S. HRG. 118–793

THE NOMINATION OF LIEUTENANT GENERAL TIMOTHY D. HAUGH, USAF TO BE GENERAL AND DIRECTOR, NATIONAL SECURITY AGENCY/CHIEF, CENTRAL SECURITY SERVICE/COMMANDER, UNITED STATES CYBER COMMAND

HEARING

BEFORE THE

COMMITTEE ON ARMED SERVICES
UNITED STATES SENATE

ONE HUNDRED EIGHTEENTH CONGRESS

FIRST SESSION

JULY 20, 2023

Printed for the use of the Committee on Armed Services

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

U.S. GOVERNMENT PUBLISHING OFFICE
63–668 WASHINGTON : 2026

COMMITTEE ON ARMED SERVICES

JACK REED, Rhode Island, *Chairman*

JEANNE SHAHEEN, New Hampshire	ROGER F. WICKER, Mississippi
KIRSTEN E. GILLIBRAND, New York	DEB FISCHER, Nebraska
RICHARD BLUMENTHAL, Connecticut	TOM COTTON, Arkansas
MAZIE K. HIRONO, Hawaii	MIKE ROUNDS, South Dakota
TIM KAINE, Virginia	JONI ERNST, Iowa
ANGUS S. KING, Jr., Maine	DAN SULLIVAN, Alaska
ELIZABETH WARREN, Massachusetts	KEVIN CRAMER, North Dakota
GARY C. PETERS, Michigan	RICK SCOTT, Florida
JOE MANCHIN III, West Virginia	TOMMY TUBERVILLE, Alabama
TAMMY DUCKWORTH, Illinois	MARKWAYNE MULLIN, Oklahoma
JACKY ROSEN, Nevada	TED BUDD, North Carolina
MARK KELLY, Arizona	ERIC SCHMITT, Missouri

ELIZABETH L. KING, *Staff Director*
JOHN P. KEAST, *Minority Staff Director*

CONTENTS

JULY 20, 2023

This hearing is printed to include all available information requested or required to be inserted for the record.

THE NOMINATION OF LIEUTENANT GENERAL TIMOTHY D. HAUGH, USAF TO BE GENERAL AND DIRECTOR, NATIONAL SECURITY AGENCY/CHIEF, CENTRAL SECURITY SERVICE/COMMANDER, UNITED STATES CYBER COMMAND

THURSDAY, JULY 20, 2023

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

The Committee met, pursuant to notice, at 9:02 a.m. in room SD-G50, Dirksen Senate Office Building, Senator Jack Reed (Chairman of the Committee) presiding.

Committee Members present: Senators Reed, Shaheen, Gillibrand, Kaine, King, Warren, Peters, Manchin, Rosen, Wicker, Fischer, Cotton, Rounds, Ernst, Scott, Mullin, Budd, and Schmitt.

OPENING STATEMENT OF SENATOR JACK REED

Chairman REED. Good morning. The Committee meets today to consider the nomination of Lieutenant General Timothy Haugh to be promoted to general and to be the next commander of U.S. Cyber Command and director of the National Security Agency.

General, congratulations on your nomination. I would also like to welcome your wife Sherry, your daughter Chandler, your daughter-in-law Hannah, and your son Michael. We are grateful to your family for the support they have given you and the military over many years.

Let me also recognize the outgoing commander General Nakasone as he prepares for retirement. I would like to express my appreciation for his 37 years of service to the Nation including his outstanding leadership of the United States cyber and intelligence forces.

General Haugh, the Committee welcomes your nomination to lead CYBERCOM and the NSA. As the current deputy you have a comprehensive understanding of the urgent cybersecurity and intelligence challenges facing the Nation.

You have held a number of senior positions at CYBERCOM and within the Air Force cyber and intelligence organizations and commands including multiple command assignments. These experiences will serve you well.

General, if confirmed, there are a number of pressing issues that will require your attention. First and foremost, it is widely under-

stood that our cyber mission forces are struggling with readiness shortfalls caused primarily by difficulties in training and retaining personnel in key positions requiring special skills.

In order to mature the cyber force and advance our Nation's capabilities to conduct cyber operations and support intelligence operations the military services must provide qualified and trained personnel to your command on time and at the beginning of their tours.

I would also note that the private sector has realized the immense value of our cyber operators and is offering them very high compensation to leave the military. The services must adjust accordingly by providing a creative combination of incentives to compete for and retain these personnel. I would like to know how you plan to address this challenge.

Additionally, over the last decade there has been a recurring debate over whether to sustain the dual hat arrangement whereby the commander of Cyber Command also serves as the director of the NSA.

Recently, an independent panel established by the Director of National Intelligence and the Secretary of Defense and led by former Chairman of the Joint Chiefs of Staff General Joe Dunford concluded that the dual hat arrangement should be sustained and we would welcome your thoughts on that issue also.

Finally, I would note that some of the tools in our toolbox like section 702 authority from the Foreign Intelligence Surveillance Act, or FISA, are critical to our ability to counter our adversaries' malign activities.

The Committee would appreciate your views on the importance of section 702 of FISA, which sunsets at the end of this year, and why you believe it is essential that we renew that authority.

We would also like to know what guardrails are in place to give the public confidence that the authority is being used judiciously.

General, these complex challenges will require the full complement of your skills. Thank you for your willingness to continue your service and lead CYBERCOM and the NSA at this critical time. I look forward to your testimony.

Let me now recognize the ranking Member, Senator Wicker.

STATEMENT OF SENATOR ROGER F. WICKER

Senator WICKER. Thank you, Mr. Chairman, and thank you, General Haugh, for being here and I join the distinguished chairman in welcoming your family.

You have been nominated by the President for commander of the United States Cyber Command. If confirmed you will be directly responsible for planning and executing U.S. global cyber operations activities and missions to defend our national interest across the full spectrum of competition and conflict in cyberspace.

This includes Department of Defense's (DOD's) cyberspace operations, enhancing the offensive and defensive capabilities of the cyber mission force, and improving the readiness of the Nation's cyber personnel to counter malicious cyber actors in a changing digital domain.

This hearing comes at a pivotal moment for defending cyberspace. General Nakasone, our Nation's outgoing commander of

Cyber Command, has said the growth in cyber warfare capabilities by our near peer adversaries like China is unlike anything he has seen before.

In recent months we have seen an increase in ransomware attacks on critical infrastructure and aggressive cyber espionage operations on U.S. networks by our near peer adversaries.

Software vulnerabilities and weak network perimeter security have added to the Nation's defensive challenges and threaten our strategic ability and decisive advantage in cyberspace.

We must keep that decisive advantage. Advancements in technology such as artificial intelligence are also poised to change the pace of the threats we face. Given these challenges, the Committee would like to learn how you plan to address the most pressing national security challenges facing our Nation in cyberspace.

Specifically, I am interested in hearing what you would do to ensure CYBERCOM's defend forward and persistent engagement strategies. Those strategies support a proactive military posture in cyberspace and remain capable of disrupting malicious cyber activity at its source and keep pace with an evolving threat.

I am concerned that our cyber readiness may suffer because of cyber mission forces serving brief tours at CYBERCOM, and the chair mentioned this in his statement. The services are providing personnel to CYBERCOM who lack necessary cyber skills, technical expertise, and training.

I would welcome your views on how to correct readiness shortfalls within the cyber mission force including how you would work with the services to align training across the department and increase the resiliency of the cyber workforce.

Strengthening partnerships across the government, private sector, and among our allies is also key to defending our national interests in a constantly evolving threat environment.

These include Hunt Forward operations in which cyber operators are deployed abroad to identify vulnerabilities and malware on the networks of partner nations. The under advisement program, which creates a forum for threat information sharing with industry, is another example of Cyber Command's unique contributions to national security.

These two initiatives exemplify how our cyber forces augment Homeland and network defenses while also exposing adversary tactics before they can be used against us in the United States.

I hope you will speak about how you would prioritize partnerships to meet the growing complexity of challenges in the cyber domain.

If confirmed, General, you would serve as the chief of the Central Security Service and would take on a dual-hatted role as director of the National Security Agency and so we will be interested in hearing your perspective on the dual hat arrangement and how it impacts CYBERCOM's ability to fulfill its individual mission.

So thank you very much, General, and thank you, Mr. Chairman.

Chairman REED. Thank you, Senator Wicker.

General Haugh, your statement, please?

STATEMENT OF LIEUTENANT GENERAL TIMOTHY D. HAUGH, USAF, TO BE GENERAL AND DIRECTOR, NATIONAL SECURITY AGENCY/CHIEF, CENTRAL SECURITY SERVICE/COMMANDER, UNITED STATES CYBER COMMAND

Lieutenant General HAUGH. Chairman Reed, Ranking Member Wicker, and distinguished members of the Committee, I am honored to appear before you today regarding my nomination as commander of U.S. Cyber Command and director of the National Security Agency.

I want to thank President Biden, Secretary Austin, Director Haines, and General Milley for their trust in nominating me for these critical positions. I would also like to thank my bride Sherry who has served with me for the last 31 years.

I would also like to thank our children, Michael and Chandler, who have sacrificed as military children are now thriving as adults. Michael is a captain and company commander in the North Carolina National Guard and Chandler is a commercial cybersecurity analyst.

Sherry and I are incredibly grateful for their sacrifices to enable our service as a family. Also with us today is our daughter-in-law Hannah, a director of strategy and product development for an advanced materials company. Joining us virtually is my mom, Leona, who with my late father instilled the value of service at an early age. Thank you, Mom.

I want to begin by thanking General Nakasone and Susan Nakasone for their service to the United States Cyber Command and National Security Agency. General Nakasone has 37 years of dedicated service culminating as commander and director for the last 5 years.

His commitment to both the mission and the people during a time of unparalleled global change has continued the legacy captured in the command's code—partner, enable, deliver. I truly believe that Cyber Command has delivered for the Nation due to his leadership.

A special thanks to Susan Nakasone for her commitment to her family and for her willingness to focus on and address tough issues facing the Army, the agency, and the command's spouses and families.

I am a career intelligence officer who has served 31 years in the joint force intelligence and cyber communities. My service and command and staff positions at all levels to include multiple assignments within Cyber Command, NSA, and the cryptologic enterprise have given me unique insights of the opportunities and challenges facing the Nation and the critical roles of Cyber Command and NSA.

As part of Cyber Command's senior leadership team and in my prior roles within the command I have gained invaluable operational experience in cyber and an appreciation for the unparalleled mission advantage that stems from the close operating partnership of these two organizations.

I consider it the highest privilege to be nominated to lead these organizations and, if confirmed, I am committed to further buildupon our competitive strengths—people, innovation, and partnerships.

I believe every great success starts with people. Both NSA and Cyber Command have some of the Nation's most talented individuals who are the backbone of mission success. To sustain that success we must focus on recruiting, training, and retaining talent from across the Nation and must provide an environment where they can thrive and succeed.

For Cyber Command that means continued focus on readiness and the growth of our acquisition force. For NSA it means hiring the right workforce for the challenges we face during a period of significant retirement turnover.

In an environment of accelerating change the ability to rapidly adapt and innovate is critical to mission advantage. Congress and the department have set the conditions for Cyber Command to rapidly mature. The expansion of its acquisition authorities and the ongoing implementation of enhanced budget control will enable improved capabilities across the force.

When coupled with the authorities to partner with industry and small business Cyber Command can deliver innovative cyber capabilities for warfighting advantage. Partnerships are a critical component of both organizations' success. The ability to work in collaboration across the interagency with the private sector and foreign partners is critically important to our Nation's success in a world of accelerating change.

We see this in the work of both organizations with partners throughout Government such as the Cybersecurity and Infrastructure Agency (CISA), FBI, as well as expanding efforts to build cybersecurity relationships worldwide.

The command's Hunt Forward operations and collaborative exposure of adversary cyber actions within NSA are proven examples to build upon.

If confirmed, I will focus on ensuring the health and effectiveness of NSA and Cyber Command's world class personnel in delivering outcomes to address the Nation's highest—the nation's security priorities. Also the priorities of the department and the combatant commands.

I will focus on strengthening the workforce, improving the readiness of our cyber mission force, investing to leverage new technologies and prioritizing threats facing the Nation, especially those from the pacing challenge posed by the People's Republic of China (PRC).

In closing, I am deeply honored to be considered for these leadership positions. If confirmed, I look forward to working with the Committee and the entire Congress to ensure we leverage our opportunities and address these challenges.

Chairman Reed, Ranking Member Wicker, and distinguished Members of the Committee, thank you for the opportunity to be here this morning. I look forward to answering your question.

Chairman REED Thank you very much, General Haugh.

I have a series of questions which are presented to all nominees. Please respond accordingly.

Have you adhered to applicable laws and regulations governing conflicts of interest?

Lieutenant General HAUGH. Yes, Chairman.

Chairman REED. Have you assumed any duties or taken any actions that would appear to presume the outcome of this confirmation process?

Lieutenant General HAUGH. No, Chairman.

Chairman REED. Exercising our legislative and oversight responsibilities makes it important that this Committee, its subcommittees, and other appropriate committees of Congress receive testimony, briefings, reports, records, and other information from the executive branch on a timely basis. Do you agree if confirmed to appear and testify before this Committee when requested?

Lieutenant General HAUGH. Yes, Chairman.

Chairman REED. Do you agree when asked before this Committee to give your personal views even if your views differ from the administration?

Lieutenant General HAUGH. Yes, Chairman.

Chairman REED. Do you agree to provide records documents and electronic communications in a timely manner when requested by this Committee, its subcommittees, or other appropriate committees of Congress and to consult with the requester regarding the basis for any good faith delay or denial in providing such records?

Lieutenant General HAUGH. Yes, Chairman.

Chairman REED. Will you ensure that your staff complies with deadlines established by this Committee for the production of reports, records, and other information, including timely responding to hearing questions for the record?

Lieutenant General HAUGH. Yes, Chairman.

Chairman REED. Will you cooperate in providing witnesses and briefers in response to congressional request?

Lieutenant General HAUGH. Yes, Chairman.

Chairman REED. Will those witnesses and briefers be protected from reprisal for their testimony or briefings?

Lieutenant General HAUGH. Yes, Chairman.

Chairman REED. Thank you very much, General.

As we both mentioned, Senator Wicker and I, one of the issues that you have addressed also is the cyber mission forces and their readiness. This is, I believe, General Nakasone's number-one challenge at this moment and it will be yours.

Where do you see this in terms of your priorities? I assume it is very close to top. And second, these forces are composed by members from the other services and how do you coordinate so that these people come ready and willing to serve and to function?

Lieutenant General HAUGH. Senator, from a cyber readiness perspective this is the top issue for Cyber Command. We just recently in response to requests from Congress submitted a report for section 1502 that identified the Cyber Command assessment of readiness and what that report says is we view fiscal year 2024 and the overall passing of both the NDAA and the appropriations bill as a critical moment that now aligns the responsibilities and authorities within U.S. Cyber Command analogous to those of U.S. Special Operations Command (SOCOM).

With the passing of the fiscal year 2024 appropriations bill U.S. Cyber Command will now have the responsibility for the cyber mission force budget, will have the responsibility for the acquisition of

the capabilities for our cyber mission force, and have the authority to set the training standards.

With those authorities it allows Cyber Command to set the investment in our training infrastructure, in our training courses, and allows the services to focus on recruiting, initial skills training aligned to our standard, and then to leverage the retention capabilities that Congress has given to the services. So those are areas now that really change the dynamic of how we will approach cyber readiness, if confirmed.

Chairman REED. Thank you, General.

General, I also mentioned in my opening remarks Section 702 of FISA, and could you comment on the importance of extending that—it will expire at the end of this year—and also the guardrails that are in place to protect the privacy of citizens in the United States?

Lieutenant General HAUGH. Senator, section 702 is an irreplaceable foreign intelligence authority. It enables the intelligence community to collect against foreign persons overseas.

It is a critical authority and as I think of it in my current role as U.S. Cyber Command the ability to identify foreign hacking of activities in the United States, whether that be U.S. companies or individuals, it is a critical source to be able to do that.

Section 702 supports 100 percent of the President's intelligence priorities. In some way it reflects either in the answer or informs that question in terms of how we ensure oversight.

First and foremost, in my experience in working with the National Security Agency throughout my career is a culture of compliance. The National Security Agency and all of the employees are focused on how to protect their fellow Americans and that includes their civil liberties.

So that inside of section 702 is a rigorous set of oversight both through personal accountability as well as technical accountability to ensure that the authority is used appropriately for its intended purpose for foreign persons overseas.

Chairman REED. Thank you. I also in my comments referred to the Dunford report regarding the status of the NSA director and commander of CYBERCOM. I assume you concur with the results of that report and I think it establishes a very good sort of framework to continue the dual hatting.

Your comments?

Lieutenant General HAUGH. Senator, I do support the results of General Dunford's study that was accepted by both the Secretary and the Director of National Intelligence. What it reflects is really a maturation of U.S. Cyber Command and that relationship and operational partnership with the National Security Agency being in the best interests of the Nation.

What it allows is, in reality, the signal's intelligence and the cyber environments are overlapping. So having a single leader with the ability to align the capabilities of NSA and Cyber Command gives us greater speed and agility.

It also allows us to at the beginning of planning be very considerate of how do we protect intelligence sources while still being able to position to produce the outcomes the Nation needs to staff.

Chairman REED. Thank you very much, General Haugh.

Before I recognize Senator Wicker, since a quorum is now present I ask the Committee to consider a list of 2,699 pending military nominations. Including in this list are the nominations of General Charles Q. Brown, Jr., United States Air Force to be Chairman of the Joint Chiefs of Staff, and General Randy A. George, the United States Army, be to the grade of general and to be Chief of Staff of the Army. All of these nominations have been before the Committee in the required time.

Is there a motion to favorably report this list?

Senator WICKER. Mr. Chairman, I so move.

Chairman REED. Is there a second?

VOICE. Second.

Chairman REED. All in favor say aye.

The motion carries.

[The list of nominations considered and approved by the Committee follows:]

MILITARY NOMINATIONS PENDING WITH THE SENATE ARMED SERVICES COMMITTEE WHICH ARE PROPOSED FOR THE COMMITTEE'S CONSIDERATION ON JULY 20, 2023.

1. **General Randy A. George, USA to be general and Chief of Staff of the Army** (Reference No. 537)
2. In the Air Force there are 83 appointments to the grade of lieutenant colonel (list begins with Julie L. Airhart) (Reference No. 599)
3. **General Charles Q. Brown, Jr., USAF to be general and Chairman of the Joint Chiefs of Staff** (Reference No. 677)
4. In the Air Force there are 30 appointments to the grade of lieutenant colonel (list begins with Justin V. Ahrens) (Reference No. 696)
5. **In the Army there are 2 appointments to the grade of major general (list begins with Mary V. Krueger)** (Reference No. 775)
6. **Col. Jack J. Stumme, USA to be brigadier general** (Reference No. 776)
7. In the Air Force Reserve there is 1 appointment to the grade of colonel (Oliver E. Barfield) (Reference No. 777)
8. In the Air Force Reserve there are 2 appointments to the grade of colonel (list begins with Ashley L. Shull) (Reference No. 778)
9. In the Air Force Reserve there are 73 appointments to the grade of colonel (list begins with Ronald Mark Alligood) (Reference No. 779)
10. In the Air Force Reserve there are 158 appointments to the grade of colonel (list begins with Brian Charles Anderson) (Reference No. 780)
11. In the Army there is 1 appointment to the grade of lieutenant colonel (Paul A. Stelzer) (Reference No. 781)
12. In the Marine Corps there is 1 appointment to the grade of colonel (Leron E. Lane) (Reference No. 783)
13. In the Navy there is 1 appointment to the grade of lieutenant commander (Andres S. Pscoya) (Reference No. 784)
14. **Col. James F. Porter, USAR to be brigadier general** (Reference No. 787)
15. **BG Beth A. Salisbury, USAR to be major general** (Reference No. 788)
16. In the Army there is 1 appointment to the grade of major (Andrew R. Updike) (Reference No. 789)
17. In the Army there is 1 appointment to the grade of colonel (Erica L. Kane) (Reference No. 791)
18. In the Army there are 31 appointments to the grade of lieutenant colonel (list begins with Joshua T. Ade) (Reference No. 792)
19. In the Marine Corps there is 1 appointment to the grade of major (William M. Schweitzer) (Reference No. 793)
20. **MG Michael J. Lutton, USAF to be lieutenant general and Deputy Commander, Air Force Global Strike Command** (Reference No. 818)
21. **LTG James J. Mingus, USA to be general and Vice Chief of Staff of the Army** (Reference No. 819)

22. **MG Thomas L. James, USA to be lieutenant general and Deputy Commander, US Space Command** (Reference No. 820)
23. **MG Charles D. Constanza, USA to be lieutenant general and Commanding General, V Corps** (Reference No. 822)
24. **MG James H. Adams III, USMC to be lieutenant general and Deputy Commandant for Programs and Resources, Headquarters, US Marine Corps** (Reference No. 823)
25. **LTG Michael A. Guetlein, USSF to be general and Vice Chief of Space Operations** (Reference No. 826)
26. **LTG Philip A. Garrant, USSF to be lieutenant general and Commander, Space Systems Command, US Space Force** (Reference No. 828)
27. **In the Space Force there are 3 appointments to the grade of major general (list begins with Donald J. Cothern)** (Reference No. 829)
28. In the Air Force there is 1 appointment to the grade of lieutenant colonel (Ryan C. Boyle) (Reference No. 839)
29. In the Air Force there are 359 appointments to the grade of major (Feysel A. Abdulkaf) (Reference No. 840)
30. In the Air Force there are 49 appointments to the grade of major (Scott A. Abuso) (Reference No. 841)
31. In the Air Force there are 391 appointments to the grade of major (Nanlisha T. Abdullai) (Reference No. 842)
32. In the Air Force there are 160 appointments to the grade of major (Matthew N. Alombro) (Reference No. 843)
33. In the Air Force there are 1,201 appointments to the grade of major (Kevin B. Abbott) (Reference No. 844)
34. In the Air Force there is 1 appointment to the grade of colonel (James H. Gutzman) (Reference No. 845)
35. In the Air Force there are 53 appointments to the grade of lieutenant colonel (Danielle N. Anderson) (Reference No. 846)
36. In the Air Force there is 1 appointment to the grade of major (Ryan C. Caguillo) (Reference No. 847)
37. In the Air Force there is 1 appointment to the grade of colonel (Mary M. Gutierrez) (Reference No. 848)
38. In the Air Force Reserve there is 1 appointment to the grade of colonel (Edward W. Hale) (Reference No. 849)
39. In the Army there is 1 appointment to the grade of colonel (Charles K. Djou) (Reference No. 850)
40. In the Army there is 1 appointment to the grade of major (Nicholas C. Molczyk) (Reference No. 851)
41. In the Army there is 1 appointment to the grade of major (David Hernandez) (Reference No. 852)
42. In the Army there is 1 appointment to the grade of colonel (Clydellia S. Prichard-Allen) (Reference No. 853)
43. In the Army Reserve there is 1 appointment to the grade of colonel (Espada J. Ruiz) (Reference No. 854)
44. In the Navy there are 4 appointments to the grade of lieutenant commander (list begins with Mary M. Ayres) (Reference No. 856)
45. In the Navy there is 1 appointment to the grade of lieutenant commander (Daniel I. Morrison) (Reference No. 857)
46. In the Navy there is 1 appointment to the grade of lieutenant commander (Alan A. Gutberlet) (Reference No. 858)
47. In the Navy there is 1 appointment to the grade of commander (Guillermo M. Arguello) (Reference No. 859)
48. In the Navy there is 1 appointment to the grade of captain (Christopher S. Williams) (Reference No. 860)
49. In the Navy there is 1 appointment to the grade of captain (Kristopher M. Brazil) (Reference No. 861)
50. In the Navy there are 10 appointments to the grade of captain (list begins with Joshua P. Corbin) (Reference No. 862)
51. In the Navy there are 14 appointments to the grade of commander (list begins with Nicholas B. Artabazon) (Reference No. 863)

52. In the Navy there are 39 appointments to the grade of lieutenant commander (list begins with Mary H. Baker) (Reference No. 864)
53. In the Navy there is 1 appointment to the grade of captain (Peter J. Maculan) (Reference No. 865)
54. **MG Shawn N. Bratton, ANG to be major general** (Reference No. 866)
55. **MG Shawn N. Bratton, USSF to be lieutenant general and Deputy Chief of Space Operations for Strategy, Plans, Programs, and Requirements** (Reference No. 867)

TOTAL: 2,699

Senator Wicker? Senator WICKER. On the dual hat, General, is the statute where it should be with regard to what you need in that role?

