

JOSH STIEFEL, *Professional Staff Member*
PETER VILLANO, *Professional Staff Member*
CAROLINE KEHRLI, *Clerk*

CONTENTS

Page

STATEMENTS PRESENTED BY MEMBERS OF CONGRESS

Langevin, Hon. James R., a Representative from Rhode Island, Chairman, Subcommittee on Intelligence and Emerging Threats and Capabilities 1
Stefanik, Hon. Elise M., a Representative from New York, Ranking Member, Subcommittee on Intelligence and Emerging Threats and Capabilities 3

WITNESSES

Nakasone, GEN Paul M., USA, Commander, U.S. Cyber Command, and Director, National Security Agency 8
Rapuano, Kenneth P., Assistant Secretary of Defense for Homeland Defense and Global Security, and Principal Cyber Advisor, U.S. Department of Defense 6

APPENDIX

PREPARED STATEMENTS:
Langevin, Hon. James R. 33
Nakasone, GEN Paul M. 50
Rapuano, Kenneth P. 36

DOCUMENTS SUBMITTED FOR THE RECORD:
[There were no Documents submitted.]

WITNESS RESPONSES TO QUESTIONS ASKED DURING THE HEARING:
Ms. Stefanik 69

QUESTIONS SUBMITTED BY MEMBERS POST HEARING:
Mr. Larsen 73

FISCAL YEAR 2020 BUDGET REQUEST FOR U.S. CYBER COMMAND AND OPERATIONS IN CYBERSPACE

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ARMED SERVICES,
SUBCOMMITTEE ON INTELLIGENCE AND EMERGING THREATS AND CAPABILITIES,
Washington, DC, Wednesday, March 13, 2019.

The subcommittee met, pursuant to call, at 2:19 p.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 INTELLIGENCE AND EMERGING THREATS AND CAPABILITIES

Mr. LANGEVIN. The subcommittee will come to order.

I want to welcome everyone to today's hearing on the fiscal year 2020 budget request for the military operations in cyberspace. I was unavoidably detained, so I apologize to everyone for making you wait, but I am glad we could get this underway.

Technology and the internet have fundamentally changed how citizens, the Nation, the military, and our adversaries in the world operate. We have more access to information and lower barriers to conduct commerce. We collectively benefit from the opportunities afforded by the technology that we incorporate into our lives. However, the connections that we rely on also create vulnerabilities and new potential avenues for our adversaries to exploit at our Nation's expense.

Cyber, as we understand it in government, will always be something that creates risk to go along with its great promise. The issues that stem from our increasing dependence on technology will never be purely military or solely for the military to solve. Technology has increased the interconnectedness of our society, and the problems that have come with it will only be solved with interconnected, interdisciplinary approaches.

The Department [of Defense] will have to work in new ways with stakeholders from agencies as varied as the Department of Commerce and the Department of Education and with nongovernmental stakeholders such as private industry and academia.

The executive branch will have to work diligently to address and solve the cyber challenges facing the Nation. Yet this administration has taken actions that call into question the seriousness with which it views this emerging domain. Most notably, the administration eliminated the cybersecurity coordinator position at the National Security Council.

Relatedly, there are several documents pertaining to cyber that Congress has repeatedly requested from the administration and has yet to receive. This includes recent guidance pertaining to operations in cyberspace. Such documents are important to creating a congressional framework for oversight. Withholding these critical documents from Congress impacts our ability to appropriately support the command and may have far-reaching consequences for the National Defense Authorization Act.

At the Cabinet level, the Department of Defense, the U.S. Cyber Command have no shortage of challenges in front of them, issues that often develop and change as fast as the technological landscape. Today we will hear about some of those challenges, including personnel recruitment and retention as well as efforts to protect critical infrastructure in tandem with domestically oriented departments and agencies.

The Cyber Mission Force achieved full operational capability [FOC] last year. This was a notable event, but it would be a mistake to assume that FOC is synonymous with readiness. We must begin to examine the differing standards by which the services are training the teams and whether CYBERCOM [U.S. Cyber Command] is adequately fulfilling its mandate to set training standards and ensure compliance.

Readiness is especially important in the context of the current strategic landscape, which has evolved significantly over the last year. In the fall, the DOD [Department of Defense] released a new cyber strategy that articulated the intent to defend forward and operate across the full spectrum of conflict through persistent engagement.

DOD also completed the inaugural Cyber Posture Review. Under the auspices of new guidance from the administration and the new DOD strategy, CYBERCOM played a crucial role in defending the 2018 elections from interference.

The military's actions in cyberspace were also enabled by multiple provisions in the fiscal year 2019 National Defense Authorization Act [NDAA]. This includes the provision to recognize the activities conducted in cyberspace as traditional military activities.

The fiscal year 2019 NDAA also allowed the National Command Authority to take direct and proportional action in cyberspace against Russia, China, North Korea, and Iran upon determination of a cyberattack against the homeland or U.S. citizens.

Congress and this subcommittee will continue to support military operations and provide the legal authority to enable CYBERCOM success against adversaries in cyberspace. However, we will also remain judicious in our oversight responsibilities to ensure that the Department operates in a manner that enhances stability in cyberspace and that is consistent with both congressional intent and American values.

So I commend CYBERCOM for its efforts during the 2018 elections. However, as a Nation, we can never rest on our laurels. We need to examine the strategic impacts that CYBERCOM operations and other whole-of-government efforts had on an actor seeking to interfere in our elections. Much like the traditional battlefield, we must measure the impact of our operations to assess our warfighting effectiveness toward the larger objectives and ensure that our

strategic vision reflects the realities of our engagement in cyberspace.

CYBERCOM's ability to execute its operations is closely tied to and enabled by its partnership with the National Security Agency [NSA]. These organizations will always have a robust partnership given the dynamism of cyberspace and NSA's deep expertise and enabling role in military cyberspace operations.

At this time, there is still one individual that leads both of these organizations. This arrangement is quite unique within the national security establishment and the intelligence community. However, this arrangement allows for the CMF [Cyber Mission Force] to mature, enables better synchronization of cyberspace operations, and permits proper consideration of the intelligence and military objectives in the domain.

Before any significant changes are implemented in the dual-hat arrangement, this subcommittee expects a robust understanding of how and why it is necessary to split the leadership function of NSA Director and CYBERCOM commander. I believe it would be premature to split these organizations in the immediate future.

CYBERCOM is a maturing organization, and I am proud of the work that we have done on the subcommittee to support its maturation. I have often said that we will never again see modern warfare without a cyber component, so CYBERCOM's continued development will remain an urgent priority.

But it is therefore important that we build for the long term with this sustainable, scalable approach to integrating CYBERCOM into DOD operations and into our whole-of-government approach to protecting our Nation's cyberspace. This is no small task, especially given the newness of this domain. But working together with full transparency, I am confident that we can head off any problems early and ensure that we reap the benefits of a free, open, interoperable, and secure internet.

Before I close, I want to just introduce our two witnesses, which I will do in just a minute. But before I do that, I am going to turn it over to the ranking member for her comments.

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

STATEMENT OF HON. ELISE M. STEFANIK, A REPRESENTATIVE FROM NEW YORK, RANKING MEMBER, SUBCOMMITTEE ON INTELLIGENCE AND EMERGING THREATS AND CAPABILITIES

Ms. STEFANIK. Thank you, Chairman Langevin. Welcome to our witnesses. Secretary Rapuano, welcome back to the committee. And General Nakasone, welcome to your first posture hearing since assuming command in May of last year.

It is fitting that we begin our fiscal year 2020 posture hearing series with cyber policy and U.S. Cyber Command, given the importance of this topic to our overall national security and, indeed, our society as a whole.

The Director of National Intelligence [DNI] in his most recent Worldwide Threat Assessment stated, quote, "At present, China and Russia pose the greatest espionage and cyber attack threats, but we anticipate that all our adversaries and strategic competitors

will increasingly build and integrate cyber espionage, attack, and influence campaigns into their efforts to influence U.S. policies and advance their own national security interests," end quote.

In our oversight role as a subcommittee, we have seen China and Russia aggressively leverage and integrate cyber information and communication technologies in a seamless way, while also utilizing top-down, government-driven agendas and strategies. As I have said before, dictators have that advantage, and their use of technologies and information is as much about exerting control over their own populations as it is confronting free societies like ours.

Since our last Cyber Command posture hearing and over the course of the last year, a lot has happened. Given this, I consider us to be at a major inflection point. We have seen Cyber Command fully elevated as a functional combatant command, and the force has achieved full operational capability, or FOC.

Recent changes to Presidential cyber policies and strategies, as well as authorities granted in the NDAA, have focused the mission set, yielded impressive operational results, and postured our Nation for strategic challenges ahead. And while we have seen these successes, the DNI's recent testimony reminds us that our adversaries are not giving us any room to breathe.

Case in point: While many of our recent operational successes have been related to securing our 2018 midterm elections, I can assure you that the adversarial influence campaign for the 2020 elections is already underway.

Further, while most of our cyber forces are fully capable on paper, they are not fully ready in practice. Standards and capabilities have yet to be defined and understood across each of the services. Relationships and responsibilities are still being worked out between Cyber Command, regional combatant commanders, and each of the services.

In short, we continue to mature, and the road ahead to true cyber readiness remains long. I am confident that our witnesses before us today fully understand these challenges and I look forward to our dialogue.

It is worth noting that our military cyber forces are only as good as the technology they depend on, and if we don't concurrently modernize our information and communication technologies across the Department, we will continue along with one hand tied behind our back.

And when I think about the promise of emerging and revolutionary technologies such as artificial intelligence, 5G, high-performing computing, and even quantum computing, my enthusiasm is unfortunately dampened when I am reminded of our Achilles' heel that is the Department's outdated and vulnerable IT [information technology] infrastructure.

So in our conversation today and moving forward, as we build the National Defense Authorization Act for fiscal year 2020, we must continually keep in mind that IT modernization, cybersecurity, and information assurance are primary prerequisites for the future of warfare, where information and data are strategic resources to be fully protected, preserved, and enabled.

The Department can and must do better in this area. As before, I trust each of our witnesses here today understand these challenges.

Lastly, I would be remiss if I didn't mention the importance of congressional oversight of current operations, including cyber operations. Now, more than ever, it is critical that the DOD communicates with this committee early and often on all aspects of cyber operations and related intelligence activities.

This will ensure that we, as your principal oversight committee, remain fully and currently informed so that we can resource you properly and provide relevant authorities that allow us to stay well ahead of our adversaries in cyberspace and information warfare.

I look forward to talking about that in our closed classified session. We have a lot to talk about. So again, thank you, and I yield back to Chairman Langevin.

Mr. LANGEVIN. I want to thank the ranking member.

I want to now welcome our witnesses here today, starting with Mr. Kenneth Rapuano, who serves as both the Assistant Secretary of Defense for Homeland Defense and Global Security and as the Principal Cyber Advisor to the Secretary of Defense.

Prior to returning to government service, Mr. Rapuano worked for the federally funded research and development corporations, focusing on issues related to homeland security, counterterrorism, and countering weapons of mass destruction.

Mr. Rapuano served as the Deputy Homeland Security Advisor in the George W. Bush administration. He served 21 years in Active Duty and the Reserves as a Marine Corps infantry and intelligence officer, and we want to welcome Mr. Rapuano here today.

Also, General Paul Nakasone serves in three capacities currently: Commander of U.S. Cyber Command, Director of the National Security Agency, and the Chief of the Central Security Service.

Before his current role, he commanded U.S. Army Cyber Command and has served as a career intelligence officer through his 32 years in uniform. This is General Nakasone's first appearance before the subcommittee since assuming command of CYBERCOM.

General Nakasone, it is a pleasure to welcome you here today.

And I thank both of you for your service to the country and thank you again for being here today.

As a reminder, after this open session, we are going to move into room 2216 for a closed, member-only session.

So with that, before opening statements, though, I do have to note that Secretary Rapuano's statement was delivered only this morning. That is more than 40 hours past the committee rules deadline and only 6 hours before the start of this hearing. Getting the testimony that late does the subcommittee a disservice, and really it does the Department a disservice.

I know that there are many hoops that you have to go through before the statement in the interagency is approved, but that is way past the time that is acceptable, especially given the importance of today's topic and the subcommittee's continued interest in advancing our Nation's cyber capabilities.

So although I am going to allow for the reading of the statement today, in the future I expect full compliance with the committee

rules, as outlined by the staff and as outlined in your official invitation letters.

So with that, we will now hear from our witnesses and then we are going to move to the question-and-answer period.

Secretary Rapuano, we will start with you.

STATEMENT OF KENNETH P. RAPUANO, ASSISTANT SECRETARY OF DEFENSE FOR HOMELAND DEFENSE AND GLOBAL SECURITY, AND PRINCIPAL CYBER ADVISOR, DEPARTMENT OF DEFENSE

Secretary RAPUANO. 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, to report on the significant progress the Department of Defense has made over the last year in regard to cyber strategy and operations.

Over the last year, the Department published a new, more proactive strategy for cyberspace and is moving forward with implementation of that strategy, using the first-ever Cyber Posture Review and the elevation of U.S. Cyber Command.

Our new approach has been enabled by the issuance of new Presidential guidance on cyberspace authorities and legislation. We leveraged all of these tools last year as we worked with our partners to ensure the security of the 2018 U.S. midterm elections.

The DOD Cyber Strategy makes clear that the ongoing campaigns of malicious cyber activity conducted by states like China and Russia are a strategic threat. Our competitors are conducting long-term, strategically focused campaigns in and through cyberspace that include stealing sensitive Department of Defense information to undermine our military advantages and place our critical infrastructure at risk.

For this reason, DOD Cyber Strategy embraces a proactive and assertive approach during day-to-day competition to deter, disrupt, and defeat these threats. Our systems must be cyber-hardened, resilient, and secure. We must defend national critical infrastructure from attacks, a new area of emphasis for the Department of Defense, and secure Department of Defense information wherever it resides.

This strategy prioritizes expanding cyber cooperation with our interagency, industry, and international partners to advance our mutual interests. The Defense Cyber Strategy mandates that the Department of Defense cyberspace forces must be defending forward, disrupting threats at the source before they reach U.S. networks. The Department must routinely operate in non-U.S. networks in order to observe threats as they are forming and have the ability to disrupt them.

This is critical to increasing military readiness. We cannot be fully prepared to take effective action in a potential conflict unless we have already developed the tools, accesses, and experience through our actions day to day.