Lieutenant General HAUGH. Senator, I think we have the guidance we need to be effective. An area that we would like to—that, if confirmed, I would like to work with the Committee is how do we communicate and ensure oversight with all of the respective committees to ensure that we are being very clear in how we are using the authorities of each of those organizations to the best effect consistent with our law, our policy, and our values.

Senator WICKER. Do you think this arrangement should always be the approach or do you see a time when another administration might not choose to go the dual hat?

Lieutenant General HAUGH. Senator and Ranking Member, in my experience, I have now worked in each sides of these organizations and so how we partner and be able to take the guidance from a single leader becomes effective in our response.

So we can move with the speed and agility today. So, from my perspective, I think that would be very difficult to replicate in a different configuration.

Senator WICKER. You would not change that?

Lieutenant General HAUGH. In my perspective I would not change that, Senator. Senator WICKER. Okay. And then on the training or lack thereof or areas for improvement tell us to what extent that is enlisted personnel officers and how about civilian hires? Lieutenant General HAUGH. Ranking Member, in terms of training in the cyber mission force the overall makeup of the cyber mission forces themselves, our technical operational elements are about 80 percent military and 20 percent civilian.

So as we approach this it is, largely, a civilian force with a significant number of officers that are balanced by civilians.

As we look at that force one of the things that we want to ensure as U.S. Cyber Command is that we are setting that baseline standard so that we can ensure across the department we get the baseline right and allow the services to do that baseline training, and now Congress has equipped us with the authority to build out the training ranges.

We have those in place today as U.S. Cyber Command the authority to build out the advanced training, which we have in place today, within U.S. Cyber Command, the National Security Agency, and now we will have the resources to scale that training.

Senator WICKER. Which one is the 80 percent?

Lieutenant General HAUGH. The 80 percent is military—

Senator WICKER. Okay.

Lieutenant General HAUGH.—and of that the majority would be enlisted.

Senator WICKER. I see. Okay. And so they would not necessarily have come to the service with cyber skills. They would have learned what they need as members of the military?

Lieutenant General HAUGH. We would—Ranking Member, what we would expect is that they would all get baselined in their service training. Many of them, the services, are doing assessments early either in the recruiting process or at basic training to assess and identify, and we will encourage and work with the services to increase that as we go forward.

Senator WICKER. It does not hurt that quite a number of whiz kids that have been playing video games since they have been able to walk are stepping forward.

Lieutenant General HAUGH. Ranking Member, there is certainly a population that is digital—that have grown up as digital natives.

Senator WICKER. Take a minute then and tell us about the under advisement program and the Hunt Forward operations, which are partnerships with your command.

Lieutenant General HAUGH. Senator, 2 years ago Congress authorized both Cyber Command and NSA to be able to do direct sharing with industry. Inside of U.S. Cyber Command, inside our sub unified command of the cyber national mission force Cyber Command created a program called Under Advisement.

Our Under Advisement program allows a small team to interact directly with industry and it helps us to be able to have an understanding of activities overseas through their lens and identify cyber threats while also allowing us to provide insights to them about threats that they might receive wherever they operate.

The Under Advisement team is also nested very closely with NSA's cybersecurity collaboration center that was also authorized by the same portion of the law as well as by DOD to do direction with industry. That is a critical component that we will seek to expand.

The Hunt Forward operations are activities of where we defend forward with a partner or ally within their networks. So they ask for our assistance. We deploy a team of experts from the cyber mission force to work with them on a network.

Provides value to us because we are able to identify adversary malware and to be able to disclose that not just to that company or to that nation but also to cybersecurity industry. It also allows us to work with those partners, build trust and confidence, and allow them to also grow their capacity.

Senator WICKER. Thank you, sir.

Chairman REED. Thank you, Senator Wicker.

Senator Shaheen, please?

Senator SHAHEEN. Thank you, Mr. Chairman.

Lieutenant General Haugh, congratulations on your nomination to you and thank you for your willingness to continue to serve and thank you to your family for their willingness to support you.

How do you see developments in AI affecting CYBERCOM and NSA?

Lieutenant General HAUGH. Senator, I think about artificial intelligence really in three ways. One is how do we leverage it to be

able to allow our personnel to be able to move faster, do that in a way that we can ensure from a national security perspective we are using it in an ethical manner, that we can see the sources of that data, ensure civil liberties are protected. But there is great opportunity, particularly from a cybersecurity perspective, when we think about scale.

The second component—

Senator SHAHEEN. Can I just interrupt for a minute? Because you say using in an ethical manner. How do you determine that? Because there are not really standards around AI at this point.

Lieutenant General HAUGH. So DOD has published AI ethical standards so there is a start point for us. For us, what we really want to do is have a partnership between a human analyst and their ability to receive data, know where that data came from, and to be able to accelerate their work, and that is an area that we are doing a study, building an AI roadmap as directed by Congress to do that with the department focused on Cyber Command and Cyber Command's interest.

The other area that I think the Nation expects from us is to understand how our adversaries use this technology and be able to inform what that looks like in terms of threat both to our national security and to our industry.

Senator SHAHEEN. And there was a lot of discussion in the earlier questioning about training and recruitment of people to Cyber Command. Is there particular training that you think we ought to be doing around AI and how do you see that? Is that something that should be done by Cyber Command? Is it a broader concern across DOD?

Lieutenant General HAUGH. Senator, in terms of Cyber Command our close partnership with the National Security Agency does allow us to build on a legacy of how NSA has leveraged data, has leveraged algorithms, has done it from its outset in a very compliant way to ensure that it is consistent with what we would expect in terms of protecting civil liberties.

So we start with a foundation in that partnership. The other area where AI has certainly been a key component within our Nation is in cybersecurity. So we start from a foundation that does look a little bit different from the rest of the department and there are areas for us that we will certainly need to be partnered with the services as they protect networks, as we give guidance for how best to apply, and think about under our acquisition authorities the ability to be able to partner with a service, partner with a small business, rapidly introduce that technology but do it in a way that is consistent with overall DOD guidance for how we do that from an ethical perspective.

Senator SHAHEEN. And you mentioned how our adversaries would be using AI. We heard from some experts earlier this week who talked about the real threat from AI and how it could be used to harm citizens in the United States and, really, around the world.

So do we need to be thinking about other regulatory responses, other penalties for those nation states and other groups that would use AI in a way that would damage the United States?

Lieutenant General HAUGH. Senator, I will not comment on the regulatory requirement but I will talk about the threat. When we

think about where China has focused much of their AI it is about information control. It is about facial recognition. It is about dominating a population.

So as they consider exporting those technologies as they have done in the past with the Great Firewall technology, it is an area from a threat perspective that we should continue to inform and understand what that means to any nation that they would be considering partnering with and the implications of that technology on that society.

Senator SHAHEEN. Thank you. I think it is something this Committee needs to continue to look at as well.

The war in Ukraine has produced less of an attack on the cyber infrastructure of Ukraine than I expected and I think that most people expected. Do you think that Ukraine is prepared to handle future attacks by Russia on their infrastructure and other utility grid in other areas?

Lieutenant General HAUGH. Senator, Ukraine gets a lot of credit for how they created resiliency in the face of a really relentless cyber actor in Russia.

They have—they thought before when they were given advance warning how to think about their data and where their data needed to be to be resilient. They thought about their partnerships with industry, their partnerships with NATO, certainly with the United States and with the department to be able to assist and how we provided an opportunity to make sure that they understood threat and they have done an exceptional job of thinking about what it looks like to be resilient in a really relentless digital environment. One of the reasons Russia has not been successful is the resilience of Ukraine.

Senator SHAHEEN. Well, thank you. I certainly agree. Thank you, Mr. Chairman. Chairman REED. Thank you, Senator Shaheen.

Senator Mullin, please?

Senator MULLIN. Thank you, Chairman. General, thank you so much for being here. It is lovely to see your family with you. It was a pleasure to meet them before the hearing started. And as I said back there, I just want to thank your family and your wife for serving alongside of you. Thank you for all that you do in holding the family together.

I have said this many times to people that work for me and people I have worked with, we can only be at our best if we—if we have a stable home life. If it is rocky we can be average, and your husband cannot afford to be average, not in this time. So thank you for laying that foundation for him to reach greatness.

General, I just want to ask a couple questions. I have made no bones about it that your predecessor and I do not get along. I do not agree with his decisionmaking.

I have made it very clear that he is very risk averse and lacks the ability to take responsibility when things do not go right, and so I want to make sure that we are not following necessarily all in his footsteps.

And so some of the questions I have really deals with some changes that you may be looking to make and I would like to get your insight in those. In your time as the deputy commander what

was the collaboration between CYBERCOM and other combatant commands? What does that look like?

Lieutenant General HAUGH. Senator, in terms of collaboration with the other combatant commands if we look at the overall National Defense Strategy we do sit in a unique place.

As a global combatant command our partnerships with each of the other combatant commands, our missions to ensure defense of the Department of Defense Information Network enables every other combatant command and we are partnered with them on that.

Our mission to defend the Nation in cyberspace is to ensure that those other combatant commands are resilient to attack by a cyber adversary. And then our third mission is to support those combatant commands with offensive and defensive cyber.

What you have seen is a maturation over the last 5 years of looking at how our elements that we provide to those combatant commands—we have teams between 30 and 50 that are embedded inside of each of the combatant commands to be able to link together to either enable their planning or help them to conduct planning so that we are integrated.

And as we think about it Ukraine has provided a really good example. I was a component to European Command at the time and so General Wolters gave us very clear requirements for how Air Force's cyber and then the broader Cyber Command enterprise could support EUCOM and NATO in their efforts to enable Ukraine.

Senator MULLIN. Do you have any examples of changes that you might want to see, moving forward—things that we could do better in those areas?

Lieutenant General HAUGH. Senator, I think the number-one thing that we will be thinking about—we have talked about cyber mission force and the relationship with the new authorities that Congress and the department are giving us.

The other thing that comes with that is an opportunity to scale. So when we think about the things that we are doing well today and our ability to defend forward, having budget control, having acquisition authority, having more control of the overall advanced training will allow us to scale and scale faster.

Senator MULLIN. How has CYBERCOM collaborated with industry partners in the past and how do we look at changing those relationships, moving forward?

Lieutenant General HAUGH. Senator, we have today authorities from both—from OSD that allow us to do partnerships with small business. So whether they are cooperative research or small contracts we have started in a number of ways working very closely with small business.

As we continue to grow our acquisition authority we are working with research and engineering to also begin to look at what is our role going to be in science and technology.

Senator MULLIN. Is there some changes we need to be looking at to help you make changes to—for that relationship to build and build to move faster?

Lieutenant General HAUGH. Senator, the most important thing that would be the passing of the fiscal year 2024 appropriations bill

and if we—with the fiscal year 2024 NDAA and the appropriations bill that will give us those authorities. Without that we will operate in our previous model until the budget is passed and then we will have to undo that work and redo it.

Senator MULLIN. What are—what are some changes we need to be making to invest in? When we are looking at the budget and we are looking at appropriating dollars where should we be focusing on to give you the advantages you need?

Lieutenant General HAUGH. Right now, Senator, when we went through the process of enhanced budget control the department did a very good job of evaluating what the services had spent on our cyber mission force and then the department added a significant number over that in the President's budget.

So as we look at the President's budget that is an accurate capture of where we are today that would enable our scaling and our ability to do that. So as we look at the final of the NDAA and the appropriations bill that is—we will be looking for is—are those numbers in the President's budget and based on that we will come back with the department, who has treated us very well through this process.

Senator MULLIN. General, thank you for being here. Ma'am, thank you for, like I said, the support and the family. Thanks for being tolerant and moving as often as you have. Really appreciate your service. Thank you.

Chairman REED. Thank you, Senator Mullin.

Senator Manchin, please?

Senator MANCHIN. Thank you, Senator.

General, thank you again and I—with my fellow senator I feel the same way about the family and the family's commitment and the support you have.

General Haugh, I believe we strengthen our own cybersecurity—and we have talked about that and your experience there working with General Nakasone and continuing on—we are only as strong as our weakest link with our partners around the world—our allied partners.

How do you see them coming to that or lifting up, investing enough, recruiting the right people? Are they able partners? Are they making every effort? Are they working with you looking for our leadership? Or where do you think we have to double down and work harder?

Lieutenant General HAUGH. Senator, this is an area that has really expanded in terms of what both that the geographic combatant commands are asking us to do with partners and those areas that the Department of Defense has asked U.S. Cyber Command to take a leadership role with partners.

And when you think about what that gives us in terms of the ability to scale collectively against common threats we are seeing that. We have a continual increase every year in our cyber flag exercise where partners come together and in a multilateral environment we work on best practices—

Senator MANCHIN. Are they making the same commitment you think as we are? Are there any of them ahead of us that we could be doing better to catch up or are they moving with us in that same timeframe?

Lieutenant General HAUGH. I think they are moving with us. I think there are partners that we are going to work with, particularly with INDOPACOM. Areas that INDOPACOM has asked us to work is a focus—in addition to our long standing partnerships with Japan and South Korea and Taiwan, Australia, they want us to look at other countries like Singapore, Thailand, and also the Philippines. So those are—

Senator MANCHIN. As we talk about—as we talk about retention and recruitment what is the force strength right now—your force strength as far as cyber?

Lieutenant General HAUGH. The overall billet structure of U.S. Cyber Command within our cyber forces is right around 6,000. We hover right around an 85 percent fill rate today. I will not do that math publicly, Senator.

Senator MANCHIN. No problem. Can you fill that void at 15 percent, do you believe, and how do you intend to do that?

Lieutenant General HAUGH. That is a partnership with the services and I think the more we refine what we need from the services and then allow them to be focused on the recruiting and the retention components and allowing us to develop that force with advanced training there is going to be a great opportunity for us to continue to—

Senator MANCHIN. And, finally, I will get to the budget because there is so many—I have talked to so many militaries retired and current off the record, if you will, that have told me that if we got our budget done on time by September 30th, which we never ever do hardly, but if we did that there would be tremendous savings within the military, especially because you have guarantees and certainties, contracts you have. I have been told at least 5 percent savings.

So if you look at—I am just—I will round it off to $880 billion budget we have for military—that is $44 billion of additional spending that you could do within the confines of what you have. Do you think those savings—I mean, by us being able to get a certain budget, not a CR or an omnibus, as the games we have played here for far too long?

Lieutenant General HAUGH. Senator, for U.S. Cyber Command for this year it is particularly acute. If for every day that we operate under fiscal year 2023 rules when the budget is passed we have to back out every single one of those transactions and then execute them under the new rules that will be passed by Congress. So we will be doubling and tripling our work for every transaction for every day we are in a CR.

Senator MANCHIN. I believe so strong in that and we have done—we have not done anything to really reprimand ourselves from not doing our job because all we keep asking for is that we will just give additional money for basic or lack of doing the urgency that needs to be done for the expertise and also for the cost savings. It is just a shame.

So with that, I appreciate it very much. Thank you, Mr. Chairman.

Chairman REED. Thank you, Senator Manchin.

Senator Scott, please?

Senator SCOTT. Sure. Thank you, Chairman. Thank you for being here. Congratulations on your nomination.

Thank you for your service and your sacrifice and the same to your family. Thanks for taking time to meet yesterday. As we know, we got a lot of enemies that are trying to infiltrate our system. One of the things that concerns me and if you could talk about, the DOD has a contract with the Chinese-owned company Tutor.com, and do you have any background of why we would contract with a Chinese company to do training?

Lieutenant General HAUGH. I am not familiar with that company.

Senator SCOTT. Okay. So—

Lieutenant General HAUGH. I can come back for—with you.

Senator SCOTT. You can come back. But just the concept of using a Chinese company to provide any service to our Department of Defense does that make any sense to you?

Lieutenant General HAUGH. Senator, I would look at that really closely from a threat perspective.

Senator SCOTT. Okay. Can you talk about AI and our ability to use AI the right way?

Lieutenant General HAUGH. Yes, Senator. I think we do have a long history of leveraging artificial intelligence, particularly in cybersecurity, and the ability to leverage U.S. industry from that perspective, world leader in terms of how we approach artificial intelligence in cybersecurity. So I think from that perspective is a well-established methodology that we want to continue to grow and expand with the services.

In terms of how we approach that from an—if confirmed how we approach that in the National Security Agency perspective, in my experience a very methodical way to ensure that we understand every piece of data that comes in, know where it came from, under what authority, to be able to ensure analysts touch that data to make an analysis of it, know where it came from and know what authority and ensure that it does not impact the civil liberties of any American.

Senator SCOTT. Do you feel comfortable on AI that any significant decision will still being made by humans, not be made by some system?

Lieutenant General HAUGH. Our methodology in terms of how we approach the things that we will require in U.S. Cyber Command and consistent with the department's standards is a human will be interfacing with that machine and with that data.

Senator SCOTT. We have another significant Presidential election coming up. How do you—and we have watched the past. We have watched outside groups, other countries try to infiltrate our systems to have an impact. Do you feel comfortable that we are in a position that we can stop that?

Lieutenant General HAUGH. Senator, I have been fortunate enough to be part of each of the department's efforts for election defense since 2018, 2020, and 2022, working with Homeland Security and FBI to look at foreign threats to our elections.

And as we look at this election cycle the area that we do have to consider that will be slightly different will be the role of genera-

tive AI as part of this and so our concern is foreign use attempting to be a part of our electoral process.

Senator SCOTT. Right. Earlier this year Communist China used malware to hack critical infrastructure on our bases in Guam. Experts said this is one of the largest known cyber espionage campaigns against the United States.

I am also—I also read an article this week about a typo leak that gave Mali, a country that has grown their relationship with Russia, access to diplomatic documents, tax returns, passwords, and travel details of top officers. So does this concern you and do we have the ability to make sure this does not happen?

Lieutenant General HAUGH. Senator, the most capable competitor that we have in cyberspace is the PRC. They use cyber to gain political, economic, and military advantage.

In the terms of what you describe at Guam, the example of how we are able to be able to identify that threat, how we communicate that threat to enable Defense, put out a joint cybersecurity advisory with the interagency, with our allies and with industry, we have got to continue to scale that and if confirmed that will be one of my focus areas.

Senator SCOTT. How comfortable you are that our space systems that we rely on for—especially for our defense are not going to get hacked, do not have risk that they are going to go down? What do you—what do you think about our ability in space?

Lieutenant General HAUGH. Senator, I will talk about two partnerships that I have been a part of in my previous experience. One is with U.S. Strategic Command and the work between Cyber Command and STRATCOM on NC3 and our nuclear command and control, which has—a critical portion of that is space.

The other is our partnership with U.S. Space Command and the Space Force. The Space Force since stand up has really invested and really been a—has set some models for how to do cybersecurity of weapon systems.

Investing in that area, establishing cybersecurity service providers all the way down to the weapons system level those areas are things we need to continue to grow across the department. But within the space segment that is an area that has been focused on by STRATCOM, Space Command, and Space Force.

Senator SCOTT. Thank you for your service. Congratulations on your nomination.

Chairman REED. Thank you, Senator Scott.

Senator King, please?

Senator KING. Thank you, Mr. Chairman.

General, if you look back at recent history the really disastrous national security breaches have often come from insiders—Robert Hanssen, Aldrich Ames, the most recent one, Edward Snowden.

We will never be able to prevent human beings from occasionally being tempted or compromised or whatever. I am interested in the ability—our ability to develop technical means to prevent or detect exfiltration of classified materials.

Can you talk to me in a nonclassified setting about thinking about that? I mean, clearly, we got to vet people and polygraphs and all of those kinds of things. But it would really have helped

in this prior case if somebody had noticed that materials were being extracted off of—out of a classified server.

Lieutenant General HAUGH. Senator, it is a great question. The protection of our classified information is paramount. It has grave impact to our national security if classified information is disclosed.

So how we approach that and how we think about it is really in two ways. One is personal accountability. How do we ensure that we are hiring the right talent and that we do maintain visibility on that talent, and some of the things that the Director of National Intelligence has done to transition from a periodic reinvestigation of everyone that has access to classified to a continuous evaluation process. That is a step on personal accountability.

From a technical perspective it is about user activity monitoring and our insider threat programs. Those programs exist at various levels throughout the department.

Senator KING. But I would hope in the light of this recent egregious problem that there would be an intensity to reexamine the technical means.

Lieutenant General HAUGH. Yes, Senator, and the Secretary has directed DOD CIO to work with the undersecretary of intelligence security to look at our overall approach to user activity monitoring to ensure that we have an approach that covers our classified network.

Senator KING. Thank you. I want to turn—the cornerstone of our whole defense posture is deterrence. That is the basis of our nuclear posture, also our development of conventional forces. My concern is that in cyberspace deterrence has not been a significant part of our arsenal, if you will. Basically, we do not respond very much.

Now, I think General Nakasone has responded effectively on elections and we saw a diminution of Russian activity in 1918, 2020, and 2022 I think in large part because of that response. But there was a recent incursion attributed to China. I have not seen any response yet.

Talk to me about your role at Cyber Command in deterrence. We are calling it Hunt Forward and various—those kinds of things—but, really, where we are talking about I want the Politburo worried about you when they think about discussing a cyber-attack on the United States.

Lieutenant General HAUGH. Senator, first, I think that both of our pacing adversaries are well aware of the capabilities that we have. The way we approach these problems and we think about integrated deterrence from a cyber perspective and how we partner with the interagency, with our allies, and with industry we think about how first do—how do we generate insights, how do we understand and articulate that threat both inside and with our partners? Second is how do we enable defense, and then third is if called upon we impose costs.

Senator KING. That is the part that I am concerned about. By the way, I misspoke. I do not think the Politburo exists anymore. I think it is just Putin and that probably is one of his problems. But the point is there should be some level of apprehension about a response. Otherwise, they are just going to keep coming after us. We cannot patch our way out of this.

Lieutenant General HAUGH. And, Senator, from our perspective, while not talking about in any specific operations how we approach the—our teammates in the interagency and how that we are able—it could be enabling a sanction. It could be enabling a very targeted demarche that has exposed an adversary activity. It can be public disclosure of those capabilities. Those are cost imposing and—

Senator KING. And I think that is right. I am not suggesting it has to be cyber for cyber, but there has to be some response and I think that is where we have failed in the last several decades there. We have these cyber-attacks. Nothing really happens in response.

One final question. You talked about 702. General officers tend to be very moderate and not deal in hyperbole. But is it possible to overState the catastrophe for national security if 702 is not reauthorized?

Lieutenant General HAUGH. Senator, in my experience, 31 years, it is irreplaceable in terms of our ability to answer critical questions for the Nation for the combatant commanders.

When we see things like the origins of fentanyl in China and its path it takes to the United States informed by 702, counterterrorism actions, the ability to see some of the egregious acts that Russia has done in Ukraine informed by 702, those are just examples at the declassified level of what it provides while also having an extensive set of control measures to ensure that every query, everything that we have done to target a foreign person overseas is done consistent with the oversight of the DOJ, of the court, of the DNI, and anytime anything goes wrong a report to all of the oversight committees.

Senator KING. Mr. Chairman, we would be unilaterally disarming in the face of one of the most serious threats this country has ever faced. Thank you.

Chairman REED. Thank you, Senator King.

Senator Schmitt, please?

Senator SCHMITT. Thank you, Mr. Chairman. Good to see you and appreciate your time in my office with our visit.

Just a couple of questions. One, and I know that AI is a big topic not just here but it has become culturally socialized now. People have a lot of questions and do not know where this is headed and I think that for me sort of dividing this into from a military context and more of the commercial application and that is—we are still trying to figure that out and get a lot of information.

But on the military side, obviously, civilizations have come and gone based on if somebody else gets a better technology and moves ahead militarily. So it is a very important race that we are engaged in.

From your perspective has the Department of Defense done enough to integrate AI into our various platforms?

Lieutenant General HAUGH. Senator, I—

Senator SCHMITT. And I guess what does that look like too is probably the followup.

Lieutenant General HAUGH. Senator, where I really focus on are those areas that are within my responsibility, really looking at how we think about cybersecurity. There are a couple key areas in there that we have done really well in terms of across each of the serv-

ices. The big data platforms that we built for cybersecurity we built them on a common framework.

One of the things that that the—that Congress authorized and the department enabled was also a weapon system inside of U.S. Cyber Command called Unified Platform. That allows us to see that data across the entire department.

So we have got some foundational components in place. I think our next challenge, and we owe you back a study by the fall, is what does that roadmap look like to acceleration and use of these technologies to be able to give us the greatest advantage, give our analysts and our defenders the greatest advantage and allowing us to scale and then doing it in a way that you are very comfortable with.

Senator SCHMITT. And I guess—we have obviously—recently China has hacked our systems and this is not the first time. It is not the last time. But one question is—I guess just want to try to get at do you feel like a layered multi-vendor approach gives us more protection?

I mean, one of the concerns that I have is if you have a single vendor you have less competition. You have less, again, layers of protection. I just want to get your thoughts. I am not trying to—this is not a trick question. I am just trying to get your feeling on this, your thoughts on this.

Lieutenant General HAUGH. So when we look at it, Senator, from a cybersecurity perspective we do have a blended series of vendors that we leverage and from that that allows us to really play to strengths, and when we think about where we are going in the cloud architecture of the department, multiple vendors to be able to leverage their inherent strengths based off mission and I think that inherently how we then grow those partnerships from a cybersecurity perspective is both a strength to us and to those respective companies.

Senator SCHMITT. And do you see your role—I mean, we have talked a lot about—it is really a focus of a lot of my questions in the INDOPACOM. You mentioned this previously and a lot of times when you ask questions this late in the game they get—you sort of ask them again, but that relationship, your resources—you feel like you have the resources to be fully integrated there? Because to me, those are where our biggest threats are from and will be from.

Lieutenant General HAUGH. Senator, the support to Admiral Aquilino—we just completed Cyber Command and INDOPACOM staff talks to ensure of our alignment and how we collaborate to ensure that we from a cyber perspective help them set the theater and that includes our partnerships and aligning to make sure that Cyber Command is helping enable the partnerships that INDOPACOM feels is essential.

There are also some specific capabilities they are asking us for. Those have been authorized and by Congress and by the department and have put us in a position to be able to deliver those capabilities for INDOPACOM.

Senator SCHMITT. You and I had a conversation and, obviously, I expressed to you that—a desire to get some of this divisive politics out of our military and I think we had a very good conversation

about that of best and brightest and merit based and that—where our focus should be and get some of this divisive stuff out.

Also, I do want to mention that you do not have to comment on this because this is not related to you specifically but there are some in the intelligence community, I think, that have viewed their role as determining what people can hear and see and think.

CISA specifically has engaged in part of a censorship enterprise working with big tech to shut down speech, and I do not actually think that is debatable anymore. It is—those are the facts.

And so I would just—a word of caution to be very aware of that. Obviously, you are dealing with real threats. But I think the First Amendment is very important.

If we are who we say we are and we believe in this robust marketplace of speech people should be able to have opinions even if they are ones that you do not agree with and I do not think the government or the Intelligence Committee's role is to decide those things. Let the American people decide that.

So that is just something, I think, for you to keep your eye on is some people view their role as the decider of who gets to hear what and I think that is the wrong approach. Thank you for your time.

Chairman REED. Thank you, Senator Schmitt.

Senator Kaine?

Senator KAINE. Thank you, Mr. Chair.

General Haugh, congratulations to you. I want to followup on two points that were raised by my colleague Senator Manchin, budgets and allies.

So on budgets, maybe particular with some colleagues here, we could get rid of the most commonly occurring CRs immediately if we would switch the Federal budget year from October 1 to January 1.

If you look at when we actually get appropriations deals done over the last 30 years we never get them done by September 30. We almost always get them done in December. Why is that?

It is because our leaders basically at the end of the year when people want to go spend time with their family say we are not going home until we get appropriations bills done.

Now, every once in a while we go into the following year but usually we are getting them done right when we leave. If we switched the Federal fiscal year to a January 1-December 31 fiscal year that pressure would still be on us. I do not think we would say, well, let us do it at the end of March. I think the leadership would still force us to do it.

This has become such a norm here that even in the debt ceiling deal that we just did we imposed a set of punishments on ourselves if we did not get the deal done by December 31.

We all know that that is the real time now and I just think we could eliminate an awful lot of the CR concern that Senator Manchin raised if we would just analyze and then be honest about what is the real budget calendar up here.

A friend of mine who is a landscape architect said if you are doing the landscape do not put down the sidewalks. Do the landscape, then see where people walk, and they will make a path and then build the sidewalks there.

We are showing where the path is to budgets and getting rid of CRs. So I will just tell my colleagues on September 30 this year I am going to introduce a bill to change the budget year to a calendar year and if it turns out that we get approps deals done by September 30 I will admit that I am wrong.

But I am not going to be wrong and I am going to introduce that bill and I would love anybody else joining me in it. I am on the Budget Committee. I would like to convince them to do that budget process change.

General Haugh, Senator Manchin asked you about alliances and I want to ask about a particular one. The NDAA that we are debating now on the floor will include provisions regarding the AUKUS framework.

So this is a framework that has two pillars. Pillar one deals with submarine technology, the working with the Australians to buildup a nuclear submarine industrial base in the 2030's that would involve some transfer of U.S. subs should we be able to kind of figure out the details right. In the 2040's the Australians would have their own submarine production capacity.

But there is also pillar two of the AUKUS deal which focuses upon cooperation with the U.K. and Australia on cyber, artificial intelligence, hypersonics, other advanced technologies.

You talked generally about the work that we do in the cyberspace with allies. Recognizing we are in an unclassified setting let us focus a little bit more on what you might see as upside opportunities in this framework with Australia and the U.K.

Lieutenant General HAUGH. Senator, in terms of our partners in the Indo-Pacific, Australia and New Zealand are clearly—have been long-standing allies.

Senator KAINE. Two of the Five Eyes nations so we have huge equities with them.

Lieutenant General HAUGH. And then, of course, the U.K. and how we think about Europe and those partners. Our partnership with both Australia and the U.K., both bilaterally and multilaterally, AUKUS presents another opportunity and it presents us an opportunity to do that through the lens of the threat of the People's Republic of China.

So from a pillar two perspective opportunity for us to really think our way through how best as all three nations and all three militaries to think about those technologies.

Senator KAINE. Great. Thank you. I noticed you are a Russian major—Russian studies major—and I wonder in the cyber field I would think that language fluency would be a big component of trying to build out a good workforce and you would be sensitive to that from that background and I know within military speak this is often called the LREC—Language, Regional Expertise, and Culture—as a kind of a strategic advantage for folks.

How are you doing within Cyber Command in terms of building out a workforce that has language capacities to enable us to be at our best?

Lieutenant General HAUGH. Senator, we have done—we have done well. Inside each one of our teams we do have language capability. Different services have approached it through different ways

and how they have grown that whether through their cryptologic community or additional training.

It is absolutely an incredibly important part of our force and as we think about what our balance is, if confirmed, that will also be the area that I look at in terms of the balance of which languages based off the threats we face today.

Senator KAINE. Thank you for your testimony. I yield back.

Chairman REED. Thank you, Senator Kaine.

Senator Ernst, please?

Senator ERNST. Thank you, Mr. Chairman, and thank you, General Haugh. It is good to see you and I want to thank your family as well for joining you today. We appreciate their support.

General, I have heard from Special Operations leaders that they are making significant investments in what they are calling their Cyber Special Operations Forces and Space Triad, kind of that that grouping there, and what is your view of this new operating concept for strategic competition and conflict? What does that look like to you?

Lieutenant General HAUGH. Senator, starting with the partnership with Special Operations Command, we are—and when you look at Special Operations Command, U.S. Space Command, and U.S. Cyber Command, really have global focus in terms of how we approach the support with the other combatant commands.

Each of us bring really strategic competitive advantages and from a cyberspace perspective, our unique authorities and our global presence with Special Operations Command physical presence with each of the combatant commands and it offers us an opportunity to look at where each of us can come together to work in support of a geographic combatant commander's needs and be able to do that more effectively together.

Personal experience for me as the component to EUCOM every day we were working with Special Operations Command Europe to be able to look at how could we together do what the EUCOM commander needed. We have an embedded staff with Special Operations Command and their components. It is our Marine component within U.S. Cyber Command, MARFORCYBER, that leads that effort for Cyber Command.

Senator ERNST. Yes. I think that is incredibly important to explain how all of these commands work together cohesively. You explained the physical presence of those SOCOM operators. Can you also explain how that ties in with Space Force then as well?

Lieutenant General HAUGH. So, Senator, when we think about what those challenges are and we think about the resiliency that is going to be required, as we think about what potential future conflict could look like how do we—how do we ensure both a redundant set of communications? Much of that is going to be built on space.

So the partnership between Cyber Command and Space Command and the Space Force is really inextricable in terms of how we think about the support to the joint force.

With Special Operations Command we also want to ensure that they are well defended from a cyberspace perspective, that we have a responsibility to ensure that we are collaborating, we understand

those unique communications needs, and how we defend individual SOCOM activities is also a core thing we are thinking about.

Senator ERNST. Wonderful. Well, and I appreciate the time that you took the other day in my office to explain this concept to me and I know how appreciative SOCOM is as well.

And how do you do foresee this? With Cyber Command and SOCOM working together how do you see that you will be able to help each other fulfill your traditional missions more efficiently?

Lieutenant General HAUGH. In the way that we approach it right now, Senator, we are looking for what is those hard requirements that a geographic combatant commander needs and those are the areas that we are focused on. How do we work together to achieve something that would have been more difficult independently?

But when we partner with unique strengths of Special Operations Command and SOCOM components with what our cyber mission force brings that capacity tied together, our goal is to satisfy hard problems for the geographic combatant commands.

Senator ERNST. Really appreciate that because as we have gone and seen in this Committee the constraints that we will be under with the budget, moving forward, we need to make sure that we are able to operate efficiently and all of you working together rather than in individual silos is just much better for us as decision-makers and much better for the mission as well.

So I just want for the other members on the—on the Committee is just to once again reiterate how important it is that we have all of our commands working together. I am glad that you have that relationship.

You mentioned General Fenton the other day, our Special Operations Command commander, and the relationships that have been built there. You also mentioned General Kurilla and others that Cyber Command will continue to work with around the globe. So really appreciate that.

How important just from your perspective—I am saying it but from your perspective how important it is that Cyber Command remain tied in with all of these other combatant commanders and the relationships there?

Lieutenant General HAUGH. Senator, when you look at the three missions that have been assigned to U.S. Cyber Command to defend the Department's network that really is in support of all the combatant commands and their ability to execute, our ability to defend the Nation and the other combatant commands from adversary hacking and then the third very specified mission is to deliver offensive and defensive capabilities in support of the other combatant commands.

Senator ERNST. Very glad to have you being nominated into this position, General Haugh, and once again, thanks to your family as well for being here. Thank you, Mr. Chair.

Chairman REED. Thank you, Senator Ernst.

Senator Peters, please?

Senator PETERS. Thank you, Mr. Chairman. General, good to see you again. Enjoyed our conversation in the office earlier.

As you know, I chair the Homeland Security and Government Affairs Committee in addition to being a member of this Committee and so I am concerned that our military installations here at home

in the homeland may be vulnerable to attacks by adversaries seeking to disrupt or even prevent normal operations and the movement of forces within the United States.

These adversaries may seek to exploit base resilience on infrastructure in the surrounding communities that help to sustain just everyday base functions. So given the interdependency between critical civilian infrastructure, military installations, and local civilian communities how would you envision CYBERCOM's role compared to the DHS role to identify, to defend, and report cyber threats posed to DOD installations and their surrounding communities, particularly those installations who are charged with deploying combat capabilities abroad are essential to national security?

Lieutenant General HAUGH. Senator, it is a great question and to start with Cybersecurity and Infrastructure Agency is a great teammate and collaborator with U.S. Cyber Command. Major concepts that we are thinking about and what we have really learned through our partnership with European Command, U.S. Strategic Command, and U.S. TRANSCOM as it relates to Ukraine, two concepts of set the theater, how do we help EUCOM ensure their networks are secure and they have resilient communications, and then set the globe because in reality anytime that the Department of Defense is operating it really is a global set of connectivity that begins in the United States.

So when we think about generating force from TRANSCOM, when we think about our nuclear command control, that is inherently a partnership that rests on the infrastructure of the United States.

Areas that in my experience—I have worked incredibly close with CISA as part of the original lead for the cyber—for the election defense activities that we conducted in U.S. Cyber Command NSA in support of Homeland Security. That was one of my first functions in U.S. Cyber Command and have now been part of that for 3 years.

One of the areas the department is investing in we currently have a strong liaison presence with DHS and they with us. The department is going to expand that to allow us to have liaisons with each sector that CISA is responsible for. So I see this partnership only growing.

Senator PETERS. Right. Are there best practices that you would recommend to streamline and optimize the collaboration between CYBERCOM and DHS, CISA in particular? Lieutenant General HAUGH. So I think, Senator, the area that we can contribute with our—with our OSD colleagues and our other combatant commands is to articulate what infrastructure is important to the department.

So we owe that to ensure that and we do that well today. But that will continue to change. As technology changes, as our demands on industry change, and as our infrastructure changes we have to ensure that there is a really clear understanding with not only our teammates in DHS but if there is a different sector agency that is responsible, but the infrastructure that CISA has to be able to work with individual sectors, how their ISACs do information sharing, those are inherent strengths for the Nation and those are areas that we should be really good partners.

Senator PETERS. Right. I recently returned from a trip to the Western Balkans where I heard from our Albanian allies about the devastating Iranian cyber-attacks against their country and it certainly—these types of attacks by both nation State and nonState actors are going on frequently and in severity against our allies.

I certainly want to applaud the actions of our embassy in Tehran along with support provided by the FBI, Microsoft, EUCOM, CYBERCOM, and others that responded very swiftly and professionally when requested by the Albanian government.

Given that, unfortunately, those threats are only going to increase in this space and they are likely to be the target of increased attacks from the Iranians.

So my question for you is what actions should CYBERCOM and interagencies be taking now to better help partners and allies proactively defend against this threat.

And then the second part of the question is how can we provide more robust medium to long-term cyber recovery relief with U.S. private sector support to help these countries rebuild their cyber infrastructure just as we would help a country recover from a natural disaster?

Lieutenant General HAUGH. Senator, first, in terms of Albania, I too have met with Albanian leadership and we—as part of the team that has responded based off of guidance from the department and then with our interagency teammates to ensure that they—we can get their networks back up and operating in concert also with their State partner to be able to make them more resilient.

It is an example, I think, from our perspective of how do we share information. So how do we share information on terms of threats with our allies and with industry in a way that makes everyone more resilient and that is an area that from the Albanian perspective is a good example of areas that we can contribute.

Senator PETERS. Great. Thank you, General. Thank you, Mr. Chairman.

Chairman REED. Thanks very much, Senator Peters. Before I recognize Senator Budd I will formally turn over the chairmanship temporarily to Senator King. I have to go to the Appropriations Committee.

Senator Budd, you are recognized.

Senator BUDD. Thank you, Chairman.

General, thanks for being here this morning. Again, thanks for your family. I enjoyed our conversation last week. So it is good to see you again.

So I want to focus on AI. I know there has been lots of questions this morning and also I want to talk about advanced computing.

So do you believe that the United States currently holds an advantage in AI technologies?

Lieutenant General HAUGH. Senator, I do.

Senator BUDD. So one of the challenges faced by CYBERCOM and NSA is recruiting and retaining talent and a lot of the focus has been on cyber operators. We talked about that.

But we also need analysts with both computer science backgrounds and also language skills. So can AI that uses large language models to interpret and analyze audio text or—excuse me,

audio or text can that replace the need for analysts or is that just a—is AI tooled to more empower workers and how should we be thinking about that?

Lieutenant General HAUGH. Senator, from our perspective it would be an enabler for an analyst to look at the most important data that would answer a foreign intelligence question or enable our planning. So it would be an enabler, not a replacement.

Senator BUDD. Thank you. So I want to talk about the cyber threat posed by China. We learned this week that China hacked the secretary—excuse me, the Secretary of Commerce Raimondo and the State Department in advance of bilateral talks.

So when we spoke last week you mentioned that probably the most pressing challenge is China's advanced efforts to steal American intellectual property. So could you please further elaborate on that threat and why it matters? And if confirmed, what do you believe your role is to inform the public on and to respond to those attacks?

Lieutenant General HAUGH. Senator, the PRC has done a sustained campaign over decades to steal intellectual property and it really is intended to enable their economy to be able to—to create economic advantage and also to buy down the military advantage that the United States has.

It has been persistent, it has been continuous, and it will continue. From our perspective, it is our job both as Cyber Command and NSA to be a part of the team that exposes that threat. Today if you go to the National Security Agency website you will see a series of reports that lay out in detail how China hackers operate and what that looks like.

That is intended to very clearly pass out to not just our allies but to our industry leaders how China operates and how they can defend. So we should be being as transparent as we can, we should be collaborating with industry wherever we can, and working with our interagency teammates to ensure wherever they have responsibility that we are clearly articulating the threat and we are thinking about this from a common defense perspective. Senator BUDD. I appreciate you making that publicly available and I hope, if confirmed, that you will make that even—if you will promote that I think that would be helpful. So you also explained that China focused its AI on expanding information control. We talked a little bit about that this morning. So what is CYBERCOM's role in supporting the interagency to defeat information control and how confident are you in your ability to accomplish that task?

Lieutenant General HAUGH. So, Senator, I think when we are thinking about that, first and foremost, is we drive—what activities we work are really aligned against what the other combatant commanders need. So when we are thinking from a Cyber Command perspective we are aligning what are the capabilities we need will be driven by those combatant commanders.

From a National Security Agency perspective, if confirmed in that role it is really NSA's job to identify the threat and to be able to communicate that threat across our interagency to then be able to determine what is the best approach if that technology is being proliferated.

Senator BUDD. Thank you. So how is CYBERCOM leveraging commercial partnerships to combat threats and maintain our competitive advantage and are there ways to do that better?

Lieutenant General HAUGH. Senator, I think right now we do have collaborative relationships with industry and particularly with small business. That is really where the department focused us initially.

Now as we gain our budget control and our acquisition authority that will allow us to expand how we interact with industry and certainly be able to bring much more resource. That will enable us with—to operate with more speed and agility aligned with our requirements and we are excited about that opportunity.

Senator BUDD. Thank you, General. I wish you luck.

Lieutenant General HAUGH. Thank you, Senator.

Senator KING. [Presiding.] On behalf of the chair, Senator Rosen?

Senator ROSEN. Well, thank you, Senator King. Appreciate the hearing and, General Haugh, we had such a lovely conversation. I know everyone is saying that.

I really appreciate what we chatted about and I so appreciate the family that moves and moves and moves along with you and does all the hard work to be sure that you can be happy at home and productive in your work. So thank you.

I want to talk a little bit about—my colleagues have been talking about all these things, AI, everything else. But in order to achieve our goals, all of these goals that everyone has talked about, we have to have the workforce. So even with AI that Senator Budd talked about you really need a person to make that final important decision that takes all the data, puts it down, and gives it to someone.

And so in March the DOD released its cyber workforce strategy to address the gaps in workforce management to ensure we are equipped to address the growing cyber threats from our adversaries.

So we discussed in our meeting just this week my Civilians Cybersecurity Reserve Act, which would provide the Department of Defense with qualified civilian personnel in our greatest time of need.

It was included in this year's pilot program and this year Senate NDAA. So what is your view, as we spoke about the nontraditional reserve models such as establishing a civilian cybersecurity reserve to support DOD's cyberspace operation, the kind of talent and maybe that it needs and the depth of experience that it needs?

Lieutenant General HAUGH. Senator Rosen, I think if confirmed one of the roles that I have the opportunity—would have the opportunity to do is really be an advocate for STEM [science, technology, engineering and mathematics education.

When we think about the National Security Agency and the need that NSA has in terms of a very technical workforce the work that we can also be advocating for with the services to make sure the service are able to recruit the right talent and that really starts with being able to tap all the talent in the United States.

So, if confirmed, I would really look forward to working with the department, work with your team as we think about what is the

right type of pilot that would allow us to really think through how we could leverage a broader portion of our population.

Senator ROSEN. Thank you. I look forward to working on that with you, and I think as we think about our workforce and our reserve force and that partnership we have to think about our international cyber partnerships, right.

And so the National Cybersecurity Strategy, well, it does rightly identify that strengthening our international partnerships it is—that capacity is really a pillar of our collective cybersecurity. We do not do it alone. The threats come from everywhere and we have to be—we are stronger together when we can share information.

So our Hunt Forward operations in Ukraine have demonstrated really the true value of these international partnerships that are critical to identifying and stopping malicious cyber activity before it threatens our critical infrastructure and our key resources.

And so the Nevada National Guard has three partner nations as part of the State Partnership Program—Fiji, Tonga, and Samoa. So, if confirmed, how would you leverage the State Partnership Program to bolster cyber partnerships with our allies and partners?

Lieutenant General HAUGH. Senator, in one of my—one of my first Cyber Command jobs when we when—we went to operate with one of our partners we found a State Partner Program already there.

So we know that they are already there. They have long-standing relationships. We ought to leverage that and we also want to make sure that if there are some of the states that are trying to build a cyber partnership how do we help them do that.

How do we ensure they have the right threat information? How do they? We want to leverage the State Partnership Program. It has been a huge effort for us.