We have worked in partnership with Congress to ensure that the authorities and policies currently in place governing cyberspace operations enable our strategic approach to competing and prevailing in this domain.

Several changes during 2018 have been particularly impactful. This includes the President's approval of an updated policy on U.S. cyber operations.

The 2019 NDAA affirms the President's authority to counter active, systemic, and ongoing campaigns in cyberspace by our adversaries against the government and people of the United States, as well as clarifies that certain cyber operations and activities are traditional military activities. Thank you very much for your support.

We have also focused on how our cyber forces operate in the homeland. For example, we are currently reissuing a memorandum detailing how National Guard personnel can use certain DOD information, networks, software, and hardware for cyberspace op [operation] activities in State status.

We have also devoted focused attention during the last year to building and enhancing our relationships with other U.S. Government department and agencies, industry, and our allies and partners. Last year, the Department signed a joint memorandum of understanding with the Department of Homeland Security detailing how our two departments can cooperate in order to secure and defend the homeland from cyber threats.

The theft of sensitive DOD information from our defense industrial base [DIB] is something that puts our future military technological advantage at risk. DOD is intensifying its efforts with industry and across the U.S. Government to implement cybersecurity protections and to share cyber threat information with our DIB partners.

The Department continues to work to strengthen the capacity of our international allies and partners to increase DOD's ability to leverage its partners' unique skills, resources, capabilities, and perspectives to enhance our cybersecurity posture.

We advocate for our allies and partners to secure their telecom networks and supply chains. We are also pressing our global partners to hold states that are acting irresponsibly in cyberspace accountable for their actions.

The Cyber Posture Review [CPR] identified gaps between where we are today and where we need to go to achieve our strategic objectives and drove the development of actionable lines of effort that are guiding the work of our Principal Cyber Advisor [PCA] team.

For example, the CPR made it clear that when it comes to cybersecurity we need to more effectively prioritize how we are spending money, allocating resources, and how we recruit and retain the most qualified people.

Our PCA team has also worked with the DOD Chief Information Officer to identify the top 10 areas where we face the greatest risk. We are currently working through pilot programs to complete and implement solutions for these challenges.

Another new Department initiative is the Protecting Critical Technology Task Force, established last year to integrate and accelerate the disparate DOD technology protection activities occurring across the Department and develop new, innovative solutions for currently unaddressed problems.

In conclusion, our new strategy has provided us with a roadmap for achieving our objectives in cyberspace, which we are rapidly implementing. We have expanded authorities that enable our mission

to defend forward, and we are doubling down on collaborating with other departments and agencies, industry, and international partners and allies.

I look forward to working with you and our critical stakeholders to ensure that the United States military will continue to compete, deter, and win in cyberspace.

Thank you.

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

Mr. LANGEVIN. Thank you, Mr. Secretary.

General Nakasone, the floor is yours.

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

General NAKASONE. Chairman Langevin, Ranking Member Stefanik, and distinguished members of the committee, thank you for your enduring support and the opportunity to testify today about the hardworking men and women of the United States Cyber Command. I am honored to lead them. I am also honored to sit alongside Assistant Secretary of Defense Rapuano.

As the commander of U.S. Cyber Command, I am responsible for conducting full-spectrum cyberspace operations supporting three mission areas: defend the Nation against cyber threats, defend the Department of Defense information networks, and enable our joint force commanders in pursuit of their mission objectives.

In the cyber domain, we are in constant contact with our adversaries, who continue to increase in sophistication and remain a threat to our national security interests and economic wellbeing.

The National Security Strategy highlighted the return of great power competition. Beyond the near-peer competitors of China and Russia, rogue regimes like Iran and North Korea continue to grow their capabilities. Using aggressive methods, adversaries have until recently acted with little concern for consequences.

The DOD Cyber Strategy identifies the need to defend forward during day-to-day competition with our adversaries. This strategy aims to maintain our superiority in cyberspace through protection of our critical infrastructure and networks. At U.S. Cyber Command, we implement the DOD strategy by adopting an approach of persistent engagement, persistent presence, and persistent innovation.

This past year witnessed the elevation of U.S. Cyber Command to combatant command status, the opening of our Integrated Cyber Center, and our shift from building the force to the readiness of the force.

The defense of the 2018 midterm elections posed a significant strategic challenge to our Nation. Ensuring a safe and secure election was our number one priority and drove me to establish a joint U.S. Cyber Command-National Security Agency effort called the Russia Small Group.

The Russia Small Group tested our new operational approach. With direction from the President and the Secretary of Defense, the Russia Small Group enabled partnerships and action across the government to counter a strategic threat.

Our response demonstrated the value of a tight-knit relationship between U.S. Cyber Command and the National Security Agency, bringing together intelligence, cyber capabilities, interagency partnerships, and our willingness to act.

Through persistent engagement, we enabled critical interagency partners to act with unparalleled coordination and cooperation. Through persistent presence, U.S. Cyber Command and NSA contested adversarial actions, improving early warning and threat identification in support of DHS [Department of Homeland Security] and the Federal Bureau of Investigation.

Beyond the interagency, we partnered and engaged with allies in public and private sectors to build resiliency. For the first time, we sent our cyber warriors abroad to secure networks outside of the DOD Information Network. Our operations allowed us to identify and counter threats as they emerged to secure our own elections and prevent similar threats interfering in those of our partners and allies.

The Russia Small Group effort demonstrated that persistent engagement, persistent presence, and persistent innovation enables success. Effective cyber defense requires a whole-of-nation effort. Our actions are impacting our adversaries. Our shift in approach allows us to sustain key competitive advantages while increasing our cyber capabilities.

As we review lessons learned from securing the 2018 midterm elections, we are now focused on potential threats we could face in 2020.

Looking forward, we need to continue to build a warrior ethos, similar to other warfighting domains. Cyber warriors are and will continue to be in constant contact with our adversaries. There are no operational pauses or sanctuaries. We must ensure sufficient capacity and capability, people, technology, and infrastructure, which we are decisively focused on now.

Through persistent presence, we are building a team of partners that enable us and them to act more effectively. The complex and rapid pace of change in this environment requires us to leverage cyber expertise broadly across public and private sectors, academia, and industry. Therefore, we aspire to increase our effectiveness and capabilities through persistent innovation across these partnerships.

Cyber defense is a team effort. Critical teammates such as the National Guard and Reserve are integral parts of our cyber force. They provide strategic depth and provide the Nation a reserve capacity of capable cyber warriors.

Finally, improving readiness is my key focus area. I continue to work with the services and the Department to accurately measure and maintain readiness, manning, training, equipping, and an ability to perform the mission.

After a year of change and progress, we see 2019 as the year of opportunity. We have much work ahead of us as CYBERCOM matures. I assure you that our people merit the trust you have placed in them and that, with your support, they will accomplish a task that our Nation expects.

Thank you again for inviting me here on behalf of U.S. Cyber Command and for your continued support. I look forward to your questions.

[The prepared statement of General Nakasone can be found in the Appendix on page 50.]

Mr. LANGEVIN. Thank you, General.

I want to thank both General Nakasone and Secretary Rapuano for your testimony.

We are going to now go to questions, myself and then the ranking member, and then we will go to members in the order of their appearance according to seniority.

General, let me start with you. You assessed one year ago to the Senate Armed Services Committee that the Cyber Mission Force and all of its—133 of its teams would be fully operationally capable by June of 2018. Yet, given the different training regimes, the services, there are differences among the teams themselves.

So I just wanted to say, how do you set performance metrics for the 133 teams within the Cyber Mission Force, and how does Cyber Command assess and measure the readiness of all of its teams?

General NAKASONE. Chairman, with regards to readiness, we take a look at two factors: first of all, a measure of quantity, and, secondly, a measure of quality.

The measure of quantity is very familiar to all of the military services. It is the manning, the training, the equipping of a force. It is very easy to calculate it. It is one that our services excel at.

One of the things that we have done at U.S. Cyber Command is establish a joint training standard. That is very important to get at the point of your question with regards to leveling the playing field. One joint standard is important for all our teams to be able to operate under. So whether or not it is a Marine team, an Army team, an Air Force team, that same training standard has been established by U.S. Cyber Command.

I mentioned the quantity aspect. Let me now shift to the quality aspect of how we measure readiness. We can have all the teams that are fully manned, fully equipped, and fully trained, but if you don't have the access, if you don't have the authorities, if you don't have the intelligence, if you don't have the platform, if you don't have the capabilities to accomplish your mission, that is something in cyberspace that puts you uniquely in a very, very difficult position.

So I see that measurement of both quality and quantity as something we will continue to work towards at U.S. Cyber Command.

Mr. LANGEVIN. So let me ask this other follow-up question. So how do you ensure that the teams also are continuously trained and then certified and recertified and prepared for the missions at the individual and the team levels? Since we can't, you know, believe that, you know, it is one and done once it is certified, but, again, the recertification process.

General NAKASONE. Chairman, I think you are speaking of collective training, as we take a look at how our teams are able to perform together. We evaluate that through a number of different mannerisms.

First of all, the ability to do a real-world mission, being able to evaluate what they are doing on a daily basis. Also within exercise.

We have a series of exercises that are set up where we are able to measure the training standard of that team. And then finally, we set parameters in terms of ensuring each team has annual evaluations by third parties. This is something that we have instituted over the past several months. I think it is very effective in terms of being able to take a snapshot in time.

However, with that being said, let me make sure that I reiterate, the teams that we have today are operating every single day against our adversaries. They are very, very capable people, and we will continue to measure their capability. But one of the benefits of working at U.S. Cyber Command is there is never a lack of training opportunities. It is real world every single day.

Mr. LANGEVIN. Thank you. And again to you, General, in your prepared testimony, you noted the incalculable value of the CYBERCOM–NSA relationship when discussing Joint Task Force Ares.

Last Wednesday, Defense One ran a story that you recommended to then-Secretary Mattis in August 2018 that NSA and CYBERCOM be split in 2020. Can you comment on the veracity of the story? And if the story is accurate, can you please explain your recommendations?

General NAKASONE. Chairman, a year ago, when I testified for my confirmation hearings, one of the points that I made in both the Senate Armed Services Committee and the Senate Select Committee on Intelligence was that in my first 90 days as both the commander and the director, I would conduct an assessment of the dual hat and provide those recommendations to the Secretary of Defense and the Chairman of the Joint Chiefs. I completed that assessment in August. The assessment was classified, and it was provided to the Secretary and the Chairman.

I am familiar with the article. I will tell you that the article is not accurate and that, you know, the topics and the actual facts behind that are classified. And so if I could save that, perhaps, for closed testimony.

Mr. LANGEVIN. Fair enough. Thank you. We will follow up on that then, sure, in the closed session.

To Mr. Rapuano, can you describe DOD and specifically CYBERCOM's support to homeland defense, specifically as it relates to the defending-forward concept in the strategy? How is the Department supporting DHS efforts in coordinating with FBI [Federal Bureau of Investigation]?

And how does the Department coordinate with the Cybersecurity and Infrastructure Security Agency at DHS, which has the lead role in protecting civilian government and critical infrastructure?

You know, I think it is important for people to understand, we talk about defending forward and being more proactive, who has responsibility for what though. You know, what is critical infrastructure supposed to do on their own? What is DHS—what is their responsibility? And then also what is DOD, CYBERCOM, NSA's responsibility in all of this, and how does it fit together seamlessly?

Secretary RAPUANO. Thank you, Chairman Langevin.

I would start by saying, of course, that the one mission that only DOD has the authority capabilities, including the breadth and

scope, to conduct is warfighting overseas, addressing adversaries overseas and threats overseas.

That said, we have a renewed focus on supporting our fellow agencies domestically. We really start that in a tri-approach.

First is sharing intelligence and warning, and we do that with the Department of Homeland Security and the FBI. And they provide that information, DHS, to State and local governments; and the FBI, to commercial and other entities.

We defend forward in terms of identifying the source of malevolent cyber activities that are threatening U.S. critical infrastructure or other equities, including malign-influence-type activities that were a significant concern during the recent elections process.

We also have the defense support to civil authorities. As I noted in my statement, we have a memorandum of understanding with DHS to facilitate and expedite our defense support to civil authorities, including DHS but other agencies as well, when they have needs that go beyond what their capacity is to respond to a particular circumstance or threat associated with cyber.

So we are working closely with them. I met with their leadership this week. We meet routinely now to discuss how we move forward, to discuss priorities. We are adding details in terms of how we can facilitate and expedite different levels of support, how we can develop and maintain real-time, full-time connectivity with the Department. We have detailees who perform those kind of roles, and we are looking to instantiate it in the longer-term context.

Mr. LANGEVIN. Thank you, Secretary.

The Chair now recognizes the ranking member for questions.

Ms. STEFANIK. Thank you.

Secretary Rapuano, you mentioned that the new cyber strategy highlights defend forward and persistent presence as major aspects of our new posture. And your statement also outlined some of the steps we are taking to shift to this footing.

But from a policy perspective and with respect to escalation dynamics, have we thought about potentially when and if this more forward and persistent posture could be interpreted as escalatory in nature by our adversaries and perhaps preemptively trigger escalation or retribution?

Secretary RAPUANO. Absolutely. Escalation is a significant concern with all military operations.

In what we call activities in the gray zone or below the spectrum of armed conflict, cyber is an especially attractive tool to our adversaries. And we have noted China and Russia as significant concerns in that context, and we see them applying asymmetric warfare below the spectrum of conflict against us.

We have come to the conclusion—and that is what informed the strategy—that continuing to not respond to those behaviors and those threats that will manifest in a cumulative context—no one of these activities has clearly crossed that line in which a kinetic or military strike would be a response. So if we ignore them, they will continue them, and they will undermine our security in a strategic way.

We have a process that is very risk-based in terms of informing the risk-benefit assessment associated with how we target malevolent activities, how we achieve access. It is a process mentioned

that was enshrined in the Presidential memorandum providing policy guidance to the process that takes place.

The first requirement is a Presidential determination for certain types of operations. That then goes into a coordination process in terms of engaging on the development of the concept of operations, particularly with those agencies with the most equities involved. And then, ultimately, there is a deconfliction execution process in terms of, if there are conflicts between key equities or elements or there are concerns, for example, about the potential for unintended escalation, those issues are addressed.

So we do have a very thoughtful process but also a process designed to operate with the speed of relevance.

Ms. STEFANIK. Thank you.

General Nakasone, what exactly does our cyber posture look like when we defend forward with persistent engagement? Does this simply mean that we are positioned to conduct more offensive operations or positioned to conduct more collection activities?

And when you answer that, can you also touch upon the interagency aspects and how we work with our international partners?

General NAKASONE. Ranking Member Stefanik, if you think about persistent engagement, I would offer two different components that are very, very important, that are foundational to persistent engagement.

First of all is the idea of enabling. How do we enable our partners? That partner could be Department of Homeland Security, the Federal Bureau of Investigation. It could be another service. It could be another member of our interagency. It could be an allied partner.

A big portion of what we do in persistent engagement, as Assistant Secretary of Defense Rapuano said, is providing information or intelligence. If I might give you an example. During the security of the midterm elections, U.S. Cyber Command, working in partnership with the National Security Agency, provided indicators of compromise to the Federal Bureau of Investigation and the Department of Homeland Security. That is an example of enablement.

The other foundational concept of persistent engagement is to act. Just as the Secretary mentioned, act is everything from understanding what our adversaries are doing within their networks; providing early warning; ensuring that we understand the malware, the infrastructure, the other capabilities that an adversary might be accumulating to perhaps conduct an action against the United States.

But it is also the idea of sending teams forward. So we sent defensive teams forward in November to three different European countries. That is acting outside of our borders that impose cost against our adversaries.

Those are the two fundamental components of persistent engagement: enabling and acting.

Ms. STEFANIK. My final question is for you, General Nakasone. You have been given flexible acquisition authorities that, frankly, the command has yet to fully use or mature into. So my question is to figure out if this unique acquisition authority for your command is even still needed, certainly since over the years we have worked to give the services more flexible acquisition authorities.

Can you provide this committee with an update on why you think you need this unique acquisition authority and what the current state of implementation is? And then specifically, how would you define cyber-peculiar acquisitions, as it is called in the law?

General NAKASONE. If I might start with the question of a quick status update.

So this year, in fiscal year 2019, I believe the amount was $75 million for acquisition. And we have executed right now about $44 million of that. We would anticipate by the end of the fiscal year to execute about $60 million to $65 million. That is not $75 million, and I obviously accept the fact that we are short of that.

But what did we invest it in? And I think it is important that we outline this. One, we invested it in tools, significant tools for how we operate with our teams. Secondly, big data analysis. Thirdly, an opportunity for our developers to operate off-site at a facility to look at new networks, new capabilities, new infrastructures. It was done rapidly. It was done, I think, obviously, very effectively and certainly within the law.

We are not to the point yet where I am satisfied with regards to operating at the amount that has been authorized for us, but we will get there. And I think the important piece is, when I think of why it is so important to us, our adversaries are rapidly changing. And we see that every single day as we operate against them. The authorities that you have granted our command to be able to do this is a first start for us to be able to operate at their speed.

The last thing I would say is, we have 10 openings that, you know, are foundational for what we do for that acquisition authority. We have filled six of them. We will fill the final four by the end of the year, and I think this will be extremely helpful for us to be able to execute the moneys.

Thank you.

Ms. STEFANIK. And just to follow up, how do you define cyber-peculiar? Because that is how it is written.

General NAKASONE. So if I might take that for the record, Ranking Member, just to make sure that I have that fully accurate.

[The information referred to can be found in the Appendix on page 69.]

Ms. STEFANIK. Thank you. I yield back.

Mr. LANGEVIN. I thank the ranking member.

Mr. Brown is now recognized for 5 minutes.

Mr. BROWN. Thank you, Mr. Chairman.

In the most recently enacted Defense Authorization Act, we, the Congress, directed the Department to study the feasibility and advisability of the establishment of Reserve Component cyber civil support teams to be assigned to each State due to the lapse in appropriation associated with the 35-day recent government shutdown. The Department did request an extension to submitting that report to Congress.

Can you give us a status, and not just, you know, when you anticipate to submit that to Congress, but give us a little flavor on, you know, what kind of either conclusions, findings, or recommendations might be in that report?

Secretary RAPUANO. Certainly, Congressman.

The Department traditionally has not assigned unique specialty areas to the National Guard, like cyber, but we have been exploring whether and where—really where the National Guard can best support DOD missions, specifically things like defense critical infrastructure, infrastructure for which we are dependent on for power projection as well as weapons systems.

The defense industrial base is another area that is critical to us, and we are at risk, as I noted in my statement, of losing our asymmetric superiority to others who are stealing our technology.

So those are areas that we are very focused on and believe there is a potential role for the National Guard. And we actually have a cyber mission assurance team that is looking at the potential role there.

In response to your question about the 2019 NDAA 1653 tasker, we have a report that is in drafting process right now. We will get it to you all by the end of April. I really can't go into details on it, but it is really looking about the trade space and the return on investment from a total force perspective and how and where those roles would be most consistent with the other priorities of the Department.

Mr. BROWN. Thank you.

Question regarding the cyber workforce. Everyone is competing for a limited pool of highly skilled and highly talented, technically trained personnel. What thoughts do you have about the role of AI [artificial intelligence] in reducing the demand signal for a cyber workforce?

Secretary RAPUANO. Well, we are looking at all the tools available out there, you know, in terms of where do we need to buy either tools or capabilities, where do we need to hire people for that human potential component of it. It is well-recognized that hiring in the cyber field is very challenging just based on the very high demand signal, so we have a number of programs; CES [Cyber Excepted Service] is prime amongst them in terms of a new tool.

AI we are looking at very hard in terms of where we can leverage AI and other advanced capabilities, analytic capabilities to perform some of those activities.

I might turn it over to General Nakasone. I know his team looks at this very closely too.

General NAKASONE. So, Congressman, I think that AI and machine learning certainly has a place as we take a look at some of the activities that we do day in and day out within our force.

But I would offer, the people that make AI go, the people that ensure that our algorithms are right for machine learning, they are the folks that I am most focused on. Because I would call them—they are the 10X or the 20X folks that do their mission 10 times or 20 times better than anyone else. That is the competition that we are in today.

So I would just offer—I give great kudos to the services for recruiting a great base of folks, and that is both military and civilian. I think we do a good job of training them; it is getting better. The hard part and the one that we work at every single day is the retention part. That is the one that is most impactful for us.

Mr. BROWN. And you mentioned the CES, Cyber Excepted Service. Can you tell us a little bit about your experience with that? And is it working? Is it effective? Tell us about that.

General NAKASONE. Cyber Excepted Service, which just came on board roughly over the past year, we at U.S. Cyber Command were the first phase of that.

I can give you the metrics of now we are looking at a drop of 60 percent with regards to the hiring capabilities and the timeline to hire someone. So we have metrics that show us 111 days before CES. Now it is at about 44 days.

We have done over 21 different fairs. We have interviewed over 2,700 people. We have, you know, provided over 90 acceptances for job applications.

My perspective, early phase, I am a supporter of it, and I look forward to continuing to utilize it.

Mr. BROWN. Great. And I hope the University of Maryland at College Park is giving you a talent pool to work with.

I yield back, Mr. Chairman.

Mr. LANGEVIN. Thank you, Mr. Brown.

You know, on the topic of the workforce and training, we recently had testimony in reference to the Cyber Excepted Service as a whole, and it is underresourced at this time. And I think it is important for it to have full support and full resourcing.

Can you comment on that, Secretary?

Secretary RAPUANO. Yes, I can. I share your concern, Mr. Chairman. I have engaged with Dana Deasy, our CIO [Chief Information Officer], as well as the Under Secretary for Personnel and Readiness. This is a priority. The challenge with the Department is we have a lot of priorities, but everyone acknowledges there is no higher priority than this.

So we are looking at additional resources that we can get. We have already put essentially two more people onto it, because we had a couple of them taken for another priority group, and that has been addressed. But we need to supplement them going forward, and we believe we have a path to resources to do that in a relatively near term.

Mr. LANGEVIN. Okay. Thank you. I think that has to be a high priority, and certainly more support for the Cyber Excepted Service is going to have the support of this subcommittee and the committee as a whole.

Secretary RAPUANO. Thank you. It very much is.

Mr. LANGEVIN. Thank you.

Mr. Waltz is now recognized for 5 minutes.

Mr. WALTZ. Thank you, Mr. Chairman.

I am also interested, very interested, with my colleague Mr. Brown in the Guard and Reserve and the role that they can play, and I would be very interested in seeing that report. I have had the same conversations with General Kadavy, the head of the Army Guard. I mean, it seemed, you know, that the challenge is with recruiting, the challenge is with keeping up with the civilian sector and the pace of technology and who bridges those two worlds.

One of the questions I have asked him is, when you are recruiting your cyber force into the Guard and Reserve, are you taking,

you know, the civilian occupation into account? Are we recruiting people who are truck drivers during the day and then into the cyber force, or people who are actually in the IT sector in Silicon Valley, in that space, so that you can leverage those two and build upon those two?

And it is not clear to me. I would be interested if the report addresses that, if that is taken into account in the recruiting on the front end, particularly for the Guard so that you can build those going forward.

Do you have any additional comments on where that is going?

So, I mean, just to be candid, talking to the Guard about counting tanks, counting aircraft, parity in fielding, that is important. They need to be interoperable with the force. But where they can uniquely, you know, take this leading role—and leveraging those civilian sector skills, I think, is something we should take a hard look at.

Secretary RAPUANO. Yes. While I cannot speak to the details of how the National Guard right now is conducting their recruiting, I am familiar enough with their process to know that they do look at what are those specialty areas that the individual is being recruited for and what skills do they bring in addition to the basic elements of education.

Mr. WALTZ. Okay.

Secretary RAPUANO. So that is something. And then, again, it will be based on how the specialties develop and evolve and potentially expand.

Mr. WALTZ. Thank you. I am eager to see the report.

General Nakasone, can you just talk to me about plans or what is in place or what is coming down the pipe to just kind of share and collaborate cyber threats ostensibly at network speed, ostensibly at cloud scale with the top U.S. companies, with industry, I mean, so we can leverage the full resources of the U.S. Government and respond to our critical infrastructure?

Have we thought about—or is there—and forgive my ignorance, if there is a cybersecurity cooperative agreement with industry to detect, respond, mitigate cyber threats? I know DHS has theirs, but I keep hearing consistently, frankly, that it is not being utilized to its full extent and, frankly, not useful to industry. I didn't know the relationship with your command and industry.

General NAKASONE. Congressman, we have been working closely within the Department on an initiative called the Pathfinder program. The Pathfinder program—and this is an outgrowth from the Secretary of Defense and the Secretary of Homeland Security's memorandum of agreement to work together to look at joint ways that we can address the critical infrastructure sectors.

As you are aware, 17 different critical infrastructure sectors. We have started with the first one to look at, working very, very closely with the financial industry, working closely with the Department of Treasury, and the Department of Homeland Security, how do we share data, how do we share it rapidly. One of the things that we have done over the past several months is had four different means of sharing data.

But it is more than just sharing data, because we are not going to get out of this issue with just sharing. It is also our technical

experts talking to their technical experts, talking to the Department of Homeland Security.

It shows great promise. And as they move on from the financial industry, I think that energy and other industries right behind it will be the beneficiaries of this.

Mr. WALTZ. Along those lines, how are the delays in moving and DOD moving into the cloud architecture, how is that affecting your warfighting mission?

General NAKASONE. So it hasn't affected my warfighting mission. I would offer that our ability to share right now is at a level that certainly is able for me to accomplish what I need to be able to do.

I think, to your point, though, how do we increase our lethality in the future as a force, I think this is one of the areas that we are working towards. As the Department moves to its investment in the cloud experience, this is one of the things we are working very, very closely with the Department, NSA, and Cyber Command to ensure that we are well-postured for it.

Mr. WALTZ. Thank you. Then a final question, just in the interest of time, and maybe we will take this for the closed session, but I would be very interested.

Data is the new gold, new oil, whatever you want to call it, the coin of the realm. And back to your issue of collaborating, particularly with sensitive data, with an eye towards AI and 5G, because we can't really get to one without the other.

But I will yield my time and look forward to the closed session. Thank you.

Mr. LANGEVIN. Thank you, Mr. Waltz.

Mr. Kim is now recognized for 5 minutes.

Mr. KIM. Thank you, Chairman.

Thank you so much for coming and speaking with us today.

I actually just wanted to take a step back for a second here and just get some of your thoughts and advice here.

The issue of cyber threats is pervasive in my district. It is something that people worry about constantly, especially given the news and given all the talks about Russia and China. And I will tell you that these concerns are ones that I hear at town halls, and they come up in a lot of different meetings. I think there is a lot of confusion about what it is that we are doing and what the capabilities are on the other side.

So I would start this by urging the two of you to think about ways that we can invest in lifting up some of that veil, making sure that—I understand the difficulties and the sensitivities of the work you are doing. But as a new command, I think it is important for the American people to understand what it is that you are working towards, what it is that we are trying to do, and what it is that we are trying to defend against.

Because this is a different type of threat than the American people in my district, in Burlington County and Ocean County, to understand compared to conventional, traditional.

With that, I want you to just imagine yourself with me in my district at a town hall when I get these questions. I would like to hear from you what you would say in response to someone who is saying, are we getting outgunned by China and Russia? Where are our

capabilities and our personnel and our resources compared to these near-peers?

When we are talking and looking at our cyber budget, how does that stack up with how our competitors are spending and moving forward in this? How would you respond to someone in that way without having to get into the classified material?

Secretary RAPUANO. I will start, and then I can hand it over to General Nakasone.

I think when you look at the United States and you look at it, certainly, from a Department of Defense perspective, we operate around the world. We have to have systems that can communicate and engage around the world. So that presents a lot of surface for adversaries in terms of who are looking to target us.

We have an open system in terms of the internet. You may have heard that China has the Great Firewall of China. So we prize free communication of information. So an open internet is something that is consistent with the way that we have operated in the world from early on, and we would like to maintain that.

So it is not an apple-for-apple in terms of our vulnerabilities and adversary vulnerabilities is something that I would offer.

We have just increased, as you know from the budget, the budget for cyber, $9.6 billion and 10 percent increase over last year. So that is in recognition of the importance of this area, the evolution of the threat, which we see. We believe that we are developing the critical capabilities necessary to address the threat, but, as you know, it is a very complex and diverse threat. So walking through each of those areas can take a little bit of effort.

But I would just say that I think that, with the advent of this strategy and authorities from a national defense perspective, we have made tremendous progress. We are making the necessary investment to keep up with the threat and be able to prevail, if necessary, in all warfighting domains, including cyber.

General Nakasone.