As the department in the new Cybersecurity Strategy articulates the next area of priority in terms of mission is our partners and allies and so that is clearly an area that, if confirmed, will be a priority for me.

Senator ROSEN. Well, fantastic. And I want to—I want to build a little bit on what Senator Budd was talking about.

China and others have talked about this and Chinese cyber aggression, particularly on Taiwan and its impact and potential threat to us as we see that acutely aware that China poses a threat in the cyber domain and it is using Taiwan as a testing ground for its cyber capabilities and recent cyber-attacks have forced Taiwan to harden their defense. What we learn there can save us here.

So China is closely monitoring the outcome of Russia's invasion on Ukraine to apply the lessons possibly learned to a potential invasion of Taiwan and so that is why this Congress with Senator Rounds and Congressman Gallagher, bipartisan legislation that we introduced to expand American military cybersecurity cooperation with Taiwan. And so this legislation has been included in both the House and Senate versions of the NDAA for fiscal year 2024.

So, if confirmed, how would you work to expand military to military cybersecurity cooperation with Taiwan to strengthen their deterrent capabilities and raise the cost of escalation for China?

Lieutenant General HAUGH. Senator, U.S. Cyber Command currently has a partnership with Taiwan. We will work with INDOPACOM and ensure that that remains strong.

Senator ROSEN. Thank you so much. Thank you, Mr. Chair. Senator KING. On behalf of the chairman, Senator Rounds?

Senator ROUNDS. Thank you, Mr. Chairman.

General Haugh, first of all, you are getting a lot of practice at this because you are responsible not just in this Committee but also within intel in the dual hatted role that you play.

I want to thank you for your service to our country as well as your family. You have heard that from a number of folks up here and we really do recognize that there is a challenge for the family because you do move regularly and we understand that that it is not something that a lot of folks across our country probably understand is part of the mission that you have. So thank you for that sacrifice for you and the family.

I have followed up in each of our hearings this year and asked each of the individuals coming before us in command positions the following. It has to do with I believe that we have a very serious issue with regard to spectrum and specifically with regard to the proposed sale by some Members of Congress, suggesting that we should sell portions of the spectrum in the area of 3.1 to 3.45 gigahertz, and this is an area in which we have significant defensive capabilities and that we utilize today.

Based on your knowledge of this issue, if there is a report, which is due out in September—if that report demonstrates that auctioning off this 3.1 to 3.45 gigahertz portion of the spectrum will adversely impact our national security what would be your advice to the President and Congress?

Lieutenant General HAUGH. Senator, I am following the ongoing study. If that comes back as high risk I would recommend not to share.

Senator ROUNDS. Thank you. There seems to be—someone somehow has continued to push this narrative that this portion of the spectrum should be sold for commercial purposes.

In your professional military opinion do you believe it is possible that our adversaries may very well be attempting to influence this debate and push the sale of the spectrum that is vital to our national security?

Lieutenant General HAUGH. Senator, in my current role I have not seen indications that that is occurring. I would expect that that is a drumbeat in standards bodies and things along that line from—in terms of trying to influence areas that would disadvantage the United States and advantage China.

Senator ROUNDS. And in this particular case that would disadvantage this country?

Lieutenant General HAUGH. Yes, Senator.

Senator ROUNDS. Thank you. Let me move on to another area that—this Committee was successful in including the provision within the Senate's version of the NDAA, which would authorize the Department of Defense to conduct cyber operations against transnational criminal organizations including the cartels.

How would you use these increased authorities to enhance the whole of government approach to combating transnational criminal organizations?

Lieutenant General HAUGH. Senator, if we—if there were authorities assigned to U.S. Cyber Command both in the law and by the department our first stop is always the supported commander and in this case we would have conversations with the U.S. Northern Command commander about priorities and where we would fit into an overall strategy that would really be interagency approach and support to what U.S. Northern Command needs.

Senator ROUNDS. Clearly, you could bring capabilities to the fight?

Lieutenant General HAUGH. Yes, Senator.

Senator ROUNDS. Thank you. We are also undergoing the largest overhaul of our nuclear triad in decades and we are doing so against the specter of two nuclear near peer rivals.

All elements of our nuclear deterrent including our command and control systems are being modernized. The cybersecurity of our NC3 systems must be a top priority.

In the current and projected threat environment what do you see as the biggest challenges for nuclear command and control from a cyber perspective? And I ask that recognizing that we are in an unclassified environment.

Lieutenant General HAUGH. Senator, I think from our perspective this is—our partnership with Strategic Command is focused on ensuring the resiliency and health of our NC3 enterprise and so from a Cyber Command perspective both today and if confirmed we have got a strong relationship with STRATCOM.

We just held a collaborative conference that brought in the services, brought in all of our partners to work—to ensure that we are providing the best threat intelligence and also thinking our way through the architecture as they advance to ensure they are doing it in a way that we would recommend from a cybersecurity perspective.

The role that Congress has done to give the U.S. Strategic Command the responsibility for the overall NC3 enterprise has also allowed us to really focus on the priorities that come from General Cotton and we are closely aligned with him and will continue to do so if confirmed.

Senator ROUNDS. Thank you. And, General, I do look forward to supporting your nomination. Thank you.

Thank you, Mr. Chairman.

Senator KING. On behalf of the chairman, Senator Fischer?

Senator FISCHER. Thank you, Senator King.

Thank you, General, for being here today and my thanks to your family for the support they offer you but also for the sacrifices that they make for this country as well. So thank you, sir.

I would like to just followup a little bit with my colleague questioning you on NC3. I understand the relationship you have with STRATCOM, with General Cotton. I am very pleased to hear about your work in establishing that architecture.

But can you tell us where you believe we are in the process there and in this setting what has been done, what still needs to be done, and if you think the timeline we are currently on is appropriate?

Lieutenant General HAUGH. Senator, what I can speak to is in terms to how STRATCOM has really approached ensuring they have visibility of the NC3 enterprise, how they have aligned their components to ensure that they are focused on the cybersecurity of the enterprise, and then the clear requirements that STRATCOM has given to U.S. Cyber Command and our components to ensure that it is secure.

In terms of the investment strategy I would defer that to General Cotton.

Senator FISCHER. Okay, thank you.

I appreciated our discussion earlier this week on CYBERCOM and NSA's efforts to share more information with the public especially about network vulnerabilities.

As I told you in our conversation, I think that the more the American people have a fuller understanding of the threats we face I know that they would be very, very supportive of the actions we need to take to make sure this country is safe.

In this setting can you speak to the value of those types of advisories on known cybersecurity threats and how they can be better leveraged to protect nongovernment—governmental assets?

Lieutenant General HAUGH. Senator, I think this is an area that from an NSA and a Cyber Command perspective the ability to share information that allows both our companies to be more resilient, so a complete understanding of what the threat environment looks like at an unclassified level, makes everything go more quickly so we can move with speed.

In terms of sharing what those threats look like, we would want every American to be able to understand what is the threat, particularly if we are thinking about ransomware or in the future what threats come from generative AI and how would that enable a hacker.

Those are conversations that we should be having very routinely both in how we communicate and in the documents that we put out but also in how we engage the U.S. population.

Senator FISCHER. You not only protect the Department of Defense, our national security, the assets that we have, but also what is your relationship to private companies that have critical infrastructure, for example, transmission lines, our ports, our airports, nuclear power facilities? Can you just on a high level tell us what your relationship is there and your feelings about it, how secure it is?

Lieutenant General HAUGH. Senator, from our perspective and U.S. Cyber Command and the National Security Agency the Department of Defense is the sector specific lead for the Defense Industrial Base.

So in terms of a series of direct sharing relationships with that segment our close partnership with CISA in terms of the Cybersecurity and Infrastructure Agency as they are—as they lead and in this case for those type of activities with the Department of Energy they are our partners and we want to ensure that both to CISA and the DOE they are getting the best threat information to allow them to ensure the sector leads across the sector councils within Energy are getting that data.

I have seen that. I have been a part of that activity in the past. Our ability, if confirmed, to sustain that and expand it that will be an area that will be a priority.

Senator FISCHER. When we go outside of the United States it is important that we collaborate with our allies as well and have our partners in a cyber domain.

It is important in this country. It is important with other governments as well. How do you believe that you will be able to increase that collaboration?

Lieutenant General HAUGH. In terms of our partners today we have a really good set of international partnerships and as U.S. Cyber Command continues to grow, if confirmed, how we apply our budget that allows us to also look at how we expand those foreign partnerships is an area that we will certainly consider.

Senator FISCHER. Thank you, sir. Thank you, Mr. Chair.

Senator KING. On behalf of the chair, Senator Warren?

Senator WARREN. Thank you, Mr. Chairman.

Our Nation's adversaries use crypto to evade sanctions and to fund their weapons programs, spying, and cyber-attacks. Now, dirty crypto transactions are often hidden but here is the part we know for sure. In 2022 cyber criminals aligned with rogue nations received over $8 billion in crypto payments in violation of U.S. sanctions.

Top of the list in its love for crypto is North Korea. Last year North Korea stole a record-breaking $1.7 billion in crypto, about two-thirds of which was stolen from crypto's so-called decentralized finance, or defi, space which allows actors to bypass traditional regulated financial intermediaries to move funds around.

Over the past 5 years North Korean hackers have stolen, that we know of, more than $3 billion in crypto. So where does that money go? Straight into North Korea's illegal nuclear program.

General Haugh, as deputy commander of U.S. Cyber Command you have seen the scale of North Korea's campaign to pay for its nuclear program with stolen laundered crypto. Do you know how much of North Korea's missile program has been funded by the spoils of crypto crime and cyber-attacks?

Lieutenant General HAUGH. Senator, I do not have a specific number but I do know that from a nation State, a ransomware actor, and DPRK both in their cryptocurrency theft and how they enable IT workers to gain funds it is an enabler for both the hackers and from a nation State and ransomware perspective and it is certainly an enabler for the DPRK to raise funds focused on their military program.

Senator WARREN. Okay. And I think the best estimates are about half of their nuclear program is paid for with stolen crypto funds. Would that number surprise you?

Lieutenant General HAUGH. It would not, Senator.

Senator WARREN. All right. So according to a recent Wall Street Journal report, since 2018 when North Korea began ramping up its large-scale crypto attacks its missile launch attempts and successes have, quote, "mushroomed."

In other words, that money has been valuable to advance what they want to do. Cyber Command, the agency that you are nominated to lead, has played a critical role in helping law enforcement

agencies track and seize crypto wallets used by North Korean hackers to steal millions of dollars in crypto and to launder that money through Chinese crypto networks.

From your experience, General Haugh, when North Korea steals billions of dollars worth of crypto and uses Chinese money laundering networks and pours that money into its nuclear programs does that pose a threat to our national security?

Lieutenant General HAUGH. It does, Senator.

Senator WARREN. So I really appreciate your forthright comments here. As you know, North Korea is not the only issue. Russian ransomware gangs, Chinese fentanyl manufacturers, transnational drug cartels, and others are using crypto to exploit the loopholes in our Nation's anti-money laundering network.

General Haugh, the Treasury Department recently recommended that the government strengthen our Nation's anti-money laundering and countering the financing of terrorism rules by, quote, "closing any identified gaps in the Bank Secrecy Act to the extent that they allow certain DeFi services to fall outside the scope of the BSA's definition of financial institutions."

So let me ask you, do you agree that we need to stitch the loopholes that allow the DPRK and other dangerous actors to use crypto to fill their coffers?

Lieutenant General HAUGH. Senator, I am not—I am not really aware of that specific recommendation. We would—that is certainly an area that we are focused on from a threat perspective and would love to be able to work with you on what is the way that we can limit adversary hackers that threaten the United States through every means.

Senator WARREN. All right. Senator Roger Marshall and I are reintroducing our crypto anti-money laundering legislation to close the gaps that let these bad actors skirt our country's laws and threaten our national security.

Congress cannot continue to sleep while North Korea and China and Russia are using crypto to threaten America's national security. So I want to close—I know I am out of time. I just want to say one word, if I can, with your indulgence, about the impact of the senator from Alabama's holds on our senior military nominees.

These officers have served our country honorably for decades and they do not deserve to be treated like a political football. I very much hope that the hold will be lifted so that we can move forward on these nominations.

Thank you, Mr. Chairman.

Senator KING. Thank you, sir. On behalf of the chairman, Senator Gillibrand?

Senator GILLIBRAND. Thank you very much, Mr. Chairman.

As you know, the vulnerabilities, equities, policy, and process establish how the government balances equities and makes determinations regarding the disclosure or retention of newly discovered zero day vulnerabilities.

As we saw in recent reporting about PRC compromise of critical infrastructure in Guam the PRC is looking to hold our critical infrastructure at risk in the event of a crisis between our countries.

How will this increased threat to U.S. infrastructure inform your thinking regarding retention versus disclosure of identified vulnerabilities?

Lieutenant General HAUGH. Senator, in my experience I have worked as part of the vet process. It is effective at ensuring that that there is a really good balance, and if I look at how we approach this in a transparent way we publish what that looks like as the U.S. Government and then counterbalance that with the law that China has passed and how they are thinking and mandating each company having to turn over every vulnerability directly to the People's Republic of China and their cyber actors. Certainly, we are taking a very transparent balanced approach versus an information control approach.

Senator GILLIBRAND. You recently commanded the 16th Air Force, which executes the Air Force's cyber missions. The 16th Air Force has entered into a range of cooperative research and development agreements with public and private entities to advance its cyber missions.

As the commander what do these agreements offer you and how do they advance our Nation's cybersecurity?

Lieutenant General HAUGH. Senator, the cooperative nature of them really help both sides of each of those partnerships. An example of those we really looked in particular at things that would have been threats to our bases, in particular the electrical systems that were on our bases.

So allowing us to do cooperative research within academia and with industry to be able to think about those threats internally as they also then apply that research to be a part of our Nation's response.

Senator GILLIBRAND. Section 1502 of the fiscal year 2023 NDAA requires an annual report on the support Cyber Command receives from the military services. We have had several hearings on this to see which services are providing personnel, which ones are having challenges.

Will you commit to being direct and candid with Congress in your 1502 reports and working to ensure that those are submitted on time each year and will you make recommendations to this Committee about how to make sure you have the complement of cyber warriors that you need to complete your missions?

Lieutenant General HAUGH. Yes, Senator.

Senator GILLIBRAND. Thank you. Thank you, Mr. Chairman.

Senator KING. Thank you, Senator. On behalf of the chair before I close the Committee session, General, I want to thank you again for your service.

Thank you to your family, which has been very much appreciated and observed today. Your answers have been impressive, thoughtful, and forthright and I think it speaks very well for your continued or your prospective stewardship of these two important agencies.

I also hope that you will convey my deep regard and respect to your predecessor, General Nakasone, who I believe is one of the most capable public servants I have ever worked with.

I think the work that he did subsequent to the 2016 election, in 2018, and 2020 was leadership at its best—creative leadership at

its best and I hope you will convey that thought to General Nakasone and to Susan.

Thank you again for your testimony today. Thank you for your willingness to serve and we look forward to working with you in these incredibly important and dangerous times that we can turn to our advantage, given the skills of yourself and the great people that you will be leading. Thank you.

Lieutenant General HAUGH. Thank you, Senator.

Senator KING. The hearing is adjourned.

[Whereupon, at 10:44 a.m., the Committee adjourned.]

[Prepared questions submitted to Lieutenant General Timothy D. Haugh, USAF by Chairman Reed prior to the hearing with answers supplied follow:]

DUTIES AND QUALIFICATIONS

Question. What is your understanding of the duties and functions of the Commander, U.S. Cyber Command?

Answer. The Commander, USCYBERCOM, is responsible for the planning of cyberspace missions; serving as the cyberspace operations joint force provider; and joint force trainer, as specified in the Unified Command Plan and 10 U.S.C. § 167b. In coordination with mission partners, USCYBERCOM: directs Department of Defense information network (DoDIN) operations; secures and defends the DODIN; maintains freedom of maneuver in cyberspace; executes full-spectrum military cyberspace operations; provides shared situational awareness of cyberspace operations, including indications and warning; integrates and synchronizes cyberspace operations with other Combatant Commands and other appropriate U.S. Government Agencies tasked with defending our Nation's interests in cyberspace; and supports civil authorities and international partners. These efforts support DOD's overall mission in cyberspace of defending the Nation, supporting the Combatant Commands, and defending Department of Defense (DoD) networks.

Question. What is your understanding of the duties and functions of the Director of the National Security Agency/Chief of the Central Security Service?

Answer. Under the authority, direction, and control of the Under Secretary of Defense for Intelligence & Security (USD (I&S)) and the Director of National Intelligence (DNI), the Director of the National Security Agency (NSA) is responsible for ensuring the NSA successfully conducts two missions: signals intelligence (SIGINT), and cybersecurity. The SIGINT mission provides America's leaders with critical foreign intelligence to defend our country, save lives, and advance U.S. goals and interests. The cybersecurity mission prevents and eradicates threats to U.S. national security systems with a focus on the Defense Industrial Base, and the U.S. Military's weapon systems. NSA's SIGINT and cybersecurity missions are also critical to fulfillment of NSA's combat support responsibilities.

Question. What background and experience do you possess that qualify you to perform these duties?

Answer. I am a career intelligence officer who has served 31 years in intelligence positions in the Air Force, the Joint Force, and the Intelligence Community (IC). I have commanded intelligence units at the Squadron, Wing, and Numbered Air Force level, and served as a Senior Intelligence Officer in special operations, a combatant command, and Air Force intelligence units in garrison and deployed. Trained as a Signals Intelligence officer, I have served in many operational assignments within the joint and Air Force cyber force, and in intelligence assignments within the NSA and the Air Force's cryptologic component. In my cyber assignments, I have commanded units within the Air Force and Joint Force responsible for executing all of USCYBERCOM's assigned missions. I have also been part of combined operations with NSA that allowed me to partner with or support NSA's Cybersecurity and SIGINT missions. I have been honored to serve with the military cyber forces and the NSA for most of my career, and have a deep appreciation for the talented professionals who execute both organizations' important missions in service of the Nation.

Question. What qualifications do you have to command military forces and military operations?

Answer. Over the past 31 years, I have served in leadership positions across the Air Force, the Joint Force, and the Intelligence Community in peacetime and during

conflict. I have commanded units at the Squadron, Group, Wing, Joint Task Force and Numbered Air Force levels prior to my current assignment as the Deputy Commander of US Cyber Command. My assignments, both in command and as a staff officer, have afforded me broad insight into command and leadership from the tactical to the strategic level, and provided substantial experience coordinating with senior government officials, congressional members and staff, senior military leaders, foreign partners, members of industry, and academia. Finally, I have been privileged to attend a number of schools for further professional education designed to prepare me for leadership and command at the senior levels of our armed forces.

Question. Do you believe that there are any steps that you need to take to enhance your expertise to perform the duties of the Commander, U.S. Cyber Command or the Director of the National Security Agency/Chief of the Central Security Service?

Answer. I am a firm believer in life-long learning. If confirmed, I would strengthen our relationships with industry, coalition partners, and interagency stakeholders, while learning from their perspectives and equities to enhance the effectiveness of our cyber and cryptologic efforts. Additionally, I intend to continue a program of self-study that involves regular interaction with those in academia, industry, the interagency, and select coalition partners to further my knowledge on leadership, technology, acquisition and cybersecurity.

RELATIONSHIPS

Section 162(b) of title 10, United States Code, provides that the chain of command runs from the President to the Secretary of Defense and from the Secretary of Defense to the commanders of the combatant commands. Other sections of law and traditional practice, however, establish important relationships outside the chain of command. Please describe your understanding of the relationship of the Commander, U.S. Cyber Command, to the following officials:

Question. The Secretary of Defense

Answer. The Commander, USCYBERCOM performs duties under the authority, direction, and control of the Secretary of Defense and is directly responsible to the Secretary for the preparedness of the command to carry out its assigned missions. If confirmed, I will work closely with the Secretary of Defense in coordination with the Chairman of the Joint Chiefs of Staff.

question. THE DEPUTY SECRETARY OF DEFENSE

Answer. The Deputy Secretary of Defense performs such duties and exercises such powers prescribed by the Secretary of Defense. The Deputy Secretary of Defense will act for and exercise the powers of the Secretary of Defense when the Secretary is disabled or the office is vacant. If confirmed, I will work closely with the Deputy Secretary, as appropriate.

Question. The Director of National Intelligence

Answer. As the head of the Intelligence Community, the Director of National Intelligence (DNI) acts is the principal advisor to the President and the National Security Council on intelligence matters pertaining to national security; and oversees and directs the implementation of the National Intelligence Program. The Director of National Intelligence coordinates national intelligence priorities and facilitates information sharing and coordination across the Intelligence Community. If confirmed, I will work closely with the Director of National Intelligence in the exercise of her authorities.

Question. The Under Secretary of Defense for Policy

Answer. The Under Secretary of Defense for Policy (USD(P)) is the Principal Staff Assistant (PSA) and advisor to the Secretary and Deputy Secretary of Defense for matters regarding the formulation of national security and defense policy, and the integration of DOD policy, strategy, plans, execution, and capabilities to achieve national security objectives. If confirmed, I look forward to working closely with the USD(P) on all policy issues affecting USCYBERCOM and NSA.

Question. The Under Secretary of Defense for Intelligence and Security

Answer. The Under Secretary of Defense for Intelligence & Security (USD(I&S)) is the advisor and PSA to the Secretary and Deputy Secretary of Defense for all intelligence, counterintelligence, security, sensitive activities and other intelligence-related matters. Moreover, the USD(I&S) exercises authority, direction, and control on behalf of the Secretary of Defense over the National Security Agency / Central Security Service, subject to authority of the DOD Chief Information Officer concerning the activities of the Cybersecurity Directorate. The USD (I&S) also exercises authority, direction and control over the Defense Intelligence Enterprise, and serves as the Director of Defense Intelligence and principal advisor to the DNI on Defense Intel-

ligence matters. If confirmed, I look forward to working closely with the USD(I&S) on matters relating to USCYBERCOM's and NSA's responsibilities.

Question. The Under Secretary of Defense for Acquisition and Sustainment

Answer. The Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)) is the PSA and advisor to the Secretary of Defense for all matters relating to acquisition and sustainment in the DOD, and serves as the senior procurement executive for the Department of Defense, with the mission of delivering and sustaining timely, cost-effective capabilities for the armed forces. Acting through the Command Acquisition Executive (CAE), the Commander of USCYBERCOM is responsible for the development, acquisition and (as applicable) sustainment of cyber operations-peculiar equipment, capabilities and services. If confirmed, in coordination with the PCA, I look forward to working closely with the USD(A&S) to ensure that the USCYBERCOM CAE executes the command's acquisition authorities consistent with Department policies in support of national priorities.

Question. The Under Secretary of Defense for Research and Engineering

Answer. The Under Secretary of Defense for Research and Engineering (USD(R&E)) is responsible for overseeing the research, engineering, and technology development activities across the DOD enterprise to ensure technological superiority for the Department. If confirmed, I look forward to working closely with the USD(R&E), in coordination with the PCA, to drive innovation and accelerate the advancement of cyber capabilities, thereby ensuring we maintain dominance in cyberspace.