General NAKASONE. Congressman, I think I would begin, if I had an opportunity to speak at your town hall, by saying the National Security Strategy identifies our threats very well. We talk about, you know, strategic and great power competition in the realm of both China and Russia. They are near-peer competitors. They have been able over the past 17 to 20 years to shrink the gap.

And then there are rogue nation-states, such as Iran and North Korea, that continue to conduct malfeasance in the domain.

But with that being said, there is still a gap between those actors and ourselves. And while I obviously hear a number of the different challenges that we have, I would also offer to your town hall that there are some strengths that are endemically part of the United States.

First of all, partnerships. We have a series of partnerships—partnerships with other allied countries, partnerships with academia, partnerships with industry—that I think are second to none.

Secondly, innovation. When we think about innovation, where do we think about? We think about Silicon Valley. We think about Austin. We think about Boston. We think about sectors within the United States. That is very, very important because we are in, obviously, a domain that is rapidly changing.

The other piece I would say is we are well-resourced. Thank you very much for, obviously, the resourcing that you have done for our efforts over this budget. I think that is tremendously powerful for us.

And the last thing is that we are also a country—and I would say, certainly within the Department of Defense, that we learn our lessons. And so we have learned our lessons. And I think that over the past several months we have been able to, obviously, apply those lessons in a manner that has addressed some of the actions of our adversaries.

Mr. KIM. Well, I look forward to working with all of you on how it is we can better explain this to the American people. Thank you.

I will yield back.

Mr. LANGEVIN. Thank you, Mr. Kim.

Before we go to Mr. Bacon, Mr. Secretary, you mentioned the $9.6 billion cyber budget request. And can you tell me what does the $9.6 cyber budget encompass? Is it IT as well as military cyber operations? And what is the totality of the budget for CMF and operations?

Secretary RAPUANO. So I will leave CMF to General Nakasone, but just in terms of the broad brush of the budget, it really starts with cybersecurity. So that is both hardware and software. We have to reduce the risk to DOD information systems.

Then it really gets to cyber operations. General Nakasone mentioned the tools, the training, all of the elements necessary for us to conduct cyber operations effectively.

And the third is the R&D [research and development] across all of these areas that we must continue to support so we can out-innovate our adversaries.

Mr. LANGEVIN. So give me, the committee, just kind of an understanding between those three categories, which—the various—the percentages, if you will, what is going to——

Secretary RAPUANO. Well, I mean, I think General Nakasone has more details on the splits.

General NAKASONE. Within that, Chairman, of the $9.6 billion, $532 million to the headquarters of U.S. Cyber Command. That is roughly 6 percent of the budget. And then $1.9 billion for a build an infrastructure. That is infrastructure across all of our four different locations that we have our teams. That will be—roughly 87 percent of that will go to the services, and the rest, about $200 million of that will stay within U.S. Cyber Command.

Mr. LANGEVIN. All right. That is helpful. Thank you.

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

Mr. BACON. Thank you, Mr. Chairman.

And appreciate both of you being here and appreciate your leadership on cyber.

A couple questions for General Nakasone.

I read that you were recommending the NSA and Cyber split sometime in 2020. Is that indeed your position?

General NAKASONE. Congressman, I had seen the article that was written. That is not accurate.

And last year about this time, during my confirmation testimony, I had indicated I would do a 90-day assessment. I did that assessment, provided it to the Secretary of Defense and the Chairman.

The assessment is classified, so we can talk about it later in closed session.

But, again, to your point, that was not accurate. And, again, the final decision, obviously, rests with——

Mr. BACON. Right.

General NAKASONE [continuing]. Not with me, so——

Mr. BACON. But maybe is it fair enough to say that you now—you would say your position is to keep them together then, the two commands, under one four-star?

General NAKASONE. So again, I think on this topic, Congressman, it is much more accurate for me to be able to talk in closed session——

Mr. BACON. Okay.

General NAKASONE [continuing]. Just to bring out the facts.

Mr. BACON. Just my view on it, without probing for your position, I just don't see how you can have them separate. I have worked in this community a little bit, with my 30 years in the Air Force, and our cyber teams are a good mix of intelligence and cyber folks that will probe or defend.

And it seems to me, from a cyber perspective, it is a symbiotic relationship with NSA. You can't do the two separate. I would be a little afraid, if you had two four-star generals, one in charge of the intelligence force and one in charge of the cyber portion, you could be pulling that team apart in two different directions.

And so I have always been a proponent that you need a unified leadership under one four-star and have the two three-stars guiding the two different ships.

But it just doesn't make sense to me from my experience in there. So I hope, at least my view or at least my recommendation would lean towards how we have it. I think we have it right.

How many cyber teams do we have?

General NAKASONE. We have 133, Congressman.

Mr. BACON. And is there a requirement for more, or is it about right?

General NAKASONE. So right now what we are doing is, through a series of both exercises and real world, looking at our force in total. My anticipation is after we have taken a thorough look at that we will make some recommendations. But right now 133 is what we have, and we are able to do our missions with them.

Mr. BACON. And all 133 are FOC, or fully operational?

General NAKASONE. Right. They are fully operational.

Mr. BACON. I have done exercises in the past in the Air Force, and we would do a full planning where you have your air targeting order or air tasking order and you build this whole plan, and then everybody leaves the room and cyber will come in and say, here are some other options.

Are we doing a better job now integrating cyber into the COCOM [combatant command] planning, where it is really baked in from the start, not an add-on after the fact?

General NAKASONE. While I hate to speak for my fellow COCOM commanders, I would say yes.

Mr. BACON. I hope so.

General NAKASONE. A couple things that have enabled us: first of all, the ability to put cyber operational integrated planning ele-

ments—those are planning elements that are well-versed in cyber—at each of the combatant commands. That has helped.

Secondly, that we have had a lot of operational experience in places like Afghanistan, Iraq, other places around the world where we have been able to do this. And even with the midterm elections, working with U.S. European Command, General Scaparrotti and myself, learned a tremendous amount of lessons in the way we need to do this.

Mr. BACON. Well, I am glad to hear that. I am glad we are evolving to where it is baked in from the beginning. Because I have been there where you do all your combat planning or this or that in space, and then everybody leaves, and it's like, okay, now what do I do with cyber? It should be integrated in from the beginning.

One last question. You know, there is a lot of convergence between cyber and electronic warfare [EW]. How much do you think cyber should be involved with electronic warfare? Is that a totally separate science, from your perspective?

General NAKASONE. So from my perspective, having worked this both as the Army service commander and now as the commander of U.S. Cyber Command, these are non-kinetic capabilities. And being able to synchronize non-kinetic capabilities, whether or not it is EW or cyber or information operations, bringing that closer together provides tremendous amount of capability for our commanders. And so that is why that close working relationship, I think, is very important.

Mr. BACON. So you would say the cyber role with EW would be more of a planning—to use an EW weapon versus a cyber weapon, but Cyber Command within itself would not have the EW weapons system. Do I have that right?

General NAKASONE. Yeah, so how we organize it, I think that is still to be determined. But in terms of the planning capability and synchronizing that, I definitely see that this is one where we would provide a synchronized look and say, hey, this is an opportunity for our combat commanders to leverage.

Mr. BACON. And from my background, the NSA has a great team working on the EW side, or at least on the ELINT [electronic intelligence], and we couldn't do it without you.

Sir, with that, I will yield back, Mr. Chairman.

General NAKASONE. So, Congressman, I would just offer that I agree with that.

Mr. BACON. Okay. Good. You get to take praise both ways.

General NAKASONE. It goes both ways.

Mr. LANGEVIN. On the EW issue, General, let me ask this. I know that after—I think it was Secretary Ash Carter that stood up the EW EXCOM [Electronic Warfare Executive Committee]. And what interaction do you all have with that body as they avail you with our EW capability? Do either one want to comment on that?

General NAKASONE. So I am not familiar with the EW EXCOM. That may have been renamed. There is a working body right now that discusses electronic warfare at the Vice Chairman level with the Deputy Secretary that normally we have, but I think it is the same purpose, and, again, the idea of how do we bring this together in a more compactful manner.

Mr. LANGEVIN. Okay. Thank you. Thank you.

And on Mr. Bacon's comment on the splitting of dual hats—see, bipartisanship isn't dead—I think you and I are definitely in sync on that one. So thanks for your comments on that.

Ms. Houlahan is recognized for 5 minutes.

Ms. HOULAHAN. Thank you, Chairman.

And thank you very much for your testimony today, gentlemen.

And, General, thank you for allowing us all to come as freshmen and tour your amazingly powerful facility.

My questions, I have two, a fairly unrelated one. The first one is to General Nakasone.

The President's budget does call for a pretty big investment in developing what he is terming a Space Force. Obviously, the space domain is very important for cyber operations.

And I was hoping—and this relates, I think, to Representative Bacon's comments and questioning—if you could talk a little bit about the relationship between CYBERCOM and the Air Force currently as it relates to the space domain and satellites in particular.

And help me assess whether or not the creation of a Space Force would either complicate CYBERCOM's work, help CYBERCOM's work, be redundant to CYBERCOM's work. How do you see that unfolding?

General NAKASONE. So we have worked very closely with the Air Force on the development of our cyber capabilities, to the first part of your question. In fact, roughly 39 of our 133 teams are from the U.S. Air Force. So we have a very strong working relationship with the Air Force and a very, very good joint force headquarters in Lackland Air Force Base in Texas that we have been reliant upon for many missions.

In terms of space, we at U.S. Cyber Command are in close partnership with not only the Air Force but U.S. Space Command, working with General Raymond, in terms of how do we ensure a couple of things: first of all, the defense of his networks. So working between U.S. Cyber Command, the National Security Agency, USSPACECOM, how do we ensure the criticality of his communications?

Secondly, what are the options for full-spectrum operations that we might be able to conduct from space that impact cyber? We are very, very excited about the possibility of the, you know, instantiation of U.S. Space Command. Being the newest kid on the block, I think that they would obviously provide, as the Department and the administration have indicated, a great capability.

We see the importance of space every single day, not only for our intelligence gathering, but also for looking at possible options as we look at adversaries for the future.

Ms. HOULAHAN. So do you have any reticence at all in terms of the interaction of what would be a new force? Or are you looking forward to that opportunity to integrate with something like that?

General NAKASONE. Really looking forward to integrating with it. I think they are a great capability. We see the importance of space, whether or not we are on the defensive side or the offensive side. And this is one of the areas that we think is going to create capability.

Ms. HOULAHAN. Thank you so much for the answer to that question.

My second one, fairly unrelated, has to do with memory chips and the fact that we only manufacture about 20 percent of the world's memory chips.

And I am wondering if you could comment, either one of you, on whether or not you feel as though we need to have organic capability of doing that domestically, whether for defense or civilian purposes, and how you think we as a Congress might be helpful in helping that, if you, in fact, believe that we should be more independent in that area.

Secretary RAPUANO. I will just give a high level on that.

We are very concerned about supply-chain security, particularly for sensitive systems or systems that may provide access to adversaries. So we are looking at the entire supply chain to understand where and what systems might be most vulnerable and how we can improve the surety associated with these chips and other elements.

Ms. HOULAHAN. Sir, do you have any other——

General NAKASONE. Yeah. So I think that the Secretary has characterized it well, in terms of, one the areas that we have to ensure—and this is the world in which we live, where they are being made today—is we have to have verification.

And the way that we do that verification, whether or not it is appropriately written into our contracts or whether or not it is being conducted, you know, periodically to ensure the veracity of these chips and their assurance that they will be, obviously, effective in their doing is really important to us.

Ms. HOULAHAN. Can you comment—I have another 49 seconds or so—on anything that we as a Congress can be doing to be helpful to begin the process of allowing us to be a little bit more independent in that area?

Secretary RAPUANO. Well, I would just say that we are working very closely with industry, as well as with the crosscutting teams associated with the assessment, the vulnerability assessment, to inform what the most effective approach is going to be to ensuring the surety of, first, national defense systems, but it expands more widely to that.

So there are locations in the United States where secure chips are built, but it is not at the scale that would cover all the needs, if there are concerns of a range of systems that could be entry points. So I don't know that we are at the point right now, but we may be coming to that point going forward.

Ms. HOULAHAN. Thank you very much, gentlemen.

I yield back.

Mr. LANGEVIN. The Chair recognizes Mrs. Trahan.

Mrs. TRAHAN. Thank you, Mr. Chairman.

So recognizing that scaling is—I mean, that that is a challenge no matter what industry you are in, in terms of the Cyber Mission Force, the 4,400 people, 133 teams, can you just give us a sense of how this team needs to grow in the next 2 to 3 years not just to meet the threat or catch up but, you know, to lead on cybersecurity?

General NAKASONE. Congresswoman, I think the piece I would offer is—so we have 133 teams on the Active side. The piece that we are focusing now is the growth on the Reserve and the National Guard side.

So the Army is going to build 21 additional teams. They are defensive teams. They will be built, all of the National Guard teams done by 2022 and all of the Army Reserve teams done by 2024. Twenty-one more teams is a tremendous amount of capacity that brings to us. I think it is the strategic depth that we as a Nation need.

To your point, then, one of the areas that we are starting to think through is, how do we effectively use that new capacity that is going to come on board in the next couple years? That is what we are starting to assess now, to the point of, are there critical infrastructure partnerships that we should start forming now with the teams that are coming on? Are there other mission sets that make a lot of sense for this new capacity?

So we are excited about that. The Army has moved out on that, and they are ahead of schedule in building those teams.

Mrs. TRAHAN. Great.

So you had mentioned, General Nakasone, that the biggest challenge is retention. Can you comment on the challenges or, you know, the root cause of retaining our talent?

General NAKASONE. I think that if you think about the talent that I was describing, the people that really are, you know, 10 or 20 times better than their peers, the first challenge is that they are looking for great missions that they can work. And that is one of the things that we think we offer, many times. I mean, it is hard to imagine places that you could go to do the things that we do in our mission force at the National Security Agency.

But that is only so far. And I think that the other piece of it is that we realize that there may be folks that want to come into the Army, whether or not it is as a military or civilian member, that only want to stay for 5 or 6 years. Not everyone is like yourself, in terms of staying 20 or 25 or 30, I guess now, years.

Mrs. TRAHAN. I just got here. I just got here.

General NAKASONE. Myself, I should say.

But that is a little bit of change in our thinking. And so we have to change, too, and say, if they are only going to be here 5 or 6 years, how do we effectively use them? Because those 5 or 6 years, they can be really, really impactful for the Nation.

Mrs. TRAHAN. Sure. And, you know, optimizing around that, once you know what your churn rate is, I think is important.

And so I guess my follow-on question—I came from business operations, so you will have to forgive me. But if retention is an issue and we know that folks are going to churn after 5 years, is the Guard enough to fill the pipeline, given, you know, the cost of training and onboarding and, you know, the current churn rate or even your projected churn rate? Is that enough?

And I guess where I am going—you can answer that question, but I will just give you my end question. Is there anything that Congress can be doing to address cybersecurity education, workforce development, those challenges with filling your pipeline beyond, you know, what we are thinking about today?

General NAKASONE. I think the last point that you made with regards to building a supply base is really important.

So when we look to recruit, we are looking for, you know, a population that is science, technology, engineering, mathematics en-

abled. And so, as we think about this as a Nation, we think about it, obviously, in the Department of Defense as, how do we engender that type of support within our young people?

I know at the National Security Agency we are working through a series of different camps that we sponsor from K–12. Last year, we touched 13,000 young people and 3,000 teachers, for a fairly small investment. That is the kind of, I guess, population that we are trying to develop so not only that the Department can recruit from but, obviously, our Nation can as well.

Mrs. TRAHAN. Thank you.

Did you have anything to comment, Mr. Secretary?

Secretary RAPUANO. I was just going to note that—and this is certainly embodied in Cyber Excepted Service, which we very much appreciate from Congress—but it is a soup-to-nuts in terms of, as General Nakasone mentioned, how and where do we best recruit? How do we develop an understanding amongst this talent pool about what we offer within the Department of Defense? And then it is, how do we ensure that they are getting professional development, horizontally and vertically?

And, ultimately, as all very capable people who are driven, they want to understand and they want to have offered to them ability to advance. So how are we ensuring that we are doing that so we are able to keep the best and the brightest? We know that a number of them will rotate out, but we want to build a certain percentage that are going to stay over the longer term.

Mrs. TRAHAN. Yep. I couldn't agree more. I mean, look, this is an enormous opportunity for our economy while also, you know, securing our country. So thinking through and co-producing programs beyond K–12 to get people the credentials that they need to serve, I think, is a noble partnership on our behalf.

Thank you. I yield back.

Mr. LANGEVIN. Thank you, Mrs. Trahan.

I just wanted to mention, General Nakasone, you had mentioned the collaboration and synchronization with the Space Force. But now, obviously, that also could mean that you are going to be competing with their people, talent, and dollars for resources as well. So another challenge you are going to have to deal with.

Ms. Slotkin is recognized for 5 minutes.

Ms. SLOTKIN. Thank you. I apologize for being late. We had another subcommittee hearing right in the middle.

My question actually goes back to something that Congressman Kim was talking about. I am a former Pentagon Assistant Secretary, and I cannot explain to people in public what we are doing to push back. And all of the people that come to my—you know, on cyberattacks. I am sorry. Let me finish my sentence.

People will ask me, from the small township officials to the average person who has had their credit card data taken by a corporation, "It feels like we are being smacked in the face every single day. You know, Elissa, you are from the Pentagon. What are we doing to actually fight back?"

And it is concerning to me that I can't tell them—I don't want to tell them anything classified, but I want to be able to say, we are not just sitting down and taking it, and here are some things I can say in an unclassified basis.

And then, secondly, just help me understand, you know, if you grow up in the defense world, you grew up with a model of deterrence, right? Conventionally, nuclear weapons. We need to maintain a strong deterrent. And I would love your help in understanding how we are doing that in the cyber realm. What are we doing to deter what feels like constant attacks on us in a way that, again, reassures me and others who are concerned that there is some price to pay for the constant barrage that we are receiving?

Secretary RAPUANO. I will take your second question and have General Nakasone take your first.

Deterrence is really about denying benefits and imposing consequences on adversaries in a way that is predictable enough for them that it dissuades or deters them from continuing them.

Historically, we have not done that in cyberspace. And that really is the paradigm shift that is really laid out in our strategy.

The third component of that is strategic messaging. How do we ensure that we, in concert with allies and partners, the rest of the international community that also abhors this kind of malevolent cyber activities, how do we galvanize this, in some sense or sometimes silent majority, to really focus on those actors who are creating the most problems?

So that is really what defending forward is all about. That is what persistent engagement at the combatant-command level is all about. It is the engagement, and it is about addressing the source of these threats.

General NAKASONE. Congresswoman, to your first point, I would turn back to, again, the recent elections, and what did we as a government do to ensure safe and secure elections. I think that, you know, the model of bringing together, whether or not it was the Department of Defense, the Federal Bureau of Investigation, Department of Justice, Department of Homeland Security, throughout the summer, very, very public appearances in terms of we are going to ensure a safe and secure election.

So we did work very, very closely with the Department of Homeland Security to protect our election infrastructure. We did work very, very closely with the Federal Bureau of Investigation to stop influence operations from other non-nation-states and nation-states from impacting our people. And we did, you know, obviously, conduct actions to ensure that any adversary that was attempting to interfere with our democratic processes, that we would address.

That is different than what we had done in the past, as the Secretary had mentioned. And I think that that is a very, very good model of where we need to move forward. Because we have to make sure that obviously our adversaries and certainly the American people understand that this is something that is obviously worth defending.

Ms. SLOTKIN. So just so I understand, you think that our response to attempts to meddle in our elections, that response provided some pain or put some pain on those who were trying to meddle, and therefore they won't do it again?

General NAKASONE. So I certainly can't assert they won't do it again. But they should certainly know, after what has occurred, that we are not going to stand back and be responsive in our approach, that we are going to defend, obviously, one of the most im-

portant things that we have in our Nation, which is our democratic processes.

Ms. SLOTKIN. Thank you. I yield back.

Mr. LANGEVIN. Thank you for the line of questioning.

And whether it is election operations or other things in the gray zone conflict, I think it is important that we meet them at every challenge. And I think we are going to see more and more of this conflict in the gray zone below the threshold of armed conflict. And I think we ignore those activities, I think, at our detriment.

And so, you know, we have to run the board and confront them everywhere. Anytime that our enemies or adversaries do something that goes unanswered, I think it just emboldens them further, in my opinion. So I think that is all part of the whole concept that we have now undertaken of defending forward. It is confronting them when and where we have to meet them.

Unless Mr. Cooper or Mr. Conaway have questions, we are going to now go to the closed session. So the committee stands in recess until the closed session begins.

Thank you.

[Whereupon, at 3:45 p.m., the subcommittee proceeded in closed session.]

A P P E N D I X

MARCH 13, 2019

PREPARED STATEMENTS SUBMITTED FOR THE RECORD

MARCH 13, 2019

Opening Statement
Chairman James R. Langevin
Intelligence and Emerging Threats and Capabilities Subcommittee
FY 2020 Budget Request for U.S. Cyber Command and Operations in Cyberspace

March 13, 2019

The subcommittee will come to order. Welcome to today's hearing on the fiscal year 2020 budget request for military operations in cyberspace.

Technology and the Internet have fundamentally changed how citizens, the nation, the military, our adversaries, and the world operate. We have more access to information and lower barriers to conduct commerce. We collectively benefit from the opportunities afforded by the technology we incorporate into our lives. However, the connections that we rely on also create vulnerabilities and new potential avenues for our adversaries to exploit at our nation's expense. "Cyber," as we understand it in government, will be always be something that creates risk to go along with its great promise.

The issues that stem from our increasing dependence on technology will never be purely military, or solely for the military to solve. Technology has increased the interconnectedness of our society, and the problems that have come with it will only be solved with interconnected, interdisciplinary approaches. The Department will have to work in new ways with stakeholders from agencies as varied as the Department of Commerce and Department of Education and with non-governmental stakeholders such as private industry and academia.

The Executive Branch will have to work diligently to address and solve the cyber challenges facing the nation. Yet this Administration has taken actions that call into question the seriousness with which it views this emerging domain. Most notably, the Administration eliminated the Senior Cyber Coordinator position at the National Security Council.

Relatedly, there are several documents pertaining to cyber that Congress has repeatedly requested from the Administration and has yet to receive. This includes recent guidance pertaining to operations in cyberspace. Such documents are imperative to creating a congressional framework for oversight. Withholding these critical documents from Congress impacts our ability to appropriately support the command and may have far reaching consequences in the National Defense Authorization Act.

At the cabinet level, the Department of Defense (DOD) and U.S. Cyber Command (CYBERCOM) have no shortage of challenges in front of them, issues that often develop and change as fast as the technological landscape changes. Today, we will hear about some of those challenges including personnel recruitment and retention, as well as efforts to protect critical infrastructure in tandem with domestically oriented departments and agencies.

The Cyber Mission Force achieved full operational capability (FOC) last year. This was a notable event, but it would be a mistake to assume that FOC is synonymous with readiness. We must begin to examine the differing standards by which the Services are training their teams, and whether CYBERCOM is adequately fulfilling its mandate to set training standards and ensure compliance.

Readiness is especially important in the context of the current strategic landscape, which has evolved significantly over the last year. In the fall, the DOD released a new cyber strategy that articulated the intent to "defend forward" and operate across the full spectrum of conflict through persistent engagement. DOD also completed the inaugural Cyber Posture Review. Under the auspices of new guidance from the Administration and the new DOD strategy, CYBERCOM played a crucial role in defending the 2018 elections from interference.

The military's actions in cyberspace were also enabled by multiple provisions in the Fiscal Year (FY) 2019 National Defense Authorization Act (NDAA). This includes a provision recognizing activities conducted in cyberspace as traditional military activities.

The FY19 NDAA also allowed the National Command Authority to take direct and proportional action in cyberspace against Russia, China, North Korea, and Iran upon determination of a cyberattack against the homeland or U.S. citizens. Congress and this Subcommittee will continue to support military operations and provide the legal authorities to enable CYBERCOM's success against adversaries in cyberspace. However, we will also remain judicious in our oversight responsibilities to ensure that the Department operates in a manner that enhances stability in cyberspace and that is consistent with both Congressional intent and American values.

I commend CYBERCOM for its efforts during the 2018 elections. However, as a nation, we can never rest on our laurels. We need to examine the strategic impacts that CYBERCOM operations, and other whole-of-government efforts, had on actors seeking to interfere in our elections. Much like the traditional battlefield, we must measure the impact of our operations to assess our warfighting effectiveness towards the larger objectives and ensure our strategic vision reflects the realities of engagement in cyberspace.

CYBERCOM's ability to execute its operations is closely tied to and enabled by its partnership with the National Security Agency (NSA). These organizations will always have a robust partnership given the dynamism of cyberspace and NSA's deep expertise and enabling role in military cyberspace operations.

At this time, there is still one individual that leads both of these organizations. This arrangement is quite unique within the national security establishment and the intelligence community. However, this arrangement allows for the CMF to mature, enables better synchronization of cyberspace operations, and permits proper consideration of the intelligence and military objectives in the domain.

Before any significant changes are implemented in the dual-hat arrangement, this Subcommittee expects a robust understanding of how and why it is necessary to split the leadership function of NSA Director and CYBERCOM Commander. **I believe it would be premature to split these organizations in the immediate future.**

CYBERCOM is a maturing organization, and I am proud of the work we have done on this subcommittee to support its maturation. I have often said that we will never again see warfare without a cyber component, so CYBERCOM's continued development will remain an urgent priority. But it is therefore important that we build for the long term with sustainable, scalable approaches to integrating cyber into DOD operations and into our whole-of-government approach to protecting our nation in cyberspace. This is no small task, especially given the newness of this domain. But working together, with full transparency, I am confident we can head off problems early and ensure we reap the benefits of a free, open, interoperable and secure Internet.

Before closing, I'd like to introduce our two witnesses.

Mr. Kenneth Rapuano serves as both the Assistant Secretary of Defense for Homeland Defense and Global Security and as the Principal Cyber Advisor to the Secretary of Defense. Prior to returning to government service, Mr. Rapuano worked for Federally Funded Research and Development Corporations, focusing on issues related to homeland security, counterterrorism, and countering weapons of mass destruction. Mr. Rapuano served as Deputy Homeland Security Advisor in the George W. Bush Administration. He served 21 years on active duty and the reserve as a Marine Corps infantry and intelligence officer. Mr. Rapuano, welcome back.

General Paul Nakasone serves in three capacities concurrently: Commander of U.S. Cyber Command, Director of the National Security Agency, and Chief of the Central Security Service. Before his current role, he commanded U.S. Army Cyber Command, and has served as a career intelligence officer through his 32 years in uniform. This is General Nakasone's first appearance before the Subcommittee since assuming command of CYBERCOM. General Nakasone, we are pleased you are here with us today.

Again, I want to thank our witnesses for appearing before us today. As a reminder, after this open session, we will move to room 2216 for a closed member-only session.

I'll now turn to Ranking Member Stefanik for her remarks.

STATEMENT OF

MR. KENNETH RAPUANO

ASSISTANT SECRETARY OF DEFENSE FOR HOMELAND DEFENSE AND GLOBAL SECURITY

AND PRINCIPAL CYBER ADVISOR

TESTIMONY BEFORE THE

HOUSE ARMED SERVICES COMMITTEE

SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

MARCH 13, 2019

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 significant progress the Department of Defense (DoD) has made over the last year in regard to cyber strategy and operations. I am testifying today in both my roles as Assistant Secretary of Defense for Homeland Defense and Global Security, and as Principal Cyber Advisor to the Secretary of Defense. I am responsible for advising the Secretary and the Deputy Secretary on cyberspace activities and the development and implementation of the Department's cyber strategy and policy with regard to cyberspace; leading our interagency coordination of our cyber efforts; and ensuring the integration of cyber capabilities across the Joint Force in support of the President and Secretary of Defense.

Threats and Strategic Objectives

Over the last year, the Department has made great strides in articulating its objectives for cyberspace, aligning the necessary resources to accomplish those objectives, and executing operations. To that end, the Administration has published a new, more proactive strategy for cyberspace, and is moving forward with implementation of that strategy using the first-ever Cyber Posture Review (CPR) and the elevation of USCYBERCOM. Our new approach has been enabled by the issuance of new Presidential guidance on cyberspace authorities, and legislation complementing the President's authority, that directs appropriate action in cyberspace against certain adversaries to disrupt, defeat, and deter active, systemic, and ongoing campaigns against the Government or people of the United States. Recent legislation also clarifies that certain cyberspace operations are traditional military activities. We leveraged all of these tools last year as we worked with our partners to ensure the security of the 2018 U.S. midterm elections.