Question. The Assistant Secretary of Defense for Homeland Defense and Global Security

Answer. The Assistant Secretary of Defense for Homeland Defense and Hemispheric Affairs (ASD (HD&HA)), under the authority, direction, and control of the USD(P), executes responsibilities including overall supervision of the homeland defense and Defense Support of Civil Authorities (DSCA) activities of the DOD, as well as defense continuity and mission assurance, and U.S. defense and security policy for other nations in the Western Hemisphere. If confirmed, I look forward to working with the ASD (HD&HA) and the USD(P) on matters regarding USCYBERCOM's assigned responsibilities.

Question. The Assistant Secretary of Defense for Space Policy and Principal Cyber Advisor to the Secretary of Defense

Answer. As a result of the recent establishment of the position of the ASD(Cyber Policy), I understand the Department is evaluating the future cyber policy roles of the new ASD (Cyber Policy) and PCA, as well as other leaders involved in the formulation of the Department's cyber policy, such as the USD(Policy), the ASD(Space Policy), and the DOD CIO. If confirmed, I will partner with USD(Policy) and DOD CIO to ensure alignment as these changes are implemented.

Question. The Department of Defense Chief Information Officer

Answer. The DOD Chief Information Officer (CIO) is the PSA and advisor to the Secretary of Defense and Deputy Secretary of Defense on policy, oversight, guidance, and coordination for all Department of Defense matters related to architecture and programs related to the networking and cyber defense architecture of the Department; information resource management; information technology; electromagnetic spectrum, including coordination with other Federal and industry agencies; coordination for classified programs; and in coordination with the Under Secretary for Personnel and Readiness, policies related to the Cyber Operations Force (COF); for nuclear command and control systems; positioning, navigation and timing. Additionally, the CIO exercises authority, direction, and control over the Defense Information Systems Agency and the activities of the Cybersecurity Directorate of the National Security Agency. If confirmed, I look forward to working closely with the Chief Information Officer on matters regarding USCYBERCOM's and NSA's responsibilities.

Question. The Chairman of the Joint Chiefs of Staff

Answer. The Chairman of the Joint Chiefs of Staff is the principal military advisor to the President, National Security Council, and Secretary of Defense. Communication between the President or the Secretary of Defense and the Combatant Commanders flows through the Chairman. By custom and tradition, and as instructed by the Unified Command Plan, if confirmed, I would routinely communicate with and through the Chairman regarding matters within USCYBERCOM's and NSA's responsibilities to ensure that he or she remains fully informed and able to provide sound and timely military advice to senior policymakers.

Question. The Secretaries of the Military Departments

Answer. The USCYBERCOM Commander's authority over assigned Service components is clear in the Goldwater-Nichols Act but requires close coordination with the Secretaries of the Military Departments to ensure that USCYBERCOM does not

intrude upon the responsibilities of the Secretaries of the Military Departments. Close coordination between the USCYBERCOM Commander, the Principal Cyber Advisor, and each of the Secretaries of the Military Departments is also essential for gaining and maintaining the Services' support to cyber operations forces as an integral part of the Joint Force.

Question. The Chiefs of Staff of the Services

Answer. The Service Chiefs are charged to provide organized, trained, and equipped forces to be employed by Combatant Commanders in accomplishing their assigned missions. Additionally, these officers serve as members of the Joint Chiefs of Staff and as such have a lawful obligation to provide military advice. Individually and collectively, the Service Chiefs are a tremendous source of experience and judgment. If confirmed, I look forward to working closely and conferring regularly with the Service Chiefs.

Question. The Combatant Commanders, and, specifically, the Commanders of U.S. Strategic Command and U.S. Northern Command

Answer. The Commander, USCYBERCOM, has both supported and supporting relationships with other Combatant Commanders, largely identified within the Unified Command Plan, the Joint Strategic Capabilities Plan, execute orders, and operation orders. In general, the Commander, USCYBERCOM, is the supported commander for trans-regional and global cyberspace operations and is a supporting commander for cyberspace operations specific to a single Combatant Commander's area of responsibility. Specific relationships with the Commander, U.S. Northern Command, and Commander U.S. Strategic Command, will be delineated by the President or the Secretary of Defense in execute and/or operation orders. If confirmed, I look forward to working with the Combatant Commanders to deepen these relationships to support national and theater security objectives.

Question. The Director of the Defense Information Systems Agency

Answer. The Defense Information Systems Agency (DISA) is a DOD Combat Support Agency that provides, operates, and assures command and control, information sharing capabilities, and a globally accessible enterprise information infrastructure in direct support of national leaders, joint warfighters, and other mission and coalition partners across the full spectrum of operations. The Commander, USCYBERCOM, must maintain a close relationship with the DISA Director to coordinate and represent requirements in this mission area in order to accomplish assigned missions. If confirmed, I look forward to working closely with the DISA Director on matters of shared interest and importance.

Question. The Director of the Defense Intelligence Agency

Answer. The Director of the Defense Intelligence Agency (DIA) manages and executes specified Defense Intelligence and counterintelligence functions across the Defense Intelligence Enterprise and for select functions across the greater Intelligence Community. The DIA analyzes and disseminates military intelligence in support of combat and noncombat military missions, and serves as the Nation's primary manager and producer of foreign military intelligence. If confirmed, I look forward to working closely with the DIA Director on matters relating to USCYBERCOM's assigned responsibilities.

Question. The Director of the National Reconnaissance Office

Answer. The Director of the National Reconnaissance Office (NRO) is the principal advisor on overhead reconnaissance to the Secretary of Defense, the Chairman of the Joint Chiefs of Staff, and the Combatant Commanders, responsible for developing, acquiring, launching, and operating space-based intelligence, surveillance and reconnaissance capabilities to secure and expand the U.S. intelligence advantage. If confirmed, I look forward to working closely with the NRO Director on matters relating to USCYBERCOM's assigned responsibilities.

Question. The Chief Digital and Artificial Intelligence Officer

Answer. The Chief Digital and Artificial Intelligence Office (CDAO) is DOD's senior official responsible for the acceleration of adoption of data, analytics, and AI to generate decision advantage. To this end, the CDAO leads strategy and policy on data, analytics, and AI adoption; provides oversight for efforts throughout the Department; develops digital and AI-enabled solutions at scale; and provides expertise to address urgent requirements and emergent challenges. If confirmed, I look forward to working closely with the CDAO, in coordination with other DOD and OSD component heads, to integrate efforts to build enduring advantage for the Department and the Nation.

Question. The National Cyber Director

Answer. The National Cyber Director is the principal advisor to the President on cybersecurity policy and strategy, and leads whole-of-government coordination of programs and policies to improve the cybersecurity posture of the United States, increase information and communications technology security, understand and deter

malicious cyber activity, and advance diplomatic and other efforts security, understand and deter malicious cyber activity, and advance diplomatic and other efforts security, understand and deter malicious cyber activity, and advance diplomatic and other efforts security, understand and deter malicious cyber activity, and advance diplomatic and other efforts security, understand and deter malicious cyber activity, and advance diplomatic and other efforts security, understand and deter malicious cyber activity, and advance diplomatic and other efforts

Question. The Director of the Cybersecurity and Infrastructure Security Agency

Answer. The Cybersecurity and Infrastructure Security Agency (CISA) Director is the operational lead for Federal cybersecurity and the national coordinator for critical infrastructure security and resilience, facilitating collaboration and partnership between all levels of government, industry, educational institutions, and the American public to reduce risk to the Nation's cyber and physical infrastructure. The CISA Director reports to the Secretary of Homeland Security and is also responsible for fulfilling the Secretary's responsibilities for the security of Federal information and information systems, except for National Security Systems. If confirmed, I look forward to continuing the close partnership my predecessors have each enjoyed with the CISA Director to deter, prevent and disrupt threats to the Nation's information systems and critical infrastructure.

MAJOR CHALLENGES AND PRIORITIES

Question. In your view, what are the major challenges that will confront the next Commander of U.S. Cyber Command?

Answer. In my view, the principal threats to national security stem from the People's Republic of China, which continues to challenge the United States on a global scale while seeking to expand its malign influence, and Russia, which remains engaged in unlawful military aggression in Ukraine and malicious cyber activity. We must constantly posture to gain and maintain enduring advantages throughout the competition/crisis/conflict continuum. Our ability to move with agility and seize fleeting opportunities in our campaigning efforts rest on rapid maturation of USCYBERCOM's service like authorities to: improve readiness across the force; implement new technologies; and scale capabilities that will outpace the threat.

Question. In your view, what are the major challenges that will confront the next Director of the National Security Agency/Chief of the Central Security Service?

Answer. In my view, the principal threats to national security stem from the People's Republic of China, which continues to challenge the United States on a global scale while seeking to expand its malign influence, and Russia, which remains engaged in unlawful military aggression in Ukraine and malicious cyber activity. We must continue to execute our mission to deliver outcomes against National priorities in foreign intelligence, cybersecurity, protecting our national security systems and provide combat support to the Department of Defense. To do that, we must focus on strengthening the workforce, ensuring a culture of compliance, investing to leverage new technologies, and focusing on threats facing the Nation, especially the pacing challenge posed by the People's Republic of China.

Question. If confirmed, what plans do you have for addressing these challenges?

Answer. If confirmed, I will perform a review of both USCYBERCOM and NSA's plans and approaches to our missions and emerging requirements; gain better understanding of challenges, gaps, and opportunities; and then work with Congress, the Department, and the DNI to address requirements and adjust approaches in each area as required.

Question. If confirmed, what will be your priorities for U.S. Cyber Command?

Answer. If confirmed as the Commander of USCYBERCOM, my priority lines of efforts will be People, Innovation, and Partnerships. People are the foundation of everything we do; therefore, we must carefully mature the entire talent management lifecycle in order to improve training and readiness. We must stay on the cutting edge of new innovations and technological advances, especially in terms of artificial intelligence and advanced computing, to build and maintain warfighting advantage. And finally, we will expand capacity by ensuring trusted collaborative relationships with our combatant command, interagency, international partners, and academia and industry.

Question. If confirmed, what will be your priorities as the Director of the National Security Agency/Chief of the Central Security Service?

Answer. If confirmed as the Director of the NSA/Chief of the CSS, I will use the same priority framework described above: People, Innovation, and Partnerships. I will focus on ensuring the health and effectiveness of NSA's world-class personnel in delivering outcomes against National priorities and providing combat support to the Department of Defense. I will look for opportunities to invest in new tech-

nologies that will allow us to outpace threats facing the Nation-especially the pacing challenge posed by the People's Republic of China. And finally, NSA's ability to work in collaboration across the interagency, the private sector, and foreign partners is one of the agency's greatest strengths and critically important to our Nation's success in a world of accelerating change.

RELATIONS WITH CONGRESS

Question. What are your views on the State of U.S. Cyber Command's relationship with the Senate Armed Services Committee in particular, and with Congress in general?

Answer. In my current role, I have seen first-hand USCYBERCOM's positive interactions with the Senate Armed Services Committee (SASC) and Congress. Our relationship is strong, built on transparency and responsiveness, and supports the requirements of advancing USCYBERCOM's mission and ensuring oversight. Members of the SASC have been very supportive of USCYBERCOM through office calls, briefings, hearings and visits. Additionally, SASC professional staff members (PSMs) have supported USCYBERCOM through meetings, attendance at conferences and staff delegations. These efforts help build relationships and ensure a common understanding to include capabilities, threats, authorities and mission execution. If confirmed, I look forward to maintaining and growing this relationship.

Question. If confirmed, what actions would you take to sustain a productive and mutually beneficial relationship between Congress and U.S. Cyber Command?

Answer. If confirmed, I would ensure a strong dialog exists between Congress and USCYBERCOM, and look forward to building an engaged partnership. I will ensure compliance with relevant statues, including provisions of the annual National Defense Authorization Act (NDAA), and other relevant law. I will buildupon the close relationship with members of the SASC and other congressional defense oversight committees, ensuring my Legislative Liaison office continues to work closely with the PSMs and personal staff members.

CYBER THREATS

Question. In your view, what are the most serious cyber threats facing the United States today, and what potential targets are the most vulnerable or susceptible to cyber attacks?

Answer. In my view, the principal threats to national security stem from the People's Republic of China, which continues to challenge the United States on a global scale while seeking to expand its malign influence, and Russia, which remains engaged in unlawful military aggression in Ukraine and malicious cyber activity. However, threats to our Nation's security are numerous—actors such as Iran and North Korea attempt to coerce their respective regions with both conventional and cyber weapons, while terror groups, malicious cyber actors, and drug cartels present ongoing and transnational threats. Rapid changes in the technological environment will require the constant development of new and better approaches in response to these threats to maintain the safety of the Nation and our allies. USCYBERCOM is addressing these challenges through a constructive plan that secures, operates and hardens our critical networks in addition to reinforcing the fabrics of our international partners.

Question. What future strategic cyber threats should the United States prepare for?

Answer. We face a challenging and volatile threat environment, and cyber threats to our national security interests and critical infrastructure rank at the top of the list. Rapid changes in the technological environment will require the constant development of new and better approaches in response to these threats to maintain the safety of the Nation and our allies; this will be a priority for me if confirmed. USCYBERCOM must continue to impose costs on our adversaries whenever we detect them conducting reconnaissance, espionage, influence, and even attacks in cyberspace.

Question. What are your views on Russia's cyber capabilities as well as intentions in light of the invasion of Ukraine?

Answer. Russia is a highly capable cyber adversary, possessing deep technical knowledge and advanced tools, tactics, and techniques. Its cyber actors employ these capabilities to conduct information operations, cyberespionage, and cyberattacks using open source, commercially available, and custom-developed tools to persistently target government networks, commercial networks and critical infrastructure within the United States, EU, and NATO. Cyber espionage likely remains the most persistent cyber threat from Russian government cyber actors. Russia will likely continue to integrate cyberwarfare into its military plans and operations to keep

pace with USCYBERCOM efforts, and conduct cyberspace operations in response to perceived domestic threats.

Question. What are your views on China's cyber capabilities and intentions, especially regarding potential cyber attacks on United States critical infrastructure prior to and during any possible military operations against Taiwan?

Answer. The People's Republic of China poses one of the most advanced cyber threats to the United States and employs its capabilities to support Beijing's political, diplomatic, and military goals. The People's Liberation Army (PLA) is investing in strong cyber capabilities as a counterbalance to United States military superiority by exploring options to attack essential warfighting networks and critical infrastructure supporting U.S. military operations and other U.S. Government activities. If Beijing feared a major conflict with the United States were imminent, the PRC might consider conducting aggressive cyberspace operations against United States critical infrastructure and military assets worldwide.

Question. What are your views on North Korea's cyber capabilities?

Answer. North Korea's cyber program poses a sophisticated threat to the United States and its allies. State actors conduct malicious cyber activity to collect intelligence, conduct attacks, and generate revenue to bypass sanctions and fund regime goals (to include its nuclear and missile programs). North Korea continues to adapt to global trends in cybercrime by stealing cryptocurrency to bring in significant amounts of revenue.

Question. What are your views on Iran's cyber capabilities?

Answer. Iran's growing expertise and demonstrated willingness to conduct aggressive cyberspace operations makes it a major threat to United States and partner networks and data. Iran likely considers its cyber program as an important tool to retaliate and gather intelligence against adversaries, as demonstrated by Iran's cyberattack last year against Albanian government networks. Domestically, Iran uses its capabilities to help control the population.

Question. What are your views on transnational terrorist groups' and transnational criminal organizations' cyber capabilities? In particular, do you believe U.S. Cyber Command should have a role in assessing and undermining these capabilities?

Answer. Transnational terrorist groups primarily leverage cyberspace to conduct activities in support of their kinetic operations. They use cyberspace for secure communications, recruitment, financial transactions, media and propaganda, and research. Foreign terrorist groups have marginal limited offensive cyber capabilities, and those they do have are largely unsophisticated and limited to website defacements. Transnational criminal organizations facilitate the flow of illicit drugs, including Fentanyl, into the United States. These TCOs are sophisticated and possess notable capability, capacity, and resources. USCYBERCOM works closely with the other combatant commands on transnational issues.

Question. Do you believe that China and Russia are engaging in cyber cooperation activities with other United States adversaries to help amplify the impact and effect of their cyber operations against the United States?

Answer. The PRC is unlikely to engage in cyber cooperation with other United States adversaries outside of a specific subset of activities, that include: attempting to set new norms in cyberspace governance, collaborating on cybersecurity by exporting Chinese information technology hardware and software, and as demonstrated following Russia's invasion of Ukraine, the spreading of disinformation that amplified Russia's themes against the United States and NATO. Russia is unlikely to share capabilities and accesses with other United States adversaries, as these remain largely the purview of Moscow's intelligence agencies. Cyberspace operations collaboration among adversary intelligence agencies is low and distrust is high.

U.S. CYBER COMMAND MISSIONS

Question. In a strategic sense, how do you define the U.S. Cyber Command mission?

Answer. In line with title 10, U.S. Code, Section 167b, the principal mission of USCYBERCOM is to direct, synchronize, and coordinate military cyberspace planning and operations to defend and advance national interests in collaboration with domestic and international partners. USCYBERCOM also has Unified Command Plan responsibilities for: planning and executing cyberspace operations, as directed, the Cyberspace Operations Joint Force Provider, and the Joint Cyberspace Trainer.

Question. How do you define the role of the National Cyber Mission Force in countering adversary cyber forces in the event that such forces undertake destructive or obstructive attacks on the United States?

Answer. The Cyber National Mission Force (CNMF) focuses on countering cyber threat actors and maneuvering against those adversaries to preclude malicious cyberspace activities, including cyberattacks and to shape adversary behavior. CNMF accomplishes this by executing cyber operations, building and refining the processes to share adversary threat data across the government and with industry; engaging with sector-specific agency partners to help them build greater resiliency within our critical infrastructure; and supporting a whole-of-nation approach to deter malicious cyber activities.

Question. Do you believe the existing command and control relationships between U.S. Cyber Command and the geographic combatant commands need to be reevaluated given the need and opportunity to provide cyber support to tactical military operations?

Answer. No, not at this time. The current command and control relationship between USCYBERCOM and the geographic combatant commands enables effective employment of cyberspace operations to achieve our assigned missions. The Department reached this model over years of maturation, which includes a close working relationship between the Combatant Commands' leadership, a heightened emphasis on the general support relationship between the Joint Force Headquarters-Cyber (JFHQ-C) and the other combatant commands, and the direct support of the Cyberspace Operations—Integrated Planning Elements established within each combatant command staff. This model has proven itself through multiple crises and is one I intend to continue to support, if confirmed.

Question. How successful has U.S. Cyber Command been at integrating its national defensive, national offensive, and command support missions with the missions and kill chains of the non-cyber operational components of the Department of Defense?

Answer. The success of USCYBERCOM's integration across the Department and its warfighting domains has been proven out through several crises. We have shown ourselves to be adaptive and responsive through the employment of the Cyber National Mission Force (CNMF) and Joint Force Headquarters-DOD Information Network (JFHQ-DODIN) for national requirements. USCYBERCOM supports requirements of other combatant commands via our general support assignment of the Joint Force Headquarters-Cyber (JFHQ-C), and the direct support of the Cyberspace Operations—Integrated Planning Elements.

Question. What organizational and authorities challenges remain at U.S. Cyber Command related to its missions? Specifically, do you think that additional organizational changes and authorities will be needed to resolve the readiness problem within the Cyber Missions Force?

Answer. Congress and the Department of Defense have given USCYBERCOM significant authorities to address the issues. Some of these authorities include Enhanced Budgetary control (EBC); establishing standards for Joint cyberspace training; strategy, doctrine and tactics development; and an expanded role in acquisition. Additionally, our Cyber Excepted Service (CES) enables us to offer civilian cyber professionals opportunities to use their skills in support of the Command. These authorities allow USCYBERCOM to align its priorities, in partnership with the Services, with its ability to execute more effectively.

Question. If confirmed, would you recommend or support any changes in the missions currently assigned to U.S. Cyber Command given that some experts have recommended that U.S. Cyber Command assume responsibility for additional elements of information warfare, including information operations and electromagnetic spectrum operations? If so, what changes would you recommend?

Answer. I don't recommend changes to the current missions assigned. USCYBERCOM has an important role to play in cyber-enabled information activities, but believe it is best done in partnership with the other combatant commands. If confirmed, this will be an area that I will review closely with the Joint Staff, USSOCOM, and the Services.

Question. Do you agree with General Nakasone that election security and defending the United States from foreign influence campaigns were "no fail" missions of both the NSA and U.S. Cyber Command? Please explain your answer. If possible, give some examples of how we are better positioned to defend against such attacks today than we were prior to 2016.

Answer. I absolutely agree. As the co-lead of the Russia Small Group during the 2018 mid-term elections, as the USCYBERCOM lead for the NSA-USCYBERCOM Election Security Group in 2020, and, as Deputy Commander of USCYBERCOM, overseeing USCYBERCOM's support to defend the 2022 U.S. elections from foreign actors, I have seen the scale of our operations and our partnerships grow exponentially. The sustained focus on this mission by NSA and USCYBERCOM, enables speed, agility, and breadth of operations to persistently engage these adversaries

and postures the organizations to defend against foreign threats to the 2024 election.

NATIONAL SECURITY AGENCY (NSA) MISSIONS

Question. What is your understanding of the NSA mission?

Answer. It's my understanding that NSA's principal missions, SIGINT and Cybersecurity, are key to the safety and security of our Nation. The NSA's SIGINT mission plays a vital role in our national security by providing America's leaders with the critical foreign intelligence they need to defend our country, save lives, and advance U.S. goals and alliances. The cybersecurity mission prevents and eradicates threats to U.S. National Security Systems (NSS), as well as identifying cyber threats the defense industrial base (DIB) and the U.S. military's weapon systems. NSA's SIGINT and Cybersecurity missions are also critical to fulfillment of NSA's combat support responsibilities.

Question. What is your understanding of the NSA mission as it relates to cyber?

Answer. NSA is responsible for securing NSS as well as preventing and eradicating threats to NSS with a focus on the DIB and the U.S. military's weapon systems. NSA also produces cyber threat intelligence products for a wide array of consumers, including making many of these products available to the public.

Question. In your view, what role should the NSA play in support of U.S. Cyber Command and does it differ from the support that NSA provides to other combatant commands?

Answer. The signals intelligence and cyber operating environments intersect in an inextricable way. As a foreign intelligence organization and a Combat Support Agency (CSA), NSA plays a significant role in generating timely and relevant intelligence that supports operational commands like USCYBERCOM. NSA's Signals Intelligence mission and the Agency's role in cybersecurity are complementary to USCYBERCOM's role in cyberspace operations and, thus, provide a unique opportunity for collaboration.

Question. In your view, in developing capabilities to support the objectives of regional combatant commanders in a conflict, should U.S. Cyber Command explore the development of strategies and operational objectives that are separate from those of kinetic conventional forces? Or should U.S. Cyber Command continue to strive to complement and reinforce traditional forms and modes of warfare?

Answer. USCYBERCOM should strive to do both. USCYBERCOM should employ strategies and operational objectives that support the Combatant Commands both defensively and offensively in support of the Joint Force. In close coordination with the other combatant commands and the interagency, USCYBERCOM should also develop strategies to defend forward by leveraging unique authorities and capabilities to degrade nation-State cyber actors seeking to target the DOD or U.S. critical infrastructure.

Question. Do you believe that any of the mass or narrow surveillance capabilities currently employed by the NSA should be reconsidered or adjusted?

Answer. As the President articulated in recent Executive Order (EO) 14086, which was issued on October 7, 2022, the United States collects signals intelligence so that decisionmakers have access to the critical information necessary to advance the national security interests of the United States and to protect its citizens and allies from harm. The signals intelligence capabilities of the United States are of the utmost importance to the ability of the executive branch to protect our security, but such capabilities also come with tremendous responsibilities and obligations, to include ensuring that all persons are treated with dignity and respect, despite their nationality, and that all persons have legitimate privacy interests in the handling of their personal information.

From my current perspective and information made known to me through my current position, I believe that all of NSA's signals intelligence activities are authorized and consistent with the principles recently articulated by the President in EO 14086. Among others, NSA's signals intelligence activities are authorized and undertaken in accordance with the Constitution and applicable statutes, EOs, proclamations, and other Presidential directives. Further, NSA's activities are subject to appropriate safeguards, and are only conducted in a manner that is proportionate to the validated intelligence priorities for which they have been authorized. Finally, NSA conducts all of its signals intelligence activities in pursuit of only those legitimate objectives contained within EO 14086. NSA does not conduct signals intelligence collection capabilities for any of the prohibited objectives identified in the EO. If confirmed, I would ensure that NSA's signals intelligence activities will continue to be carried out in adherence to all safeguards contained within EO 14086.

Question. Do you believe that the NSA is appropriately transparent about its surveillance priorities and processes? If improvements are possible, how do you intend to ensure that they are carried out?

Answer. Transparency in the IC is a balancing act, since the IC cannot perform its mission effectively unless it protects its classified intelligence sources and methods from disclosure to the Nation's adversaries. Maintaining public trust, however, is essential for the IC to be successful in its foreign intelligence mission. If confirmed, I would ensure that NSA complies with the letter and spirit of the Constitution and statutes, and exercises candor with all overseers across all three branches of government. Additionally, NSA must make available to the public information about its activities to the greatest extent possible.

SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

Question. Section 702 of the Foreign Intelligence Surveillance Act will expire at the end of calendar year 2023 unless renewed by Congress. There is bipartisan concern that queries of data collected under 702 using U.S. Persons search terms are conducted without a probable cause-based court order.

In your view, what is the continuing value of section 702 collection?

Answer. As a current customer of Foreign Intelligence Surveillance Act (FISA) Section 702 derived products, I recognize the value and importance of this key authority in providing unique foreign intelligence to fulfill national priorities. In my experience, intelligence derived from Section 702 has been critical in counterterrorism, cybersecurity, counterintelligence, countering international drug trafficking, and strategic competition. It is also my understanding that all of the President's intelligence priority topics reported on by NSA were supported by Section 702. I defer to the White House, ODNI, DOD, and NSA leadership, however, to fully characterize the value of this authority. If confirmed, I commit to working with Congress to ensure that surveillance conducted pursuant to Section 702, and all activities governed by FISA, are performed consistent with the Constitution, U.S. law and policy.

Question. What is your understanding of the guardrails and processes in place to ensure that this authority is executed within current statutory guidelines and to protect U.S. citizens from the possible abuse of this authority?

Answer. If confirmed, I will be in a better position to evaluate the specifics of NSA's Section 702 compliance and oversight systems. From my current vantage point I am aware that NSA has a robust compliance regime designed to ensure adherence to all statutory and procedural requirements, including those relating to Section 702. I know NSA's workforce is dedicated to compliance with the laws and policies that govern NSA's missions, including its Section 702 activities. NSA has a dedicated corporate compliance organization, and has instilled a culture of compliance within its workforce. Based on my prior experiences, I know that NSA's compliance team is part of each stage of the analytic process—from initial targeting decision to review of the responsive content—supporting the mission and ensuring that NSA's culture of compliance is maintained day in and day out.

Where possible, and consistent with the need to continue to protect classified sources and methods, NSA and the U.S. Intelligence Community have publicly released materials describing the compliance processes in place that pertain to Section 702. For example, NSA's Section 702 targeting, minimization, and querying procedures are all available to the public with minimal redactions. These documents describe how NSA uses Section 702 to target the communications of non-U.S. persons located outside of the United States to collect foreign intelligence, and the protections that NSA applies to ensure that NSA properly handles any U.S. person information within Section 702 collection. Additionally, NSA's Section 702 activities are overseen by an internal compliance organization as well as NSA's independent Inspector General. Every NSA Section 702 targeting decision is reviewed by the Department of Justice (DoJ), and NSA must report any incidents of non-compliance to DoJ and the Office of the Director of National Intelligence. DoJ attorneys investigate each potential incident of non-compliance, work with agencies to remediate any such instances, and report any incidents of non-compliance to the FISC and to Congress.

Question. If section 702 were to be extended without limiting the authority to query the data using U.S. persons' identifiers or search terms, how do you think that would impact NSA's mission?

Answer. Although I am generally familiar from sources such as the IC's Annual Statistical Transparency Reporting that NSA at times performs queries relating to U.S. persons, this is an issue I have limited familiarity in my current role with USCYBERCOM. At this time, I defer to current NSA leadership to fully characterize the impact to NSA's missions and other aspects of the current efforts taking

place under this authority. If confirmed, I fully commit to working with Congress on all matters related to this important authority.

Question. If 702 data base is queried using U.S. persons identifiers for the positive purpose of victim notification, in your view, is it feasible to construct a set of rules that would permit such searches while requiring a court order for criminal or intelligence investigations? How do you think that would impact NSA's mission?

Answer. If confirmed, I would be in a better position to judge how technically feasible such a change would be for NSA systems, and whether that would negatively impact the ability of NSA to carry out its missions effectively.

Question. What is your understanding of the Attorney General-approved guidelines pursuant to Executive Order 12333 for the government to query data that NSA has collected outside the United States using U.S. persons identifiers or search terms without reaching the probable cause standard?

Answer. Based on training and past experience, I am aware that NSA, as a component of the Department of Defense (DoD), is required to follow the Attorney General (AG)-approved procedures contained in DOD Manual 5240.01 when the Agency conducts activities pursuant to authority granted by EO 12333. NSA's signals intelligence (SIGINT) activities are further regulated by the AG-approved procedures contained in the Manual's SIGINT Annex (DoDM S–5240.01-A). In general, DODM 5240.01 permits DOD components to evaluate U.S. person information (USPI) acquired during intelligence activities to determine if the USPI qualifies for permanent retention. The SIGINT Annex adopts all of the requirements contained in the Manual, but places additional restrictions on the circumstances under which NSA may conduct queries of raw SIGINT information to intentionally retrieve communications of or concerning a U.S. person. The SIGINT Annex permits multiple types of U.S. person queries of raw SIGINT without requiring a probable cause finding, and I understand that many of these queries can be approved internally by NSA personnel. Examples include, but are not limited to situations where the United States person:

1) has consented to the query;
2) appears to be a victim of foreign cyber activities;
3) is being held overseas as a hostage of a foreign power; or
4) may be referenced in a foreign power dataset.

COMBAT SUPPORT AGENCY

Question. What is your understanding of the role of a combat support agency?

Answer. Under Title 10 of the U.S. Code, as amended by the Goldwater-Nichols Act, a Combat Support Agency (CSA) is one that provides combat support or combat service support functions to joint operating forces across a range of military operations and in support of Combatant Commanders executing these operations. CSAs perform support functions or provide supporting operational capabilities, consistent with their established directives and pertinent DOD planning guidance. The combat support mission of a CSA is that portion of its mission involving support for operating forces engage in planning for, or conducting, military operations, including support during conflict or in the conduct of other military activities related to countering threats to U.S. national security.

Question. If confirmed, how would you delineate the roles and activities of the NSA as a combat support agency in support of U.S. Cyber Command versus the support provided to U.S. Cyber Command as a cyberspace domain partner under the dual-hat arrangement?

Answer. USCYBERCOM follows standard processes for submitting signals intelligence requirements to NSA to enable combat support. As cyberspace domain partners, NSA and USCYBERCOM have distinct and complementary authorities. If confirmed, I will direct clear recognition across both NSA and USCYBERCOM that each organization has separate roles, resources, and responsibilities, and that our inter-service support agreements, memoranda of understanding, and special partnership agreements are followed and enforced.

Answer. Under the Goldwater-Nichols Act, the Chairman of the Joint Chiefs of Staff is required to regularly conduct assessments of the readiness of combat support agencies to support the combatant commands.

Question. What is your understanding of how the NSA has performed in these assessments?

Answer. It's my understanding that the CJCS is required by law to submit biennial assessments to Congress of the responsiveness and readiness of each CSA to support the combatant commands (CCMDs). In my current position, I do not have insight into how NSA has performed in these assessments, but if confirmed, I look forward to reviewing the CJCS's assessment of NSA.

Question. What is your understanding of how the Director of National Intelligence has expressed concern, if any, that the support NSA provides to U.S. Cyber Command is excessive or unjustified in light of NSA's role as a combat support agency or as a cyberspace domain partner with Cyber Command under the dual-hat arrangement?

Answer. Last year the DNI and the Secretary of Defense commissioned a study of the dual-hat arrangement led by the former Chairman of the Joint Chiefs of Staff, Ret. General Joseph Dunford. The review found that the dual-hat arrangement provided substantial benefits for the Nation. The study found that although there have been concerns in the past with respect to structure, budget, and oversight, any negative effects in these areas have been effectively mitigated by agreements and processes now in place to ensure clear accountability, cost reimbursement, and oversight. Following a review of findings from the Joint Study, the Secretary of Defense, Director of National Intelligence, and Chairman of the Joint Chiefs of Staff agree that it is in the best interest of the Nation to maintain the Dual-Hat leadership arrangement of the National Security Agency (NSA) and the United States Cyber Command.

ACT OF WAR IN CYBERSPACE

Question. In general, what do you believe would constitute an act of war in cyberspace?

Answer. It is generally accepted that cyber operations that cause death, injury, or significant damage to property would likely be considered a use of force, triggering a nation's inherent right of self-defense under international law. Ultimately, whether an act in cyberspace warrants a U.S. response in self-defense is a determination for our civilian leadership.

Question. Do you believe that current U.S. Government policy provides adequate guidance and decision space for making a determination of what types of actions might constitute an act of war in cyberspace?

Answer. Yes. U.S. policy and domestic and international law provide a sufficient framework and decision space to advise our civilian leadership whether malicious cyber acts, alone or in concert with other acts, warrant invoking the U.S. right to use force in self-defense.

Question. Concerning acts of aggression in cyberspace, do you believe the Department of Defense has a comprehensive understanding of the actions that may constitute a hostile act under the Law of Armed Conflict, particularly as it relates to U.S. critical infrastructure, and the energy, transportation, power, and financial sectors within the U.S.?

Answer. As with malign activity in any other domain, Departmental leaders, in coordination with the Intelligence Community, the State Department, and other key executive branch partners, are able to assess and advise the President whether malicious cyber acts alone or in concert with other acts, are sufficient to invoke the U.S. right to use force in self-defense. It is important to note that malicious cyber activities that do not constitute hostile acts of aggression may nonetheless cause strategic effects, constitute violations of other international legal rules or international norms, or warrant appropriate responses.

DEPARTMENT OF DEFENSE'S ROLE IN DEFENDING THE NATION FROM CYBER ATTACK

Question. What is your understanding of the role of the Department of Defense in defending the Nation from an attack in cyberspace? In what ways is this role distinct from those of the homeland security and law enforcement communities?

Answer. DoD employs the military instrument of national power while defending the homeland from foreign threats abroad. DOD, through USCYBERCOM and NSA, works together with a larger Executive branch team to defend the Nation from malicious cyber activity, including cyber attacks. In order to defend the Nation from malicious cyber activities, the Department can defend forward in three ways: generating insights about the threat; providing advice to Federal, State, local, and foreign partners to enhance their defenses; and, acting when necessary and consistent with DOD's authorities, to disrupt adversary cyber actors. DOD may also provide defense support of civil authorities, upon request, should a cyber incident exceed the capacity of another department or agency.

Question. What is your understanding of the specific role of the Cyber National Mission Force in disrupting cyber attacks on U.S. critical infrastructure and other non-military targets?

Answer. The CNMF works abroad to persistently engage foreign malicious cyber actors who threaten U.S. critical infrastructure. Through Hunt Forward missions, where we deploy teams of cyber operators to work with allies and partners to find

and enable them to defend against malicious cyber actors operating on foreign partner networks, we discover cyber threats before they reach the United States. These operations do several things: they enable USCYBERCOM to posture to take action to disrupt the threat to the United States, they strengthen partners and allies' defenses, and they give us insight into new threats. We then share that threat information with domestic partners like the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and with industry to enable measures to harden cyber-defenses here at home.

Question. Can you describe how a request for Defense Support to Civil Authorities (DSCA) by appropriate civilian leadership might be made in the event of a cyber incident? Are those processes trained for and exercised with U.S. Cyber Command, and the inter-agency community?

Answer. When requested by another Federal department or agency and approved by the appropriate DOD official, or as directed by the President, DOD responds to a cyber incident pursuant to the long-standing Defense Support of Civil Authorities (DSCA) process. The DOD weighs each DSCA request individually to determine if it has sufficient capability and capacity to support. Through collaborative partnerships with NSA, DHS/CISA, U.S. Northern Command (USNORTHCOM) and/or U.S. Indo-Pacific Command (USINDOPACOM), the National Guard Bureau, and others, USCYBERCOM is well-postured to respond to such requests when they occur.

Question. In your view, does U.S. Cyber Command have the capacity and the authority to directly operate in the networks of domestic critical infrastructure providers to defend against major cyber attacks?

Answer. As an Active component military force, USCYBERCOM's mission and authorities are focused on foreign operations against foreign actors. The command does not conduct operations inside the United States, but enables those domestic partners with appropriate authorities, including the Department of Homeland Security and the FBI. As directed, USCYBERCOM can support civil authorities to defend U.S. critical infrastructure from malicious cyber activities in and through cyberspace, in coordination with or in support of USNORTHCOM and/or USINDOPACOM in the exercise of their homeland defense and DSCA missions.

Question. What is your understanding of the expected role of the National Guard in defending critical infrastructure from cyber attacks in support of civil authorities?

Answer. The National Guard is both a force multiplier for USCYBERCOM missions and a critical capacity for their states. Many of our U.S. National Guard and Reserve members have significant and relevant private-sector experience and can rapidly share appropriate information on malicious cyber activity with State and local authorities. These members can conduct state-authorized operations domestically under State law to protect critical infrastructure while in a State Active Duty status or , if need be, can be mobilized on Federal Active Duty to join the USCYBERCOM mission directly.

Question. What is your understanding of the government's policies in recognizing and responding to cyberspace gray zone activities below the threshold of war in which cyber attacks might be used against U.S. Homeland critical infrastructure and military assets worldwide to deter U.S. Military action by impeding U.S. decisionmaking, inducing societal panic, and interfering with the deployment of U.S. Forces?

Answer. U.S. policy is to use all instruments of national power to counter cyber attacks and malicious cyber activity of foreign adversaries that target the United States and threaten our national security. Executive branch policies prioritize enhanced cybersecurity for U.S. critical infrastructure and National Security Systems, and DOD has been granted statutory authorities to conduct appropriate and proportionate military activities in foreign cyberspace to disrupt and defend against foreign malicious cyber activity directed against our government, people and critical infrastructure. These policies have contributed to DOD's ability to recognize and mitigate these threats in collaboration with domestic and international partners.

DETERRENCE THROUGH COST IMPOSITION

Question. Multiple annual threat assessments of the U.S. Intelligence Community have concluded that the People's Republic of China (PRC) would attack United States critical infrastructure through cyber operations if Beijing decided to invade Taiwan and expected the United States to intervene. The Defense Science Board (DSB) Task Force report on Cyber Deterrence, issued in February 2017, concluded that it is critical for the Department of Defense (DOD) to develop cost-imposing deterrence options based on scalable offensive cyber capabilities to hold at risk a range of assets that the leaders of strategic adversaries value most highly. The DSB report urged the Secretary of Defense to develop "a policy framework for cyber deterrence

including: updated declaratory policy relating to U.S. responses to cyber attack and use of offensive cyber capabilities, guidance for the employment of offensive cyber, a public affairs plan, and an engagement plan for adversaries and allies."

What are your views on the conclusions and recommendations of this Task Force?

Answer. I believe that USCYBERCOM's role in campaigning in cyberspace below the level of armed conflict is critical to reinforce deterrence and to impose costs on our adversaries. The DSB study predated Congress' action on declaring cyber a domain of traditional military activity, enabling alignment of U.S. law, policy, and authorities to DOD. The 2023 National Cyber Strategy and 2023 DOD Cyber Strategy—which nests within the 2022 National Defense Strategy (NDS—address many of the areas of the DSB study by clearly and publicly articulating that all tools of national power will be used in a more intentional, more coordinated approach to cyber defense. For the Department of Defense, that means that USCYBERCOM will work with the interagency, private sector, and our partners and allies to deliver cyberspace options in combination with other kinetic and non-kinetic capabilities to deter, disrupt, and respond to malicious cyber actors.

Question. Do you believe it is important to adopt and articulate a cost-imposing deterrence strategy based on credible options for responding against targets that adversaries' value with offensive cyber operations to cyber attacks against U.S. critical infrastructure?

Answer. Cost imposition is one of three DOD approaches to deterrence—all are important. DOD's potential responses, however, should not be limited to the cyber domain. USCYBERCOM is participating in Department-wide and whole-of-government collaboration and coordination efforts to reduce the perceived and actual utility of cyber attacks on critical infrastructure, and USCYBERCOM is also collaborating with allies and partners to develop options to impose collective costs, leveraging the convergent power that remains a U.S. competitive advantage. As we implement the department's National Defense Strategy, our focus on integrated deterrence, campaigning, and building enduring advantage will support deterrence efforts to prevent strategic attacks, aggression, and defense of the homeland.

Question. In light of the conclusions of the Intelligence Community, what is your assessment that the PRC is currently deterred from conducting cyber attacks against United States critical infrastructure?

Answer. I assess that the PRC understands the potential for a high cost in response to a cyber attack against United States critical infrastructure during peacetime. However, during conflict, it remains a potential option for the PRC.

Question. In your view, how effective is U.S. Cyber Command's current deterrence posture, and are there areas for improvement?

Answer. The command supports the whole of government approach to deterrence in support of national security objectives. We implement our part on national strategic deterrence through the department's integrated deterrence effort and our role in providing cyberspace operations options to senior leadership. We can further enable this effort by investing in the resilience of the Department's Information Networks, enabling the defense of non-Department networks, building the cyber capacity of, and generating cyberspace options for, allies and partners, and investing in strategic cyberspace attack capabilities. We will also aggressively utilize our new enhanced budget and acquisition authorities to meet future deterrence needs with the continued support, sustainment, and growth of the CMF.

DUAL HAT

Question. Last year, the Director of National Intelligence and the Secretary of Defense conducted a study of whether to continue the "dual hat" arrangement whereby the Commander of U.S. Cyber Command also serves as the Director of the National Security Agency.

Do you believe that the dual hat arrangement should be maintained?

Answer. Yes, maintaining the dual hat arrangement enhances the effectiveness of both organizations and is in the best interests of the Nation. The signals intelligence and cyber operating environments substantially overlap. Eliminating the dual hat would reduce relevant visibility and understanding across both mission sets, increasing risk to intelligence sources and operational activities. It would reduce the speed and effectiveness of cybersecurity collaboration in the protection of National Security Systems (NSS), the DODIN, and the DIB by slowing and complicating information sharing and work with overlapping partners. Finally, ending the dual hat would complicate relationships with allies and partners that conduct their own signals intelligence and cyberspace operations.

Question. In your view, are the demands of both commanding U.S. Cyber Command and directing NSA overly stressing for a single official?

Answer. No, the demands of each position are effectively managed given the separate and distinct missions, authorities, and organizational structures senior leadership teams, staffs, and organizational structures of each organization.

Question. In your view, would it be as time-consuming and complex for separate NSA Directors and Commanders of U.S. Cyber Command to coordinate and integrate their mission sets and capabilities?

Answer. Yes. It would be more time consuming, more complex and less effective. Fracturing the current USCYBERCOM—NSA command arrangement would degrade flexibility, adaptability, and speed of action now provided through close and interconnected processes; ultimately impacting mission outcomes.

Question. If confirmed, what are your views on NSA's budgets and personnel subsidizing U.S. Cyber Command and the non-National Intelligence Program budget of the DOD?

Answer. All resources must be used for the purposes appropriated. NSA's budget and personnel do not subsidize USCYBERCOM. The Senior Steering Group that was commissioned to study the dual hat found that, although there have been perceptions in the past with respect to structure, budget, and oversight, any negative effects in these areas have been mitigated by agreements and processes now in place to ensure clear accountability, cost reimbursement, and oversight. If confirmed, one of my priorities would be to ensure that the teams at USCYBERCOM and NSA continue those best practices, and if necessary, buildupon the activities that have made those agreements and processes effective.

Question. If confirmed, what are your views on U.S. Cyber Command often gaining accesses to targets from NSA for military purposes that negates their significant value for NSA's national intelligence mission?

Answer. As a result of the overlap of the signals intelligence and cyber operations environments, NSA and USCYBERCOM have developed a close partnership in this area. Under the current leadership arrangement, a single, fully informed decisionmaker, responsible for the separate and distinct mission outcomes of both organizations, is able to protect our Nation's most sensitive signals intelligence equities while operating in defense of national interests and ensuring both organizations are aligned with the Nation's priorities. If confirmed, I will continue to utilize and improve processes for identifying and evaluating the sharing of accesses, where appropriate, from NSA to USCYBERCOM, from USCYBERCOM to NSA, and with other key partners, to deliver the best outcomes for the Nation.

Question. If confirmed, what are your views on U.S. Cyber Command preparing for or undertaking operations against targets due to objections that such actions would jeopardize intelligence collection? What are your views of such tradeoffs?

Answer. This is perhaps the most critical advantage of the dual hat—a single decisionmaker, responsible and accountable for the mission outcomes of both organizations, is best equipped to protect critical intelligence equities while executing national priorities, as directed. It ensures fully informed tradeoff decisions are made under accountability to both the Secretary of Defense and Director of National Intelligence.

Question. In your view, is the degree of support that U.S. Cyber Command receives from the NSA detrimental to the support that NSA provides to other combatant commands and to national policymakers?

Answer. No. The Senior Steering Group that was commissioned to study the dual hat found that, although there have been perceptions in the past with respect to structure, budget, and oversight, any negative effects in these areas have been mitigated by agreements and processes now in place to ensure clear accountability, cost reimbursement, and oversight.

CRYPTO MODERNIZATION

Question. In fiscal year 2022, the Joint Staff Director for Command, Control, Communications and Computer (C4)/Cyber, and Chief Information Officer refused to continue issuing waivers for cryptographic systems that NSA had determined were obsolete, vulnerable and should be replaced.

What is your understanding of the problems in the overall cryptographic system modernization program?

Answer. It is my understanding that there are two overarching challenges associated with cryptographic modernization across the Department. The first is that a significant portion of the existing cryptographic inventory is, by NSA's assessment, either obsolete or approaching obsolescence—meaning that it is within reach of today's technology and vulnerable to compromise by a meaning that it is within reach of today's technology and vulnerable to compromise by a

The second cryptographic modernization challenge, more vast in scope and scale, is proactively preparing for potential future realization of a sufficiently large quantum computer in adversary hands that could break public-key cryptosystems used within the U.S. and around the world.

Modernization efforts are focused on the elimination of the already vulnerable cryptography in use today and also ensuring that the DOD's cryptographic inventory is completely quantum resistant by the year 2034.