We are continuing to gather and apply the lessons we have learned to defend the Nation from cyber threats.

This matter is urgent. The DoD Cyber Strategy makes clear that the ongoing campaigns of malicious cyber activity conducted by states like China and Russia are a strategic threat. Although our conventional military superiority is deterring these competitors from challenging the United States directly, our adversaries are increasingly resorting to malign activities in and through cyberspace to undermine U.S. security and prosperity. Their objective is to win without going to war. To achieve that goal, our competitors are conducting long-term, strategically focused campaigns in and through cyberspace that include stealing sensitive DoD information to undermine our military advantages, infiltrating our critical infrastructure so they can hold it at risk during a crisis or confrontation, and, in conjunction with activities in other domains, conducting influence operations targeting the American public.

Although the consequences of any single intrusion or action may be limited, in the aggregate these cyber campaigns are a strategic threat to the United States. Coordinated malicious cyber activity threatens our prosperity, our democratic institutions, and our national security, including by eroding our military advantage should a conflict occur.

For this reason, the DoD Cyber Strategy makes clear that the Department must embrace a proactive and assertive approach during day-to-day competition to deter, disrupt, and defeat these threats. The Department's networks and systems must be made so secure, resilient, and well-defended that we can be assured that the Joint Force will be able to execute its critical missions. During wartime, our forces must be able to operate even while under attack in cyberspace. The DoD

Cyber Strategy also directs U.S. cyber forces to target adversary weaknesses, offset adversary strengths, and enhance the effectiveness of the Joint Force. In order to succeed, our cyber forces must be well trained, properly equipped, and provided with the operational latitude and properly delegated authority to prepare the battlefield in advance of potential conflict.

Based on the guidance provided in the National Security Strategy, the National Defense Strategy, and the National Cyber Strategy, the DoD Cyber Strategy sets five clear defense objectives in cyberspace.

First, the Department must ensure that the Joint Force can achieve its mission in a highly contested cyber domain. The credibility of our military deterrence depends upon making clear that we are prepared to fight and win even against a capable modern adversary. Our systems must be cyber-hardened, resilient, and secure.

Second, cyber operations must enhance U.S. military advantages and strengthen the Joint Force. Cyber capabilities can increase the speed, reach, and precision of the Joint Force by creating novel, temporary, or reversible effects unmatched by traditional weapons. We are working to expand the scope and capacity of our cyber capabilities and to integrate them into Joint Force planning, exercises, and training.

Third, we must defend national critical infrastructure from significant foreign malicious cyber activity. This is a new area of emphasis for the Department and reflects the facts that competitors are targeting these assets, and that any large-scale disruption or degradation of national critical infrastructure, not just DoD infrastructure, would be a national security concern. We seek to preempt, defeat, or deter malicious cyber activity targeting national critical

infrastructure against a significant cyber incident by defending forward to stop threats before they reach their targets and will support the Department of Homeland Security in fulfilling its responsibility to coordinate the overall Federal effort to promote the security and resilience of the Nation's critical infrastructure.

The fourth objective of the strategy is to secure sensitive DoD information wherever it resides. Nearly every day, the news features a report of a major hacking incident, and states like China are relentlessly seeking to acquire both classified and unclassified data that they can use to gain economic, political, or military advantage over the United States. Innovation is the seed stock of our future security, and the Department is taking a much stronger approach to protecting that information and the systems on which it resides.

Fifth and finally, the strategy prioritizes expanding cyber cooperation with our interagency, industry, and international partners to advance our mutual interests, including the protection of infrastructure upon which we rely.

The DoD Cyber Strategy also articulates a proactive and assertive approach for achieving these goals. It states that DoD cyberspace forces must be defending forward: disrupting threats at the source before they reach U.S. networks. This is an essential element of a defense-in-depth approach that protects the Nation from cyber threats, despite imperfect cybersecurity. The Department must routinely operate in non-U.S. networks in order to observe threats as they are forming and have the ability to disrupt them. This is also critical to increasing military readiness. We cannot be fully prepared to take effective action in a potential conflict unless we have already developed the tools, accesses, and experience via our actions day-to-day.

The necessity of this shift to a proactive approach was made clear in our efforts to secure the midterm elections by defending forward. USCYBERCOM and the National Security Agency (NSA) established an interagency group to fuse information, operational expertise, and resources to contribute to interagency efforts to protect the elections from foreign interference and influence. We expanded our cooperation with the Department of Homeland Security (DHS) and took steps to ensure that, if our assistance was requested, Defense Department personnel could provide support to DHS in a timely and effective manner. We also partnered with several European countries.

In addition to our immediate work to secure the 2018 U.S. midterm elections, the Department has taken further steps to translate our strategy into a plan of action. The first step was the completion of the first-ever Cyber Posture Review (CPR). The CPR involved a comprehensive analysis including data collection, war gaming, modeling, and extensive expert inputs from within and outside the Department. The CPR examined the resources, capabilities, manpower, and organization needed to implement the strategy, and identified existing gaps between where we are today and where we need to go to achieve our strategic objectives.

The CPR gap assessment drove the development of actionable lines of effort that are guiding the work of our cross-functional Principal Cyber Advisor Team. This team is growing to ensure it has the capacity to oversee the full range of actions needed to strengthen our cyber posture. This is a high priority for the Department. Mr. David Norquist, currently performing the duties of the Deputy Secretary of Defense, is personally overseeing bi-weekly meetings to ensure that we are holding leaders accountable for change. Although much work remains to

be done, we have made enormous progress in the past year and continue to build momentum.

Authorities and Policies

I would now like to provide some examples of specific changes we have been making to the way we operate in cyberspace. We have worked diligently, and in partnership with Congress, to ensure that the authorities and policies currently in place governing cyberspace operations enable our strategic approach to competing and prevailing in this domain. Several changes during 2018 have been particularly impactful. In the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (NDAA for FY 2019), the affirmation of the President's authority to counter active, systemic, and ongoing campaigns in cyberspace by our adversaries against the Government and the people of the United States (Section 1642) as well as the clarification that certain cyber operations and activities are traditional military activities (Section 1632) have been force multipliers. Thank you very much for your support. On the policy front, the President had approved updated policy on U.S. cyber operations.

These changes have advanced and modernized how the Department operates in cyberspace and enabled the missions described in the DoD Cyber Strategy. We have also worked hard to align our internal policies with our cyberspace objectives. In particular, we focused on how our cyber forces operate in the homeland. Last May, we reissued our memorandum on Defense Support to Cyber Incident Response (DSCIR). The DSCIR memorandum provides guidance to the Department on how DoD cyber capabilities can be employed in response to a request for support to augment civil authorities. We faced a real-world example of

this as we prepared for the 2018 U.S. midterm elections, when we worked to ensure that the appropriate procedures were in place in case we received a DSCIR request from DHS. Fortunately, DHS never had to make such a request. However, the lessons we learned during that period will be useful moving forward. My goal in the long-term is to normalize cyber support to civil authorities by fully integrating it into the Department's existing and long-standing policies and procedures for Defense Support to Civil Authorities (DSCA) across all domains.

Partnerships

In addition to updating our DSCA policies, we are continuing to refine Department guidance concerning the day-to-day partnerships between military cyber forces and State and local governments. We are currently reissuing a memorandum that provides policy guidance for all DoD personnel on the provision of cyber support and services to non-DoD organizations and activities when those services are provided incidental to military training. The memorandum also details how National Guard personnel can use certain DoD information, networks, software, and hardware for State cyberspace activities.

The DoD Cyber Strategy emphasizes the importance of working with partners to maximize our successes in this domain. To that end, we have devoted focused attention during the last year to building and enhancing our relationships with other U.S. Government departments and agencies, industry, and our allies and partners. Last year, Secretary Mattis and Secretary Nielsen signed a joint memorandum of understanding (MOU) detailing how our two departments can cooperate in order to secure and defend the homeland from cyber threats. The MOU reiterates DHS's primary role as the U.S. Government lead for protection of national critical infrastructure, and emphasizes DoD's unique mission of defending

forward. These roles are mutually reinforcing; DHS's efforts at home enable DoD to project power both in cyberspace and in the physical domains, even as our efforts outside the homeland help to secure U.S. infrastructure.

As part of the efforts to implement this MOU fully, DoD and DHS senior leaders, including myself, recently signed a charter creating a Cyber Protection and Defense Steering Group. This steering group provides us with visibility into existing areas of DoD-DHS cyber cooperation, enabling us to synchronize our efforts more effectively. By bringing leaders from both departments into the same working group, we are able to collaborate better, and to ensure that our two departments are able to address cyber threats synergistically, rather than work at cross-purposes.

One area of major concern for us is the theft of sensitive DoD information from our DIB partners. The scale and scope of this theft from the DIB are putting our future military technological advantage at risk. DoD continues to work with industry, in coordination with DHS, to implement cybersecurity protections and to share cyber threat information with DIB partners. We are taking a variety of actions to secure our information more effectively, including the formation of an interagency working group, led by the Federal Bureau of Investigation (FBI), to ensure that the U.S. Government is operating in a unified manner and maximizing the unique capabilities and authorities of every participating department or agency.

Our efforts to enhance our partnerships are worldwide. The Department will work to strengthen the capacity of our international allies and partners to increase DoD's ability to leverage its partners' unique skills, resources, capabilities, and perspectives to enhance our mutual cybersecurity posture. We are dependent on other countries for many services that enable the U.S. military to function,

including our communications networks and the physical infrastructure that enable power projection. To help ensure that our allies and partners are as robust as we need them to be, we are working to enhance the Department's cyberspace partner capacity-building capabilities by promoting standards for cybersecurity practices, building international situational awareness and information-sharing mechanisms, and broadening DoD's coalition of close cyberspace partners.

We are also pressing our global partners to hold states that are acting irresponsibly in cyberspace accountable for their actions. At our bilateral and multilateral engagements, we advocate responsible state behavior in cyberspace during peacetime. We know that some of our competitors act irresponsibly in pursuit of their national interests. Consequently, we are working with other countries to enhance our combined ability to impose consequences in response to malicious and destabilizing behavior in cyberspace.

A third international issue that we have prioritized is advocating for secure telecommunications networks and supply chains. We are engaging with our allies and partners to encourage them to maintain secure and reliable networks and information technology supply chains, including as it applies to their 5G telecommunications infrastructure. This is especially critical for countries with whom we have strong defense relationships. Our military relies on secure and resilient telecommunications infrastructure to operate alongside foreign forces. These risks can persist even outside the borders of those countries as a result of equipment exports and service contracts. We routinely encourage allies and partners to consider the risks they are building into their networks and supply chains when awarding contracts, and we urge them to exercise vigilance to ensure their security is guaranteed.

Cybersecurity and Personnel Reform

The CPR made it clear that the Department will not be able to achieve its objectives in cyberspace by continuing to conduct "business as usual." When it came to cybersecurity, it was clear that we needed to prioritize more effectively how we were spending money, allocating resources, and recruiting and retaining the most qualified people.

Our PCA team worked with the DoD Chief Information Officer (CIO) to identify the "Top Ten" areas where we faced the greatest risk. We prioritized these Top Ten areas during our most recent budget cycle and are currently working through pilot programs to implement solutions for several of them.

One focus area from the Top Ten is enhancing the recruitment and retention of the cyber workforce. In 2015 (FY 2016), Congress gave the Department the authority to create the new DoD-Cyber Excepted Service (CES) personnel system. The CES allows for the more agile recruitment of candidates with cyber expertise by streamlining HR procedures and delivering more competitive market-based salary packages. To date, 403 civilian positions have been converted from the competitive service to the CES positions across U.S. Cyber Command, Joint Force Headquarters DoD Information Networks, and the DCIO Cybersecurity Directorate. Currently, we are in the process of completing phase II CES implementation across the Service Cyber Components and the Defense Information Systems Agency (DISA), which spans approximately 15,000 positions. The CES is a key initiative within the "First Four," a subset of the Top Ten. We are focused on driving the pace of the CES to ensure we recruit, retain, develop, and train the best cyber professionals to execute the Department's mission

successfully. The Department continues to address the new hiring authorities (pay enhancements, direct hiring authority, and targeted local market supplements) to address the implementation requirements outlined in the Cyber Strategy. To that end, we are working closely with the Office of the Under Secretary of Defense for Intelligence (USD(I)) to improve the security clearance process to ensure that when we attract the best talent we are also able to onboard those individuals in a timely manner. We are also energizing the uniformed services to use their recently-granted authorities to recruit and retain the best and brightest military officers with deep cyber expertise..

Another new Department initiative is the Protecting Critical Technology Task Force (PCTTF), established last year at the direction of Secretary Mattis to improve protection of DoD technology. As Major General Murphy briefed this subcommittee last week, the PCTTF is integrating and accelerating the disparate DoD technology protection activities occurring across the Department and developing new innovative solutions for currently unaddressed problems. Cyber is, of course, a central concern of the PCTTF, and the Task Force is evaluating a range of measures to increase the cybersecurity and resilience of our DIB private sector partners.

Conclusion

In summary, our new strategy has provided us with a roadmap for achieving our objectives in cyberspace. We are now focusing on implementing that strategy and ensuring that the various elements necessary for success are properly aligned. We have made great strides in the last year. We have expanded authorities that enable our mission to defend forward. We are working to ensure that our internal policies support our vision for the Department's role in the homeland. And, we are

doubling down on collaborating with other departments and agencies, industry, and our international partners and allies. Notwithstanding the significant progress made, we understand there is still more work to be done. I look forward to working with you and our critical stakeholders, both within and outside the U.S. Government, to ensure that the U.S. military will continue to compete, deter, and win in cyberspace.

Kenneth P. Rapuano
Assistant Secretary of Defense for Homeland Defense and Global Security

Mr. Kenneth P. Rapuano is the Assistant Secretary of Defense for Homeland Defense and Global Security. Previously Mr. Rapuano was a Senior Vice President at the ANSER Corporation, and the Director of the Studies and Analysis Group which provided multi-disciplinary studies and operational analysis for a broad array of government clients in the national security, homeland security areas. Up until November of 2016, Mr. Rapuano Directed the Homeland Security Studies and Analysis Institute (HSSAI), a Federally Funded Research and Development Corporation (FFRDC) operated by ANSER, a mission oriented not-for-profit organization.