Question. In your view, has the Department of Defense made significant changes in the way that cryptographic modernization is overseen and managed that make that program more effective? Please explain your answer.

Answer. In light of the threat posed by technologically advanced near peer nation states, significant changes to the oversight of crypto modernization have occurred. DOD, under Joint Staff oversight, has made tremendous strides in completing and advancing cryptographic modernization across a number of systems. However, challenges remain with completing modernization on several operational systems due to their sheer volume of material and scale of operations. Military Department sponsors of systems that are not yet fully modernized from obsolete cryptography are required to provide plans, with resources aligned, to the Joint Staff outlining their path to full modernization. Joint Staff, with NSA support, then adjudicates the way forward.

Significant planning measures are underway in DOD and, via NSM–10, have also now begun for the Federal Government at large with the goal of full modernization across Government systems by 2035 (2034 for DOD). Though this end goal is 12 years away, success in the coming years will require continued, significant interagency coordination as well as alignment of budgetary and technical resources needed to accomplish the goal. The DOD CIO is coordinating an integrated DOD cryptographic modernization roadmap that will be delivered to OMB this summer.

Additionally, cryptographic modernization progress across DOD is reported quarterly to the DEPSECDEF.

Question. In your view, will the tracking and reporting requirements established in Section 1512 of the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023 (Public Law 117–263) significantly improve compliance with cryptographic modernization requirements? If not, what changes to those requirements might be needed to make it more effective?

Answer. There is certainly an expectation that Section 1512 of NDAA 2023 will be effective in driving compliance and reporting of cryptographic modernization progress, reinforcing and complementing directives already in place.

Question. If confirmed, what are your views on the pace of progress in developing and deploying quantum-resistant cryptographic solutions in the Department of Defense, in National Security Systems across the government, and in the private sector, as compared to the pace of progress of the development of quantum computers that would be able to break public key encryption?

Answer. An end goal of full post-quantum cryptographic modernization will touch the vast majority of today's cryptographic inventory, including commercial cryptographic technologies. In DOD and across the executive branch, this will affect almost every National Security System. NSM–10 establishes a goal of full post quantum cryptographic modernization by 2035 for the Federal Government. We believe this is a challenging, yet manageable, end goal, after which the risk accelerates in terms of the potential for adversary availability of a sufficiently large quantum computer. Within DOD, we have an excellent start and are working toward full modernization by 2034. NSA and the Military Departments issue cryptographic modernization roadmaps annually. DOD CIO, NSA, and the Military Departments are collaborating on delivering an integrated DOD cryptographic modernization roadmap and implementation plan later this Summer. At the Federal Government and commercial level, the National Institute of Standards and Technology (NIST) is aggressively leading the assessment and selection of commercially available quantum resistant cryptographic algorithms and protocols.

RADIO-FREQUENCY ENABLED CYBER OPERATIONS

Question. It is recognized that a wide variety of military systems may be vulnerable to cyber attacks through radio-frequency apertures. These systems include command and control networks, data links, sensor systems (both active and passive), weapons platforms and systems, and navigation systems. Section 1647 of the National Defense Authorization Act for Fiscal Year 2016 required the Department of Defense (DOD) to assess and remediate the cyber vulnerabilities of all major weapons systems. However, these assessments reportedly did not factor in the attack vector presented by radio-frequency apertures.

In your view, do you think that the Department of Defense is sufficiently focused on the threat posed by Radio-Frequency (RF) enabled cyber attacks?

Answer. The Department needs to be able to identify, characterize, and generate agile responses to all shapes and forms of threats, that include RF threats, based on intelligence driven assessments as well as assessments of individual weapons systems. RF-enabled cyber threats pose real risks to operation of weapons systems, but must be considered in context of a full risk analysis and addressed as part of system-wide mitigations.

Question. Do you think such threats should be addressed by such vulnerability assessment programs, such as the one mandated by Section 1559 of the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023 (Public Law 117–263)?

Answer. While the assessment programs defined in Section 1559 of the NDAA are a good start, the implementation and robustness of those assessment programs are key to accurate assessment of warfighter mission risk, and to applying full-spectrum mitigations. The most important value of the programs defined in Section 1559 will be informing overall cyber risk assessments of weapons systems and expanding the scope of potential mitigations against cyber threats.

Question. What are your views on the potential utility of tactical cyber forces able to deliver such non-kinetic effects?

Answer. Expeditionary cyber forces have already demonstrated potential to extend the reach of cyber enabling activities and close the gaps that limit cyber forces' ability to access important tactical targets in forward locations. If confirmed, I will work with the Services to ensure any tactical forces will meet USCYBERCOM training standards, follow Department deconfliction policies, and when leveraging USCYBERCOM authorities, ensure interoperability with Joint Cyber Warfighting Architecture.

Question. Do you think such forces should be service-retained and controlled by the geographic combatant commands or should they be part of the Cyber Mission Force under the command of U.S. Cyber Command? Please explain your answer.

Answer. If confirmed, I will work closely with the Services and geographic combatant commands as we study the issue to include training, standards, interoperability, and authorities to implement requirements under Section 1510 of the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, Integrated Non-Kinetic Force Development, to optimize the delivery of effects.

Question. In your view, do you think that cyber operations against tactical military systems will become more common in the future? If so, are we developing the technology and the operational concepts needed to enable such operations at an adequate pace?

Answer. Yes. The nature of modern network-centric warfighting is such that nearly every piece of electronic equipment represents a potential cyber-attack surface, to include tactical military systems. USCYBERCOM capabilities are always evolving to take advantage of cutting-edge technology, research, and development. Just as we continually improve our own defenses against novel cyber threats, so do our adversaries; if confirmed, it is my intent for the Command to seek new and innovative means, methods, and doctrine to achieve our mission and provide a comprehensive suite of non-kinetic effects when called upon to do so.

Question. In your view, will this lead to a higher valuation of the cyber mission by the combatant commands and the military services?

Answer. Yes. In my opinion, developing new and novel capabilities and approaches to deliver non-kinetic effects will benefit the Combatant Commands and the Services. The unique value of the cyber domain is that it crosses, supports, and enhances every warfighting domain by ensuring the secure operation of the Department's decisionmaking systems, disrupting malicious cyber actors' capabilities and ecosystems before they can threaten our networks and platforms, and, when called upon, deliver non-kinetic effects to enable Joint Force Commanders to achieve early initiative during contingencies.

ENHANCED BUDGET CONTROL (EBC)

Question. The National Defense Authorization Act for Fiscal Year 2022 (Public Law 117–81) included legislation that provided enhanced budget control (EBC) for the Commander of U.S. Cyber Command. This EBC authority included the ability to propose a budget for the cyber mission to the leadership of the Department of Defense.

In your view, what impact, if any, has the EBC authority had on the resources allocated to the cyber mission?

Answer. EBC authority allows USCYBERCOM to articulate cyber resource requirements directly into Department PPBE processes. EBC authority will allow USCYBERCOM to ensure resources for Cyber Mission Forces (CMF) are aligned with the USCYBERCOM Commander's priorities. These resources fund the CMF Teams, their operational headquarters, the Cyber National Mission Force Headquarters, the USCYBERCOM Headquarters, the cyber planning elements at each Combatant Command, and the development and fielding of the capabilities required by each of those organizations needed to conduct operations.

Question. In your view, is the increase in funding in the President's Budget Request for Fiscal Year 2024 a result of actions taken due to EBC invested in the Command?

Answer. The President's Budget Request for fiscal year 2024 includes increased funding for readiness, forces, and capabilities. Select programs with requested funding increases include: the Persistent Cyber Training Environment, continued growth of the Cyber Mission Force, and the Joint Common Access Platform.

Question. What is your understanding of the effectiveness of the transition to this new budget process?

Answer. This transition is ongoing. We effectively participated in the Department's process to build the President's Budget for fiscal year 2024. Funding the fiscal year 2024 budget request will allow USCYBERCOM to demonstrate competence in execution of EBC. Concerns remain about the impact of a fiscal year 2024 continuing resolution. A continuing resolution will delay the implementation of EBC and generate a significant amount of re-work based on the shift in appropriation between fiscal year 2023and fiscal year 2024.

Question. In your view, are there any indications that the military services will as a result of EBC reduce the level of support for the cyber mission in those areas where budget authority was not transferred to the Command, such as basic research and intelligence analysis?

Answer. USCYBERCOM has not seen any indications that the military services will reduce their level of support for the Cyber Mission Forces. We will continue to partner with the services in a number of areas, to include: the assignment and initial training of their military personnel, some administrative and logistics support for their teams, as well as basic research and intelligence analysis.

Question. What mechanisms do you have to monitor and respond if the services take such action?

Answer. There are a number of mechanisms that will allow USCYBERCOM to monitor and respond if the services reduce their level of support. We will have an opportunity to review each service's program and highlight any issues during DOD's program budget review process. We will also be able to engage with the Principal Cyber Advisor and the Chief Information Officer to monitor and respond to unanticipated reductions in the levels of support from the services.

CYBER FORCE

Question. Since the establishment of U.S. Cyber Command in 2010, Congress and the leadership of the Department of Defense have modeled the evolution of the Command on U.S. Special Operations Command. However, there has been some support for creating a separate Cyber Force, partly in response to persistent readiness problems.

What are your views on whether DOD should continue to mature U.S. Cyber Command according to the SOCOM model or instead create a separate cyber service? Please explain your answer in detail.

Answer. We have patterned USCYBERCOM after the U.S. Special Operations Command (USSOCOM) model that vests Service-like authority within a combatant command. USSOCOM has proven that this model is successful in leading a formidable capability for our Nation. Congress and the Department have set the conditions for U.S. Cyber Command to achieve this same success, leveraging expanded acquisition authorities and enhanced budget control to train and equip our cyberspace forces. These tools are just now coming to a point that will allow the command to ensure prioritization, resource allocation, and efforts to deliver the necessary cyber systems and capabilities. We should continue this approach to allow adequate time to see the results of these authorities in improving the readiness and capabilities of our cyberspace forces. Additionally, there are several statutorily required tasks from the fiscal year 2023 NDAA that are currently underway to examine readiness and force generation challenges. If confirmed, I will work with Congress to understand the results of these assessments and any associated recommendations for improving the USSOCOM-like model for U.S. Cyber Command.

Question. What are some of the potential downsides that could result from a decision to establish a separate cyber service?

Answer. The success of our operations to support the 2022 National Defense Strategy depends on training and readiness. We have prioritized improving the readiness of our cyber forces since USCYBERCOM became a unified Combatant Command in 2018, and there has been progress. With the passage of the fiscal year 2024 budget, USCYBERCOM will now have the USSOCOM-like authorities and resources to improve readiness and capabilities across the force. Changing course to stand up a new Cyber Service before allowing sufficient time for these authorities to impact readiness would be premature, necessitating significant additional resources and would actually detract from our efforts to improve readiness over the next 3–5 years.

Question. In your view, can DOD solve the readiness problem in the Cyber Mission Force units pursuant to legislative actions and direction from the Secretary and Deputy Secretary of Defense? Please explain your answer.

Answer. For USCYBERCOM, fiscal year 2024 is the first year USCYBERCOM will be able to fully realize the opportunities provided with the newly granted EBC and service-like authorities. The command will work with the Services to develop a strategy to increase and sustain readiness by prioritizing billets for CMF that require sustained, high fill rates from each service; codifying assignment policies that ensure at least two consecutive tours in the CMF; improving service-level training courses; providing consistent incentives across the services to recruit and retain the best cyber talent; and standardizing cyber readiness reporting requirements. If confirmed, I will brief Congress on the progress of these efforts and any further recommendations.

Question. Do you think that it is necessary to enhance the authority of the Commander of U.S. Cyber Command in the area of personnel policy, training, and retention in order to ensure stability in the readiness of the Cyber Mission Force? If so, what specific steps would you recommend?

Answer. At this time, I do not think it is necessary to enhance the authority of the Commander of USCYBERCOM in the area of personnel policy, training, and retention in order to ensure stability in the readiness of the Cyber Mission Force. Our service-like authorities allow the Commander to establish readiness standards for the Department and at the same time identify unique service initiatives that could be scaled into Departmental policy/practice.

IMPACT OF ARTIFICIAL INTELLIGENCE/MACHINE LEARNING

Question. Recent advances in Artificial Intelligence (AI) promise to enable the automation of sophisticated analysis of situations and conditions, and adept control of large numbers of complex machines and operations. Subject to appropriate human controls, in the cyber domain, AI may enable even modest numbers of cyber operators to achieve much greater levels of scale, speed and impact. However, in contrast, intelligence collection operations in cyberspace are generally characterized as slow, methodical, and manually intensive because of the care that must be taken to avoid detection. U.S. Cyber Command, having emerged from the U.S. signals intelligence (SIGINT) culture, remains strongly influenced by the SIGINT community's tactics, techniques, and procedures and emphasis on careful preparation and covert tradecraft.

Is there potentially a different model for operating in cyberspace that would be more conducive to the application of AI to achieve scale and speed in offensive cyber operations? For instance, could focusing on exploiting known vulnerabilities with existing, well-known tools make it easier for AI technologies to be adapted to helping orchestrate cyber intelligence and attack operations at greater rates and scales?

Answer. AI offers a wide range of new opportunities for operating in cyberspace. When applied to the cyberspace missions, AI has the potential to enhance exploitation of vulnerabilities, improve vulnerability research and access development, and accelerate the speed and scale of many aspects of conducting cyberspace operations. USCYBERCOM is in collaboration with partners across the Department to create the AI Roadmap and Implementation Plan for the Cyber Operations Force to determine how to most effectively utilize these new applications. As we begin executing enhanced budget control and acquisition authorities, CYBERCOM will be well postured to align and accelerate the delivery of AI capabilities to the warfighter.

Question. Alternatively, are recent advances in AI better suited to supporting defensive cyber missions, where spotting and correlating anomalous but ambiguous events in noisy environments is at a premium?

Answer. ill be a force multiplier for network defenders in threat hunting, incident response, terrain introspection, security compliance, patching, and the deployment of zero-trust policy engines. We have collaborated with NSA and our Service Cyber Components to leverage Commercial off the Shelf AI capabilities for malware analysis. USCYBERCOM continues to evaluate additional applications of AI in support of defensive cyberspace operations through the development of the AI Roadmap and Implementation Plan.

Question. What are your views about the potential impacts of AI on the future cyber threat, the information warfare threat, and military operations in cyberspace, and when would you expect to see them?

Answer. The enhancement of cyberspace operations with AI could be a disruptive technology change. Cyberspace operations enhanced by AI have the potential to achieve an accuracy and precision which were previously only attainable through skillful interaction between computer systems and human operators exercising strategic decisionmaking—at a competitively advantageous scale, speed, and rate of discovery. Sustaining a global advantage will require continual adoption and evolution of both the technology and the processes, doctrine, and culture of our organization.

Question. Are U.S. Cyber Command and the military services, and the defense agencies such as the Defense Advanced Research Projects Agency (DARPA), investing aggressively in AI technology in direct support to the cyber mission, and is there now a heightened awareness and acceptance of the significance of this technology for offensive and defensive cyber warfare, and information warfare more broadly?

Answer. USCYBERCOM is working to identify applications for an increased adoption of AI/ML technologies for the cyber mission. We are most mature in leveraging AI/ML techniques that are integrated in commercial off-the-shelf tools or services. Through the recently established Constellation pilot program, CYBERCOM will be able to more quickly leverage DARPA's investments in this area to mature and transition new cyber capabilities to the operational warfighter. USCYBERCOM is in collaboration to create the AI Roadmap and Implementation Plan for the Cyber Operations Force with DOD Chief Information Office (CIO), Chief Digital and Artificial Intelligence Office (CDAO), DARPA, NSA, OUSD(R&E), and other partners. We expect this to be transformative for our operations.

Question. In all of these cases, what data sources or repositories are needed to enable these activities? Is the problem one of better leveraging sources we already have, or developing all new data sources and repositories?

Answer. Computational infrastructure and data sources to meet current operational requirements with AI/ML analytics largely exist across USCYBERCOM and NSA systems. The Joint Cyber Warfighting Architecture (JCWA) programs are continually working to optimize data movement and system access to expand the use of AI/ML. Establishment of the JCWA Program Office will help facilitate efforts to optimize and better leverage our current architecture.

Question. How would you assess the AI capabilities of U.S. adversaries and near-peer competitors?

Answer. China and Russia are both pursuing AI to support military decision-making, weapons systems, and autonomous vehicles. Over the past decade, China has established a robust framework to bolster its AI and made contributions to the field on a global scale. Rapid changes in the technological environment will require the constant development of new and better approaches to collection, analysis, and dissemination of intelligence about these threats to maintain the safety of the Nation and our allies; this will be a priority for me if confirmed.

CYBER POSTURE REVIEW

Question. The Department of Defense (DOD) conducted a cyber posture review, including a gap analysis, in 2022 to inform the development of the DOD Cyber Strategy and future capability planning and funding.

In your view, what are the most significant findings of the posture review?

Answer. In my opinion, the most significant findings of the posture review relate to people, partners and capabilities. Beginning with people, USCYBERCOM must recruit and retain the talent to efficiently and effectively perform the mission. USCYBERCOM must better integrate partners across foreign military, intelligence, and the private sector to meet growing defensive requirements by burden sharing. Finally, USCYBERCOM must invest in developing capabilities to enhance flexibility and options for cyberspace operations.

Question. If confirmed, where in your priority list does addressing the gaps identified in the posture review fall?

Answer. If confirmed, my priorities are people, innovation, and partners. We have to work with the Services to bring in capable people, train them, and provide them

career opportunities to retain them. USYCBERCOM must invest in the technology, capabilities, and infrastructure necessary to support the joint force. Critical to the Department's success is the ability to build and maintain strong collaboration with the agency partners, industry, academia, and our allies and partners to counter the threats to our national security.

Question. Do you have any concerns with any significant findings and recommendations of the posture review?

Answer. The CPR highlights the use of our Cyber Protection Teams. USCYBERCOM's Cyber Protection Team is a capability that defends friendly networks, bolster tactics, technics, and produces, and enhance collaboration with allies and partners. This supports each of USCYBERCOM's enduring missions in cyberspace and mitigates attacks against the Department's networks, the Nation, and our allies and partners. We reviewed the CPR and have incorporated feedback to improve Cyber Protection Teams operations.

NATIONAL CYBER STRATEGY

Adversary Cyber Presence in the United States

T*Question.* he intelligence and military cyber forces of adversary nations such as Russia, China, Iran, and North Korea are effectively deployed and constantly operating inside the United States. However, the vast U.S. private and commercial cyberspace is largely a sanctuary for adversary cyber actors, allowing them to essentially deploy forces inside the United States and operate clandestinely. The March 2023 National Cybersecurity Strategy contends that the very technically proficient American commercial internet industry, with incentives and assistance, could provide a potent solution to this problem without impinging on privacy.

What is your assessment of the potential for the major U.S. Internet service providers and platforms, if incentivized and motivated, to prevent malicious cyber actors from abusing their platforms and services?

Answer. U.S. Internet Service Providers (ISPs) and platforms have an enormous responsibility and are faced with many challenges, to include the misuse and abuse of their infrastructure by foreign malicious cyber actors. Many ISPs already taken action to prevent and eradicate malicious cyber actors on their services, though more can be done. There are efforts being considered across the U.S. Government to review and implement incentives for the private sector to increase their level of cybersecurity for their products and services. NSA certainly plays a role in this effort by sharing information an ISP will need to identify foreign malicious activity in an effective and efficient manner and to educate the ISP cybersecurity personnel regarding what measures will be effective at mitigating the threats, thus reducing the resources required on the part of the company to better secure their platforms against misuse and abuse. If confirmed, I will partner with other Federal agencies and continue to work with service providers on this issue.

Question. How do you think the next iteration of the Cybersecurity Maturity Model Certification (CMMC) program that is in development may help improve the cybersecurity posture of businesses to defend against such malicious actors?

Answer. The theft of intellectual property from U.S. companies for both espionage and economic gains has long been a problem, especially within the Defense Industrial Base (DIB). These companies are critical to the defense of our Nation and the effectiveness of our warfighters. Therefore, it is imperative that we protect the sensitive information, operational capabilities, and product integrity created, housed, and used by the DIB to ensure the generation, reliability, and preservation of U.S. warfighting capabilities, and CMMC is a key tenet in this strategy. CMMC will ensure baseline security is in place for organizations supporting sensitive, but unclassified DOD programs, ensuring that a minimum standard be met prior to contract award. While advanced nation-State actors will continue to pursue ways into these networks and systems, CMMC could greatly diminish both the attack surface across the DIB, and the amount of time malicious cyber actors may spend in these networks before they are detected and eradicated, ultimately reducing data theft.

Question. In your view, how useful is the NSA Cybersecurity Collaboration Center in scaling this model by providing intelligence-and technology-driven cybersecurity assistance through open, collaborative partnerships with industry and the Department of Homeland Security?

Answer. antage point, I believe that NSA's Cybersecurity Collaboration Center (CCC) has made tremendous strides in scaling the public-private partnership model for collective cyber defense. The U.S. technology and cybersecurity sectors build, maintain, and defend the infrastructure upon which DOD, USG, and critical infrastructure operate. We find that many of these companies are motivated to keep those technologies secure from state-sponsored malicious actors. The CCC provides

information and context that helps inform and prioritize those efforts. Those companies also have unique insights through their routine business and are able to share those back with NSA to help inform its cybersecurity and foreign intelligence missions, creating an iterative communications cycle that improves the collective understanding of the actor, their activities, and ways to defend against them.

U.S. CYBER COMMAND ROLE IN DISRUPTION CAMPAIGNS

Question. The National Cybersecurity Strategy (March 2023) establishes the goal to "make malicious actors incapable of mounting sustained cyber-enabled campaigns that could threaten the national security or public safety of the United States" by disrupting and dismantling such actors.

In your view, would you expect that U.S. Cyber Command will be called upon to execute "sustained" offensive operations against cyber adversaries to disrupt their ability to conduct malicious operations, including operations to disrupt malicious activity before it effects its intended targets?

Answer. Yes, USCYBERCOM remains committed and ready to defend the homeland, support the Joint Force, and safeguard and advance U.S. national interests in and through the cyber domain. This requires USCYBERCOM to execute sustained cyber operations in campaigning with the combatant commands, the interagency, industry, and our allies and partners.

CYBER INTELLIGENCE CENTER

Question. Every operational domain other than cyberspace—land, sea, air, and space—has a dedicated Science and Technology and Foundational Intelligence Center. U.S. Cyber Command has concluded that the cyberspace operational domain also merits such an intelligence center.

What is your understanding of the result of the recent study on this topic by the Defense Intelligence Agency?

Answer. The offices of Undersecretaries of Defense for Intelligence and Security and Policy are engaged with DIA and USCYBERCOM for a review of the Command's requirement for foundational intelligence consistent with the support that every other Combatant Command receives from the Defense Intelligence Enterprise. Foundational intelligence in the domain of cyberspace is critical to conducting all of USCYBERCOM missions, and if confirmed, ensuring that Cyber Command's requirements are met will be a focus of mine.

Question. In your view, is such a center is necessary?

Answer. Yes. A consolidated Cyber Intelligence Science and Technology Center would close gaps in intelligence support to cyberspace operations. If confirmed, I will work with USD(I&S) and DIA to evaluate feasibility and executability of solutions to close these intelligence gaps.