Prior to joining ANSER Mr. Rapuano was the Director of Advanced Systems at the MITRE Corporation. He was responsible for guiding crosscutting strategic national and homeland security mission initiatives, with particular focus on counterterrorism, intelligence, aviation security, crisis management/decision support, national preparedness, and CWMD.

Previously, Mr. Rapuano served at the White House as Deputy Homeland Security Advisor to President George W. Bush from 2004-2006. He was responsible for managing the development and implementation of homeland security policies among departments and agencies, chaired the Homeland Security Council Deputies Committee, and co-chaired the White House Counterterrorism Security Group. He left the White House in 2006 to volunteer for deployment as a Marine Corps officer to Afghanistan with a Joint Special Operations Task Force, establishing and directing a targeting fusion center tracking high-value terrorists and insurgents. He also served in Iraq in 2003, commanding the Joint Interrogations and Debriefing Center of the Iraq Survey Group established to conduct the mission of surveying and exploiting possible weapons of mass destruction activities across Iraq.

In 2003, Mr. Rapuano was appointed Deputy Under Secretary for Counter Terrorism at the Department of Energy, responsible for nuclear counter terrorism, homeland security, emergency response, and all related special access programs for DOE and the National Nuclear Security Administration. Previous to that, he was the National Security Advisor to the Secretary of Energy. Mr. Rapuano has also served as Special Assistant to the Assistant Secretary of Defense, International Security Policy. He served 21 years on active duty and in the reserves as a Marine Corps infantry officer and intelligence officer.

Mr. Rapuano has also served as a Distinguished Research Fellow at the National Defense University's Center for the Study of WMD, as a member of the Defense Science Board Task Force on the Role of DoD in Homeland Defense, the Pacific Northwest National Lab's National Security Advisory Committee, the FBI's Weapons of Mass Destruction Directorate Advisory Group, the DHS Quadrennial Homeland Security Review Advisory Committee, and the DHS Science and Technology Advisory Committee.

Mr. Rapuano received a bachelor's degree in Political Science from Middlebury College, a master's degree in National Security Studies from Georgetown University, and has attended the Marine Corps Air-Ground Task Force Intelligence Officer Course at the Navy and Marine Corps Intelligence School.

STATEMENT OF

GENERAL PAUL M. NAKASONE

COMMANDER

UNITED STATES CYBER COMMAND

BEFORE THE

HOUSE COMMITTEE ON ARMED SERVICES

SUBCOMMITTEE ON INTELLIGENCE, EMERGING THREATS, AND CAPABILITIES

13 MARCH 2019

Chairman Langevin, Ranking Member Stefanik, and distinguished members of the Committee, thank you for inviting me to represent the men and women of US Cyber Command (USCYBERCOM). I am honored to lead them, and grateful for the opportunity to highlight their accomplishments. Our Command has seen a year of change and progress, featuring the elevation of USCYBERCOM to a unified combatant command with an expanded mission and additional authorities and responsibilities, and the completion of the build of 133 teams in our Cyber Mission Force (CMF). We have transitioned from building the force to ensuring its mission readiness, and in 2018 we enhanced that by opening our new, state-of-the-art Integrated Cyber Center. Enabled by changes in law and policy, we have produced defensive and offensive operational successes. My testimony will summarize threats and opportunities in our strategic environment, explain how we prepared ourselves to meet them and what we did, and explain our priorities for the future of a USCYBERCOM that enables our partners and acts in cyberspace to defend the nation.

USCYBERCOM's task 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. Our responsibilities include providing mission assurance for the Department of Defense by directing the operation and defense of the Department's information systems (what we call the DoDIN); deterring or defeating strategic threats to national interests and infrastructure; and helping the combatant commanders achieve their missions in and through cyberspace. This fiscal year we are executing a budget totaling roughly $610 million. Our full-time personnel amount to 1,520 military and civilians, plus contractors. This January we had 4,406 Service members and civilians in our Cyber Mission Force, building to a total of 6,187 people. We also have both Guard and Reserve personnel on active duty serving in our forces.

USCYBERCOM comprises a headquarters organization that directs operations through its components. These include the Cyber National Mission Force (CNMF); the Joint Force Headquarters-DoD Information Network (JFHQ-DoDIN); and Joint Task Force Ares; plus our Joint Force headquarters elements, each of which is paired with one of the Services' cyber

components. Those Service components are Army Cyber Command, Marine Forces Cyberspace Command, Fleet Cyber Command/Tenth Fleet, Air Force Cyber/24th Air Force, and U.S. Coast Guard Cyber.

Our efforts and our continued success depend upon the support of the Congress and of this Committee. Thank you in advance for the assistance you are providing us in 2019 as we pursue opportunities in five areas: (1) Supporting strategic competition; (2) Establishing a warfighting ethos across the Command; (3) Improving the readiness of our cyber forces; (4) Enhancing partnerships across government, allies, and the private sector; and (5) Deploying improved operating infrastructure.

The Strategic Environment

Cyberspace is a contested environment where we are in constant contact with adversaries. The nation faces threats from a variety of malicious cyber actors, including non-state and criminal organizations, states, and their proxies. We see near-peer competitors conducting sustained campaigns below the level of armed conflict to erode American strength and gain strategic advantage. USCYBERCOM ensures two critical capabilities against these threats: it enables partners in whole-of-nation efforts to build resilience, close vulnerabilities, and defend critical infrastructure; and it acts against adversaries who can operate across the full spectrum of cyberspace operations and who possess the capacity and the will to sustain cyber campaigns against the United States and its allies.

Renewed Strategic Competition. The *National Security Strategy* (2017) emphasized the emergence of great-power competition and noted its spread into cyberspace. In implementing that guidance, the Department issued the *DoD Cyber Strategy*, which described the environment we face:

> *We are engaged in a long-term strategic competition with China and Russia. These States have expanded that competition to include persistent campaigns in and through cyberspace that pose long term strategic risk to the Nation as well as to our*

> *allies and partners. China is eroding U.S. military overmatch and the Nation's economic vitality by persistently exfiltrating sensitive information from U.S. public and private sector institutions. Russia has used cyber-enabled information operations to influence our population and challenge our democratic processes. Other actors, such as North Korea and Iran, have similarly employed malicious cyber activities to harm U.S. citizens and threaten U.S. interests. Globally, the scope and pace of malicious cyber activity continue to rise. The United States' growing dependence on the cyberspace domain for nearly every essential civilian and military function makes this an urgent and unacceptable risk to the Nation* [emphasis in original].

I assess we are seeing what we term *corrosive threats*, in which malicious cyber actors weaponize personal information, steal intellectual property, and mount influence campaigns. Such measures have had and will have strategic effects on our nation and allies.

Changes in Strategic Guidance and Authorities. USCYBERCOM has recently improved the scope, speed, and effectiveness of its operations with the help of legal and policy changes. I want to thank Congress for its support of DoD's cyberspace operations as reflected in provisions of the FY19 National Defense Authorization Act (NDAA) that enhanced our agility to execute missions consistent with law. We also received updated policy guidance that, in conjunction with the NDAA provisions, significantly streamlined the interagency process for approval of cyber operations and thus facilitated recent activities.

The *DoD Cyber Strategy* asserts that the Department has a significant role in defending the nation. To be effective in doing so, the *Strategy* mandates that DoD components "defend forward, shape the day-to-day competition, and prepare for war," enabling the Department "to compete, deter, and win in the cyberspace domain." We must be active because inaction on our part cedes advantage to capable adversaries willing to flout international law and impose their own norms of cyber conduct. In keeping with guidance to defend forward, the Department is aiming to take the initiative against those who act against us. The *DoD Cyber Strategy* states that the Department must be prepared to defend assertively the functioning of even non-DoD

critical infrastructure systems -- whether at home or abroad -- that are essential to project, support, and sustain Departmental forces and operations worldwide. In practice, this means confronting our adversaries from where they launch cyber attacks and developing robust capabilities that are responsive to Defense Support to Civil Authorities (DSCA) activities.

A New Operating Construct. We are implementing the *DoD Cyber Strategy* through the strategic approach of persistent engagement, which includes partnering with other US Government elements to build resilience into US networks and systems, defending against malicious cyberspace activities as far forward as possible, and contesting adversary attempts to disrupt our nation's key government and military functions.

Our operators, analysts, developers, leaders, and support personnel, enabled by new and modified policy guidance, are operating more effectively in coordination and partnership with other agencies, partners, and allies. Last fall we supported US European Command (USEUCOM), US Northern Command (USNORTHCOM), the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and others to defend the integrity of America's 2018 mid-term elections. Working together under my command, USCYBERCOM and the National Security Agency (NSA) undertook an initiative known as the Russia Small Group to protect the elections from foreign interference and influence. By enabling our fellow combatant commands and other partners, USCYBERCOM assisted the collective intelligence and defense effort that demonstrated persistent engagement in practice. The tight links between USCYBERCOM and NSA created a mutually beneficial, intelligence-operations cycle that let us rapidly find and follow leads, discover new information, and create opportunities to act in conjunction with partners. Additionally, our co-location in the new Integrated Cyber Center optimized our collaboration for efforts of this nature. We created a persistent presence in cyberspace to monitor adversary actions and crafted tools and tactics to frustrate their efforts. We shared information through DHS with state election officials to help identify vulnerabilities and improve threat warning. We also enabled Department of the Treasury and FBI actions in conjunction with the private sector, for instance, by posting foreign malware for the first time to VirusTotal, a private site for crowdsourcing analysis of cyber threats. Finally, working with

USEUCOM, and with the consent of several European countries, we sent defensive teams forward to conduct operations in support of our mission to help secure the mid-term elections.

Opportunities and Challenges for US Cyber Command

I note the progress we have made during the past year and see opportunities ahead, with corresponding challenges as well. We have achieved much under the *National Defense Strategy*'s commitment to prioritize investments in cyber defense, resilience, and the continued integration of cyber capabilities into the full spectrum of military operations. We must use our recent successes to inform future activities, ensuring that accomplishments are not isolated events but parts of a larger trend of improved operational proficiency.

Supporting Strategic Competition. Cyberspace is a domain in which opponents can attain strategic results without using armed force. Our adversaries in cyberspace are acting and taking risks in seeking to gain advantage without escalating to armed conflict; they are conducting campaigns to gain cumulative advantage (these include theft of intellectual property and personal information, malign influence and election interference, efforts to circumvent sanctions, and probes and positioning to threaten critical infrastructure).

We see evidence of such cyber campaigns in many places, such as the foreign efforts to find vulnerabilities in the Department of Defense's Information Network. JFHQ-DoDIN used its authorities to direct global Department of Defense network operations, security, and defense. By operationalizing the network sensors, they assessed effectiveness and risk through focused data analysis. This in turn helped improve the fidelity of our sensors and analytics, showing us the risks and the requirements for mitigation. The data JFHQ-DoDIN collected in this effort proved that state-sponsored adversaries in cyberspace are conducting rapidly evolving campaigns to hamper the routine functions of the DoDIN and to find seams in its defenses. DoDIN protections are robust, but we must continue to innovate in our data collection and analysis to build resilience and counter the dynamic nature of adversary threats.

In the face of strategic competition in cyberspace, USCYBERCOM brings unique advantages in planning, deconflicting, executing, and assessing cyberspace operations at-scale.

Our efforts in defense of the 2018 elections taught us the value of persistent engagement to contest adversary campaigns, the power of enabling partners, and the ability to impose costs. The *DoD Cyber Strategy* notes we cannot afford inaction – our values, economy, and society are exposed and we must assertively respond at all levels. USCYBERCOM is working with the combatant commands, DHS, FBI, across the Intelligence Community, and in conjunction with private sector and foreign partners to improve understanding and act to contest and frustrate adversary cyber activities. Through persistent engagement we identify and close vulnerabilities in DoD networks, act to contest threats, and enable partners in building resilience and in the defense of the nation. These steps complement and support national efforts to prepare for conflict, to deter adversaries, and to establish cyber norms while we simultaneously support combatant commanders in contingency operations.

Supporting the Combatant Commands and Establishing a Warfighting Ethos. A competitive mindset is needed to prevail in a deeply competitive domain. Such a mindset also helps us prepare to fight and win the nation's wars. To support combatant commanders and their missions we are engaged in a growing variety and number of activities, from planning to intelligence missions to operations in and through cyberspace. We bring to the combatant commands a wartime ethos reinforced by daily contact with cyber adversaries.

Our cyberspace operations support kinetic and information operations against terrorists across several regions. We are employing cyber capabilities to improve force protection, bolster intelligence, understand and shape the information environment, and disrupt the operations, command and control, and propaganda of several insurgent and terrorist groups in support of US Central Command (USCENTCOM), US Africa Command (USAFRICOM), and US Special Operations Command (USSOCOM). Cyberspace operations in places like Iraq, Syria, Yemen, and Afghanistan today integrate and synchronize cyberspace and information operations with kinetic missions, with each enabling the other for offensive, force protection, and intelligence purposes. Our persistent engagement with this adversary for the past several years shows the continuing value of our command in being able to operate across all of these regions against the key enablers for these groups (e.g., media, finance, and foreign fighters). In this context, we have expanded the remit of our Joint Task Force Ares, and shifted its chain of command from

Army Cyber Command to Marine Corps Forces Cyberspace Command while maintaining its principal task of operating against the Islamic State. JTF-Ares has also embarked on a special mission partnership with NSA to act together as a hub for whole-of-government cyber planning in the ongoing counter-terror fight (thus further demonstrating the value of the USCYBERCOM and NSA partnership).

The maturation of the Cyber Mission Force has increased the number and proficiency of the cyber units working to protect the networks and weapons systems that combatant commands rely on to perform their missions. Each combatant commander controls organic Cyber Protection Teams (CPTs) that work in conjunction with local and regional cyberspace security providers and administrators. The expertise and databases at USCYBERCOM tie these teams together and greatly increase their collective power. US Indo-Pacific Command (USINDOPACOM) and US Forces Korea have hosted frequent visits of our teams and experts to assist in surveying and hardening their military critical infrastructure in advance of any contingencies in East Asia and the Western Pacific. US Transportation Command (USTRANSCOM) has benefitted from similar assistance in support of its global operations and commitments. In Europe we assisted USEUCOM, NATO allies, and other partners to secure their networks from foreign interference. Finally, our efforts helped US Southern Command (USSOUTHCOM) and USNORTHCOM in election security, border security, and disaster recovery efforts.

Evolving national and departmental guidance creates opportunity for timely cyber operations in support of the combatant commands and in our role in the Chairman of the Joint Chiefs' global integration efforts. This includes both planning cyberspace operations support to trans-regional campaigns and prioritizing the allocation of high-demand, low-density cyber assets across the commands and in all phases of conflict. The Department and the Chairman have clarified the command and control of cyberspace forces, and in accord with this guidance we are building "cyberspace operations integrated planning elements" (CO-IPEs) at each combatant command.

The new, Service-like authorities and responsibilities that USCYBERCOM gained as result of elevation are similar to those authorized for USSOCOM on behalf of the nation's Special Operations Forces. USCYBERCOM is the Department's Joint Force Provider and Joint Cyberspace Trainer for cyberspace forces. In these roles, we develop strategy, doctrine, and tactics; prepare and submit program recommendations and budget proposals; exercise authority, direction, and control over the expenditure of funds; validate requirements; establish priorities for requirements for cyberspace capabilities, forces, training, and operations; and ensure the inter-operability of equipment and forces. We are working with the Department to build approaches across the force and leverage these new responsibilities to better measure, access, and improve the quality and readiness of the entire cyber force.

Improving Readiness. The rapidly evolving cyber domain makes achieving and maintaining force readiness a challenge. Similar to other Department forces, the readiness of our cyber forces can be understood as a two-part equation. First, we are evaluating the readiness of the teams that the Services (under their man, train, and equip missions) present to the Command. Second, we are studying the readiness of those teams to perform the missions they have been assigned by USCYBERCOM, something we refer to as "mission posture."

The Cyber Mission Force completed its build in May 2018, and we started formally reporting team readiness in the Defense Readiness Reporting System (DRRS) shortly afterward. USCYBERCOM is working with the Services to ensure that they present cyber forces that meet a common, joint standard so that the Soldiers, Sailors, Airmen, and Marines coming to the Command have proficiency with foundational cyberspace tools, techniques, and procedures. As part of that plan, the Services recently assumed the training mission for personnel in the CMF that USCYBERCOM (together with NSA) had overseen during the build. We are refining training curricula and standards, as well as simplifying and updating course requirements so we can ensure the right number complete their training with the appropriate skills.

The second part of the equation—mission posture—is not as accurately reflected by traditional metrics. Thus we are developing metrics that go beyond those traditionally used in order to capture cyber-unique requirements such as authorities, accesses, capabilities, and

intelligence. Such dependencies are not always measured in conventional DoD readiness reporting, yet they play a critical role in generating successful cyber operational outcomes. Our goal is to ensure operational proficiency in our CMF teams by taking an appropriately holistic view of readiness and applying resources to shortfalls. Working with the Services and the Department, we will develop and institutionalize the changes necessary for us to accurately measure and maintain team and mission readiness across the CMF.

To help sustain an advanced cyber force, all of the Services are applying hiring and retention incentives (especially for high-demand, low-density skill sets) as well as utilizing the flexibility in managing talent that Congress recently granted us by authorizing the new Cyber Excepted Service. The retention of top talent—particularly in some critical, high-skill jobs—is a significant concern because it will be crucial to our continued success. We track attrition closely, as the competition with the private sector and other government agencies for talent will be an enduring challenge. An important element of building certain low-density skill sets, moreover, is outreach to and utilization of our Reserve Component.

Underpinning our readiness are the operational lessons we learn from continuous operations in cyberspace. Operations in support of JTF-Ares and the counter-terrorism fight, the security of the 2018 midterm elections, and ongoing support to combatant commands across both the defensive and offensive mission sets, are improving our training, informing how we structure our teams, and indicating how best to employ our capabilities and teams.

Enhancing Partnerships. Securing the nation in cyberspace requires whole-of-nation efforts and effective collaboration with allies. It is a priority for USCYBERCOM to expand its ability to collaborate effectively with other government agencies, the private sector, academia, and allies. We must do this because they directly and indirectly complement and enhance our warfighting capabilities; indeed, enabling our partners is a key element of persistent engagement. We are working with a range of partners who support, enable, and assist our operations.

The National Security Agency is our most important partner; the strength of this relationship will remain critical to the defense of the nation. The Agency's world-class

expertise, technical capabilities, and accesses are crucial to USCYBERCOM's success. The USCYBERCOM-NSA relationship is proving mutually beneficial as the Command has matured. Indeed, I believe the speed and agility that USCYBERCOM and NSA demonstrated in joint operations to defend last fall's elections is evidence of the mission benefit of unity of effort and direction, the close proximity between USCYBERCOM and NSA, and our joint focus on outcomes for the defense of the nation.

USCYBERCOM works daily with partners in DHS, FBI, and other federal agencies, sharing information and intelligence, as the U.S. government furthers efforts to work even more effectively with the private sector. Since May 2018 we have worked to broaden these ties, both at the leadership and the action-officer levels. I have mentioned last fall's whole-of-government effort to defend the mid-term elections, but our collaboration with interagency partners is continuous and far broader. We interact constantly with the US Coast Guard's cyber forces and have Coast Guard senior officers integrated in USCYBERCOM. In addition, the CYBER GUARD exercise last year included USCYBERCOM, DHS and FBI elements practicing a whole-of-government response to an incident involving the nation's critical infrastructure.

We see growing partnerships with industry (particularly in critical infrastructure sectors like energy and finance) as a natural extension of such relationships. Working with the DoD-Chief Information Officer and NSA, USCYBERCOM has developed a Pathfinder program with DHS, sector-specific agencies, and select critical infrastructure partners to share threat information, conduct collaborative analysis of vulnerabilities and threats, and mitigate those risks. This whole-of-nation collaboration is crucial to our ability to deter or defeat strategic threats to US national interests and infrastructure. This is a complex mission in both technical and policy terms, in part because our work in this field occurs at the request of and in collaboration with federal government partners, particularly DHS and FBI. Recent changes to our policy guidance -- especially those crafted in agreements with these and other agencies – have brought clarity to this process. By partnering with DHS, FBI, and sector-specific agencies we are building persistent presence to improve the resilience and the defense of our nation's critical infrastructure.

USCYBERCOM has been active with current and prospective foreign partners, especially countries contemplating or building their own cyber forces. We have integrees from our "Five Eyes" partners (including a Canadian brigadier general) on the Command staff. USCYBERCOM in FY 18 conducted bilateral cyber exercises with France, Estonia, and Japan, while two dozen countries sent observers to our annual CYBER FLAG exercise last June. We also provided advanced training to a FVEY partner via our first Foreign Military Sales case, and provided defensive operations guidance to Singapore. Lastly, we maintain robust operational relationships with a variety of international partners in the continued fight against violent extremist organizations globally.

We are building strategic depth in our cyber forces with assistance from the Reserve Component, and in so doing are assisting the whole-of-nation effort to secure our networks. Reservists serve in positions across our headquarters staff, the Cyber Mission Force, and our Service cyber components, as well as playing vital roles in our exercises and training for defending critical infrastructure. Indeed, our Reserve strategy seeks innovative ways to utilize the Reserve Component in unique missions. Finally, Reserve Component personnel not only bring important skill sets to USCYBERCOM, they also enhance our efforts to create cybersecurity coalitions of public and private partners, particularly with industry innovators.

Our engagement with the National Guard Bureau and the 54 state and territorial Adjutant Generals is continuous. We created a framework for DoD to sponsor access to classified information for National Guard personnel supporting local and state election systems while in a State Active Duty status (this was done in coordination with DHS and the National Guard Bureau). We are also exploring options with the National Guard State Partnership Program (SPP), which fosters trust with foreign militaries through bilateral engagements with roughly 70 partner nations. While our Command develops our global partnerships in the cyberspace domain, my intent is to work through the geographic combatant commands in growing theater security cooperation efforts.

Deploying Infrastructure. The Command depends on innovative cyber tools and capabilities in crafting strategic and tactical options for senior leaders. The DoD Chief

Information Officer and the Services are making necessary investments, in both funding and in finding the right people to develop and maintain cyber tools and capabilities. These Service investments need to continue and be balanced against global mission requirements. Such investments feature the right mix of capabilities for USCYBERCOM to achieve its readiness goals and generate successful mission outcomes.

Our cyberspace forces require a comprehensive, integrated cyberspace architecture to achieve and sustain the insight, agility, and lethality necessary for maintaining competitive advantage against near-peer adversaries. Over the past year we have developed the Joint Cyber Warfighting Architecture (JCWA) to guide capability development priorities to this end. The JCWA has five elements: common firing platforms at our four cyber operating locations (each operated and employed by our Service cyber components) using a comprehensive suite of cyber tools; a "Unified Platform" for integrating and analyzing data from both offensive and defensive operations with intelligence and partners (including the private sector); joint command and control mechanisms for situational awareness and battle management at the strategic, operational and tactical levels; sensors that support defense of the network and drive operational decisions; and a Persistent Cyber Training Environment where teams can train and even rehearse missions under realistic conditions. The JCWA is not a fixed future state, but rather an adapting set of capabilities continually evolving along with technological change, operational outcomes, and shifting threats. The Department has leveraged the architecture to make critical JCWA program investments that, when realized, will allow us to not only gain advantage in competition with cyber adversaries, but also to fight and win in conflict.

Acquisition authorities are also a critical enabler for us. I thank this Committee and Congress for extending our tailored acquisition authority through FY 2025, and will work with the Department to implement and recommend refinements. That extension allows us to craft more contract actions under our current authorities rather than having to leverage existing contracts held by other partners. In FY18 we executed 32 contract actions totaling $43 million, and we could reach as much as $75 million in this fiscal year. Our acquisition priorities include the geographically distributed set of redundant and reliable infrastructures noted above as well as a virtual arsenal of capabilities (comprising both open-source and high-end tools);

implementation of cloud and engineering services in support of a big data platform; foundational architecture portions of the Command's continuous monitoring capabilities; and a competitive cyber tool contract. Cyber tools can be highly perishable, unlike conventional munitions, but they are also like munitions in that, as they are expended, we must continuously invest in their development and procurement.

Conclusion

Thank you again for inviting me here today on behalf of U.S. Cyber Command. Your continued support is vital to the work we do, both to enable our partners and to act in cyberspace on behalf of our nation. USCYBERCOM made significant progress in the past year. We have been elevated to a Combatant Command and are maturing in our new responsibilities. All of our Cyber Mission Force teams are built and, in conjunction with the Services, we are working to enhance and sustain their readiness. The Department is investing in essential operational infrastructure and is committing additional resources to build the Joint Cyber Warfighting Architecture that the Command needs. Enabled by new law, policy, and mission guidance, we are conducting operations every day – both to support combatant commands and forces engaged overseas, and to contest cyber adversaries in defense of the nation. Persistent engagement initiatives, like the operations conducted in partnership across government, with allies, and with the private sector in defense of the 2018 elections, will cumulatively impose cost on our adversaries and change their risk calculus for future operations.

Looking ahead, the work we have done to date may soon seem both crucial and preliminary. We are in continuous daily contact in cyberspace with capable adversaries determined to erode our nation's strategic advantages. Our efforts to act against them and to enable our partner combatant commands, government agencies, and allies have helped to defend our nation and its interests. Those efforts, however, must rapidly become more agile, more capable, and more sustainable. My vision for the Command encompasses a continuous role for our forces in making our fellow combatant commands and our whole-of-nation partners even more effective in competition with adversaries and in preparing for and acting in conflict.

We have much work ahead, of course, and your continued endorsement and assistance are both necessary and gratefully appreciated. Our people are superb. They merit your trust, and, with your support, USCYBERCOM will continue to meet every challenge, in both competition and conflict.

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

MARCH 13, 2019

RESPONSE TO QUESTION SUBMITTED BY MS. STEFANIK

General NAKASONE. Section 807 of the FY 2016 NDAA does not specifically define cyber-peculiar. However, the 2016 DOD implementation plan submitted pursuant to Section 807 of the FY 2016 NDAA provides "cyber operations-peculiar (CO-peculiar)" and "cyber capability-peculiar" equipment, capabilities and services as "Equipment, materiel, supplies, non-materiel solutions, and services required for select joint CO-peculiar requirements or established DOD Agency-provided service or product." In the Report on USCYBERCOM Acquisition Authority submitted pursuant to the Joint Explanatory Statement accompanying Section 1635 of the FY19 National Defense Authorization Act, dated Oct 2018, USCYBERCOM defined cyber-peculiar capabilities and services as: Any acquisition effort that supports or facilitates any of the three Cyberspace Missions as defined in Joint Pub 3–12; Offensive Cyber Operations, Defensive Cyber Operations, or Department of Defense Information Network operation. These three mission types comprehensively cover the activities of the cyberspace forces. [See page 14.]

QUESTIONS SUBMITTED BY MEMBERS POST HEARING

MARCH 13, 2019

QUESTIONS SUBMITTED BY MR. LARSEN

Mr. LARSEN. Given adversary exfiltration of sensitive data from the DIB: How can the Department of Defense work to promote cybersecurity within the DIB? What tools exist to require robust cybersecurity as part of the contracting process? How does the Department help the DIB detect and report cyber incidents? What potential consequences exist for a contractor that fails to practice robust cybersecurity?

Secretary RAPUANO. The Department of Defense (DOD) promotes cybersecurity within the defense industrial base (DIB) through two primary means: a voluntary information sharing program with DIB entities and through requirements directed by the Defense Federal Acquisition Regulation Supplement (DFARS).

- Voluntary Information Sharing: DOD's DIB Cybersecurity (CS) Program enhances and supplements DIB participants' capabilities to safeguard DOD information that resides on or transits DIB unclassified networks or information systems. Under the DIB CS Program, DOD and DIB participants share unclassified and classified cyber threat information to bolster public and private cybersecurity postures and receive technical assistance from the DOD Cyber Crime Center (DC3) including analyst-to-analyst exchanges, mitigation and remediation strategies, and best practices.
- Mandatory Reporting Requirements: DFARS 252.204–7012 directs contractors to rapidly report cyber incidents to DOD when incidents are discovered that affect a covered contractor information system or the covered defense information residing therein, or that affects the contractor's ability to perform the requirements of the contract that are designated as operationally critical support. When contractors discover malicious software in connection with a reported cyber incident, that malicious software must be submitted to DC3.
- Minimum Cybersecurity Standards: DFARS 252.204–7012 requires contractors to safeguard covered defense information that resides on a contractor's internal unclassified information system by implementing the security requirements in National Institute of Standards and Technology (NIST) Special Publication 800–171 "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations." Contractors that fail to implement DFARS 252.204–7012 requirements when applicable to contract performance may be subject to contractual, administrative, and civil remedies by DOD.