Question. Do you think that NSA could provide much-needed technical intelligence if additional resources were available?

Answer. Yes. NSA's technical intelligence capabilities are superb. If confirmed, I will work with USD(I&S) to evaluate any additional resource requirements.

Question. In your view, would there still be a shortfall in the provision of all-source intelligence analysis?

Answer. Yes. The Intelligence Community is still maturing all-source analysis, particularly as it relates to Order of Battle of Cyberspace Forces and targeting in the cyberspace domain.

THE NATURE OF OFFENSIVE CYBER OPERATIONS IN A CONFLICT

Question. The NSA, as an intelligence agency, appropriately places the highest importance on remaining undetected, and accordingly invests in high-end—and therefore expensive and hard-to-develop—technical tools and tradecraft, following a deliberate methodology for developing and maintaining capability. U.S. Cyber Command, as a military combatant command, could in many circumstances have different interests and objectives. For example, it could seek the capability to act rapidly against targets for which there has been no time available to methodically access, and it may need tools and processes that can be used without fear of compromise during military operations. It could be argued that supported combatant commanders cannot wait weeks or months once a conflict has started for U.S. Cyber Command to be able to conduct follow-on operations to those which may have been pre-planned.

What are your views on these tradeoffs? Do you have any ideas for how to balance the competing institutional needs and goals for U.S. Cyber Command and NSA in this respect?

Answer. The most positive aspect of the dual hat is the ability of a single decisionmaker, responsible for the separate and distinct mission outcomes of both organizations, to allocate resources, set priorities, and execute complementary actions to produce critical outcomes for the Nation. It ensures that a single, fully informed decisionmaker is able to protect our Nation's most sensitive signals intelligence equities and ensure both organizations are aligned with the Nation's priorities.

Question. In your view, are there ways in which U.S. Cyber Command can operate effectively against meaningful targets in a conflict for which there has been no prior preparation?

Answer. Developing cyber capabilities in support of the Combatant Commanders in conflict is a key element of USCYBERCOM's mission. If confirmed, I welcome the opportunity to have a deeper discussion in the appropriate setting.

Question. In your view, should it be accepted that the most important offensive cyber contributions to combatant commanders' objectives in a conflict will be limited to a series of unique, pre-planned operations?

Answer. Developing cyber capabilities in support of the Combatant Commanders in conflict is a key element of USCYBERCOM's mission. If confirmed, I welcome the opportunity to have a deeper discussion in the appropriate setting.

ACQUISITION OF ACCESSES AND EXPLOITS AND THE JOINT CYBER WARFIGHTING ARCHITECTURE

Question. Congress transferred responsibility for acquiring the Joint Cyber Warfighting Architecture (JCWA) from military department executive agents in the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023 (Public Law 117–263).

In your view, is it critical to the success of the JCWA initiative that the military services sustain support for the JCWA programs until U.S. Cyber Command has acquired the workforce and acquisition expertise necessary to manage and integrate these programs effectively?

Answer. Yes, JCWA's success is predicated on support from all branches of the military. In conjunction with other stakeholders, USCYBERCOM is working to establish the Program Executive Office (PEO) JCWA, as directed in Fiscal Year 2023 NDAA Sec. 1509.

Question. What is your understanding of the military services commitment to providing that support until a suitable transition can be planned?

Answer. The military services have agreed to the establishment timeline, which will result in a PEO JCWA being fully operational by fiscal year 2027. Accordingly, the Army remains responsible for sustaining the Persistent Cyber Training Environment (PCTE) and Joint Common Access Platform (JCAP). The Air Force remains responsible for sustaining Unified Platform (UP) and Joint Cyber Command and Control (JCC2).

Question. In your view, is it critical that U.S. Cyber Command also receive support from the Secretary of Defense and Principal Staff Assistants to acquire the necessary acquisition expertise to manage the complex JCWA acquisition and integration challenges?

Answer. Yes. USCYBERCOM has received strong support from OSD(A&S) on this issue.

Question. If confirmed, are you confident that you will receive that support? What tools or processes will you have to monitor and enforce any support commitments that need to be sustained from the services?

Answer. Yes. USCYBERCOM will use enhanced budget control and different acquisition authorities to ensure continued support from the services. Beginning in fiscal year 2024, USCYBERCOM will meet with the service's program management offices (PMO) monthly to track fund execution status. In relation to acquisition, USCYBERCOM meets with the services PMOs quarterly to provide prioritized operational and engineering requirements for development. These regular engagements allow issues to be quickly identified and remedied.

Question. The Defense Advanced Research Projects Agency (DARPA) has volunteered, and U.S. Cyber Command accepted the offer, to provide a flow of software-based capabilities to the Command for integration into JCWA.

In your view, what are the important features and advantages of this initiative, both for the Command and DARPA?

Answer. The Constellation program aims to quickly transition technologies, capabilities, and prototype systems into JCWA to enable full spectrum cyberspace operations to deter, disrupt, and defeat adversary cyber actors, through close coordination between the cyber mission force (CMF), DARPA and the DOD S&T community. Through streamlined acquisition, assessment, approval, deployment processes, and

modern DevSecOps development processes, Constellation will enable the rapid and continuous delivery of cyberspace technologies, capabilities, and prototype systems to the warfighter.

Question. In your view, does U.S. Cyber Command have the necessary authorities and processes to acquire accesses and tools to support offensive and defensive capabilities from the private sector when the opportunity arises?

Answer. orities to acquire tools and capabilities from the private sector. I will continue to work with R&E on the evolving role of USCYBERCOM in the DOD S&T community to ensure USCYBERCOM is properly postured to provide the COF with the most advanced and extensive cyber capabilities.

Question. Does the Department possess the requisite relationships with private sector entities and vendors to rapidly acquire cyber capabilities? If not, what recommendations would you make to build those relationships?

Answer. USCYBERCOM has worked to establish and maintain its private-sector relationships, which are critical to our ability to rapidly acquire cyber capabilities. Through this continued utilization of our authorities, USCYBERCOM is able to leverage internal activities, as well as partner with other Department entities, in order to acquire cyber capabilities on a scale and tempo that supports our operations.

FORCE MIX OF CIVILIAN, MILITARY, AND CONTRACTOR PERSONNEL IN U.S. CYBER COMMAND

Question. In your view, describe any legal restrictions concerning whether a given position must be filled by military personnel, rather than a government civilian?

Answer. Determinations regarding how positions must be filled are made using the guidelines in

DEPARTMENT OF DEFENSE INSTRUCTION (DODI) 1100.22, POLICY AND PROCEDURES FOR DETERMINING

Question. Workforce Mix. Planners review mission requirements and organizational structure to determine the appropriate workforce mix. The guidelines in DODI 1100.22 identify which functions are inherently governmental, then determine which will be performed by DOD civilian employees, and which will or must be performed by military personnel.

What are the legal and policy parameters surrounding the use of contractor personnel for the execution of military cyber operations?

Answer. Contractor-provided services support a variety of important functions for USCYBERCOM. These functions encompass vital support to both the Command, and the CMF. DOD policy requires that military operations involving the planned use of destructive capabilities, including offensive cyber capabilities, must be performed by Federal military personnel, rather than civilian or contractor personnel. Civilian and contractor personnel may perform other cyberspace operations, including support to offensive cyber operations not meeting the policy requirement described above, although contractor personnel may not perform inherently governmental functions. It is essential that Federal military personnel and U.S. Government civilian employees maintain proper oversight and ensure inherently government functions are performed by government personnel.

Question. What do you believe is the appropriate force mix between civilian, military, and contractor personnel accounting for the mission, educational requirements, any legal restrictions, the ability to recruit and retain military personnel in this field, and career progression for cyber personnel?

Answer. As USCYBERCOM engages in worldwide operations, the mission will determine the necessary mix of Active forces, the Reserve component, DOD civilians, and contracted workforce to achieve our military objectives. We will continue our efforts to recruit well-trained and educated professionals.

USCYBERCOM continues to achieve the appropriate force mix. USCYBERCOM has received additional civilian employee allocations under the Joint Chiefs of Staff Joint Manpower Validation Board, and these will take the command staff to a mix of approximately 41 percent military members and 59 percent civilian personnel. This mix is appropriate given the specific functions of staff personnel.

Question. What recommendations might you make for policies to improve recruiting and retaining cyber military and civilian personnel to help reduce the increasing competition for these professionals with the commercial sector?

Answer. Future talent management, with a focus on recruitment, retention, and equipping warfighters in targeted areas, is part of the effort to retain a high-quality workforce. We are working with the Services and across the Command to identify recruiting practices to gain talent, which is innovation and enduring advantage. We

need motivated and talented people to serve our Nation, and USCYBERCOM continues its commitment to attract candidates with a wide range of backgrounds and experiences.

Congressional Oversight

Question. In order to exercise legislative and oversight responsibilities, it is important that this committee, its subcommittees, and other appropriate committees of Congress receive timely testimony, briefings, reports, records—including documents and electronic communications, and other information from the executive branch.

Do you agree, without qualification, if confirmed, and on request, to appear and testify before this committee, its subcommittees, and other appropriate committees of Congress? Please answer yes or no.

Answer.

Question. Do you agree, without qualification, if confirmed, to provide this committee, its subcommittees, other appropriate committees of Congress, and their respective staffs such witnesses and briefers, briefings, reports, records—including documents and electronic communications, and other information, as may be requested of you, and to do so in a timely manner? Please answer yes or no.

Answer. Yes.

Question. Do you agree, without qualification, if confirmed, to consult with this committee, its subcommittees, other appropriate committees of Congress, and their respective staffs, regarding your basis for any delay or denial in providing testimony, briefings, reports, records—including documents and electronic communications, and other information requested of you? Please answer yes or no.

Answer. Yes.

Question. Do you agree, without qualification, if confirmed, to keep this committee, its subcommittees, other appropriate committees of Congress, and their respective staffs apprised of new information that materially impacts the accuracy of testimony, briefings, reports, records—including documents and electronic communications, and other information you or your organization previously provided? Please answer yes or no.

Answer. Yes.

Question. Do you agree, without qualification, if confirmed, and on request, to provide this committee and its subcommittees with records and other information within their oversight jurisdiction, even absent a formal Committee request? Please answer yes or no.

Answer. Yes.

Question. Do you agree, without qualification, if confirmed, to respond timely to letters to, and/or inquiries and other requests of you or your organization from individual Senators who are members of this committee? Please answer yes or no.

Answer. Yes.

Question. Do you agree, without qualification, if confirmed, to ensure that you and other members of your organization protect from retaliation any military member, Federal employee, or contractor employee who testifies before, or communicates with this committee, its subcommittees, and any other appropriate committee of Congress? Please answer yes or no.

Answer. Yes.

[Questions for the record with answers supplied follow:]

QUESTIONS SUBMITTED BY SENATOR MAZIE K. HIRONO

SEXUAL HARASSMENT

1. Senator HIRONO. Lieutenant General Haugh, since you became a legal adult, have you ever made unwanted requests for sexual favors, or committed any verbal or physical harassment or assault of a sexual nature?

Lieutenant General HAUGH. No.

2. Senator HIRONO. Lieutenant General Haugh, have you ever faced discipline, or entered into a settlement, related to this kind of conduct?

Lieutenant General HAUGH. No.

EXTREMISM'S ROLE IN UNAUTHORIZED DISCLOSURES

3. Senator HIRONO. Lieutenant General Haugh, earlier this year the Department of Defense (DOD) suffered a major intelligence leak due to the actions of someone with a deeply troubling history of racist and violent remarks. Though not the norm,

what threat does domestic extremism pose to our national security and if confirmed, how would you lead U.S. Cyber Command (CYBERCOM) in defending against it?

Lieutenant General HAUGH. As reflected in the oath every service member takes, extremist activities are inconsistent with the responsibilities and obligations of military service. Active participation in extremist activity is prohibited. Extremist behavior undermines good order and discipline, erodes the effectiveness of the Command, and challenges national security. If confirmed, I will ensure leaders take appropriate steps to identify, intervene, and take appropriate actions to eliminate extremist behaviors if discovered within our ranks.

SECTION 702 ABUSES

4. Senator HIRONO. Lieutenant General Haugh, your predecessor has cited the Foreign Intelligence Surveillance Act (FISA) Section 702 authorization as critical to intelligence gathering for the military. Yet, there have been clear examples of Americans' 702 communications getting searched in inappropriate ways. With respect to these "backdoor searches" or "U.S. person queries," some discussed solutions are warrant requirements, statutory limits, greater judicial oversight, or prohibiting such queries entirely. Would any of these solutions—which would only affect the subsequent use of data already collected under existing section 702 authorities—prevent you from conducting your national security mission against foreign actors?

Lieutenant General HAUGH. My answer below is predicated on my current understanding of the issue, noting that in my current role I am not directly involved in the oversight of NSA's use of FAA Section 702.

It is my understanding that NSA's use of U.S. person query terms is limited, carefully controlled, and subject to robust internal and external oversight. Restricting NSA's authority to conduct queries using U.S. person query terms in section 702 data, including requiring a probable cause determination or prior FISC authorization on some or all such queries, would undermine the effectiveness of the tool for national security purposes. It would create a significant administrative burden and time delay in a process that is valuable particularly for its efficiency. When time is of the essence, such a change may require NSA to identify alternative means of locating critical foreign intelligence. In many circumstances, it would be extremely challenging, if not impossible, to pinpoint this information in time to protect U.S. national security interests, including victims of malicious cyber activity, hostages, or targets of malign activity by hostile foreign intelligence services.

As noted at the outset, this position is based on my current understanding. I also understand that the Administration and Congress are currently considering a variety of reforms to U.S. person queries into section 702 data. If confirmed, I look forward to studying this issue further and participating in those discussions.

5. Senator HIRONO. Lieutenant General Haugh, do you have recommendations for additional safeguards to prevent the abuse of data collected under section 702?

Lieutenant General HAUGH. If confirmed, I will be in a better position to evaluate the specifics of NSA's Section 702 compliance and oversight systems in order to offer recommendations for additional safeguards. I am aware that NSA has a robust compliance regime designed to ensure adherence to all statutory and procedural requirements, including those relating to section 702. I know NSA's workforce is dedicated to compliance with the laws and policies that govern NSA's missions, including its Section 702 activities. NSA has a dedicated corporate compliance organization, and has instilled a culture of compliance within its workforce. Based on my experiences, I know that NSA's compliance team is part of each stage of the analytic process—from initial targeting decision to review of the responsive content—supporting the mission and ensuring that NSA's culture of compliance is maintained day in and day out.

Additionally, NSA's Section 702 activities are overseen by an internal compliance organization as well as NSA's independent Inspector General. Every NSA Section 702 targeting decision is reviewed by the Department of Justice (DOJ), and NSA must report any incidents of non-compliance to DoJ and the Office of the Director of National Intelligence. DoJ attorneys investigate each potential incident of non-compliance, work with agencies to remediate any such instances, and report any incidents of non-compliance to the FISC and to Congress.

ENSURING ELECTION SECURITY

6. Senator HIRONO. Lieutenant General Haugh, if confirmed, you will have an important responsibility to help maintain our Nation's free and open democratic elections. In your prospective role, how would you prevent foreign actors from inter-

fering with our democratic process, whether through disinformation campaigns or cyber-attack?

Lieutenant General HAUGH. Foreign adversaries such as Russia, China, Iran and their proxies persistently use their cyber and disinformation capabilities to shape, target, and influence the United States democratic process. State-sponsored online influence operations are unremitting and increasingly sophisticated. In addition, developments in artificial intelligence could provide new opportunities to spread disinformation to U.S. audiences. If confirmed, I will uphold our focus on the election security mission to ensure USCYBERCOM and NSA continue to operate at the necessary speed and agility to persistently engage adversaries that seek to threaten our elections.

7. Senator HIRONO. Lieutenant General Haugh, how would you ensure that any information your team may discover gets passed to the relevant local election officials, who do not have security clearances?

Lieutenant General HAUGH. USCYBERCOM passes relevant, elections-related information to the appropriate Federal agency—typically DHS or FBI, which have established relationships with the states. The appropriate Federal agency then disseminates to the relevant local election officials.

CYBER WORKFORCE DEVELOPMENT AND RETENTION

8. Senator HIRONO. Lieutenant General Haugh, CYBERCOM has gained increased responsibilities for joint and advanced cyber operations training; but, CYBERCOM has little role in ensuring that trained talent is retained by the Services. How do you envision CYBERCOM conducting advanced cyber professional training and what changes are needed to ensure this cyber talent is retained by DOD?

Lieutenant General HAUGH. Using the authorities provided to the Command, USCYBERCOM works closely with the Services to resolve readiness challenges across the Cyber Mission Force (CMF). With the passage of the fiscal year 2024 budget, USCYBERCOM will increase its role under enhanced budgetary control, and the expanded role in acquisition Congress gave USCYBERCOM in the Fiscal Year 2023 National Defense Authorization Act (NDAA) will provide USCYBERCOM with the ability to provide additional supporting infrastructure for this training. As we progress under these expanded authorities, we will provide updates to Congress regarding our readiness and retention initiatives with the services under Section 1502 of the Fiscal Year 2023 NDAA. If confirmed, I commit to working with the Committee through regular updates and other reports to address challenges in resolving readiness and retention shortfalls.

QUESTIONS SUBMITTED BY SENATOR ANGUS S. KING, JR.

ACADEMIA PARTNERSHIP

9. Senator KING. Lieutenant General Haugh, collaboration and partnership between academia and the Department can bring about positive contributions for future research and activities. Places like the University of Maine and the Roux Institute at Northeastern, are doing amazing things in the world of cybersecurity, data analytics, systems modeling, network science, and artificial intelligence. How is CYBERCOM and the National Security Agency (NSA) partnering and leveraging academia to develop novel ideas and concepts along with the future cyber workforce?

Lieutenant General HAUGH. Academic partnerships are a critical enabler for the USCYBERCOM and NSA workforce in meeting challenges to our national security. The Academic Engagement Network (AEN) of colleges and universities at USCYBERCOM has grown to over one hundred colleges and universities. Through these partnerships, the Command leverages innovative thinking in cybersecurity, data analytics, artificial intelligence, networks, and modeling and simulation, which inform and equip our cyberspace forces to address our ever-changing national security challenges.

The National Security Agency (NSA) manages the National Centers of Academic Excellence in Cybersecurity (NCAE-C) program. This program aims to create and manage a collaborative cybersecurity educational program with community colleges, colleges, and universities that establishes standards for cybersecurity curriculum and academic excellence; addresses challenges facing cybersecurity education. There are more than 400 colleges and universities identified as NCAE-Cs, spanning 48 states, the District of Columbia, and Puerto Rico.

2023 AND 2024 NATIONAL DEFENSE AUTHORIZATION ACT REPORTING REQUIREMENTS

10. Senator KING. Lieutenant General Haugh, the 2023 and 2024 National Defense Authorization Act (NDAA) Senate Armed Service (SASC) reports require multiple CYBERCOM-related direct reports: (1) Election Security Group report (2023): This is a biennial report on CYBERCOM's efforts to ensure election security throughout the preceding Federal election cycle and a briefing to the committees on the election security threat assessment preceding each Federal election through the 2032 election cycle; (2) Classified Report (2023): Without going into detail, a classified report is required of CYBERCOM by the 2023 NDAA—I wanted to make sure the requirement was understood and on track at CYBERCOM; and (3) Cyber Personnel Readiness Report (2024): Calls for the service secretaries to report how they Man, Train, and Equip (MET) the 133 Cyber Mission Force (CMF) teams.

a. Please assure me you will comply with these reports and inform my staff and I when you brief the committee.

Lieutenant General HAUGH. Yes, you have my assurance.

b. Request your review of the classified reporting requirement from the Fiscal Year 2023 SASC Report 117–30 and provide me a followup assessment should you be confirmed.

Lieutenant General HAUGH. I have reviewed the reporting requirements and, if confirmed, will followup with my assessment.

c. Please provide an update on your assessment in preparedness for the next Federal election cycle.

Lieutenant General HAUGH. In my various positions leading election security efforts since 2018, I have seen the scale of our operations and our partnerships grow significantly. The sustained focus on this mission enables speed and agility with which we have been able to engage adversaries that threaten our elections. The resulting insight into adversaries' plans and intentions against U.S. elections helps secure election infrastructure and mitigate adversary activities, degrading and exposing adversary capabilities and operations. If confirmed, this will remain a priority.

d. Please provide your initial assessment on the progress the Services are making for providing trained and ready forces for CYBERCOM.

Lieutenant General HAUGH. We work closely with the Services to provide trained and ready forces to the CMF. Through their collaboration with each Service and routine dialog with the Service Chiefs and Principal Cyber Advisors, we assess quarterly progress on readiness and address issues in need of attention.

Under Section 1534 of the Fiscal Year 2023 National Defense Authorization Act (NDAA), the Command is working with the Department and the Services to develop a plan to improve recruitment and retention of our cyber teams. When combined with the annual report required by Section 1502 of the same NDAA, the Command will relay to Congress the outstanding challenges in readiness, and work with the Services to identify appropriate solutions.

QUESTIONS SUBMITTED BY SENATOR GARY PETERS

ELECTRONIC WARFARE/CYBERSPACE CONVERGENCE

11. Senator PETERS. Lieutenant General Haugh, as you're aware, my colleagues and I in Congress are heavily focused on electronic warfare issues. As head of CYBERCOM, you would be critical in facilitating electronic warfare operations across the Services. How can CYBERCOM take a more active role in helping to synchronize electronic warfare capabilities across the Joint Force, both in a training context and for real-world defensive and offensive operations?

Lieutenant General HAUGH. If confirmed, I will work closely with the Services as well as the combatant commands to ensure we meet the Fiscal Year 2023 NDAA requirement to develop a strategy for converged cyber and electronic warfare, specifically for service-retained assets. As evident within the conflict in Ukraine, both sides of the conflict have extensively engaged in military electronic warfare (EW) operations. The Services have deployed organic electronic warfare capabilities to support joint requirements, and USCYBERCOM closely coordinates with other combatant commands to synchronize EW capabilities on the battlefield. We must continue to plan and participate in large-scale, realistic, joint exercises to jointly operate in combat environments.

12. Senator PETERS. Lieutenant General Haugh, the Fiscal Year 2023 National Defense Authorization Act (NDAA) mandated requirements for the Department of Defense to develop a strategy for "converged cyber and electronic warfare" conducted by and through deployed military and intelligence assets operating in the radio fre-

quency domain to provide strategic, operational and tactical effects in support of combatant commanders. Given this mandate and your recommendations as the 16th Air Force Commander to converge and grow cyber and electronic warfare, how do you envision mandated collaborations between CYBERCOM, combatant commands (COCOMs), and the Services who have the primary task to man, train and equip forces with capabilities to deploy and employ cyber and electronic warfare capabilities abroad?

Lieutenant General HAUGH. If confirmed, I look forward to working with the Department and USSTRATCOM to develop a strategy for converged cyber and electronic warfare. The opportunities inherent in a more holistic view of the electromagnetic spectrum and cyberspace makes USCYBERCOM's role even more important as we seek to gain information advantage over our adversaries. Linking Combatant Commander requirements with our Service components ensures that future force development, including the capabilities of cyberspace and EW forces, are effective. This level of force integration contributes to the information advantage for the joint force and enables the responsibilities of USCYBERCOM as Joint Force Provider for cyberspace operations.

13. Senator PETERS. Lieutenant General Haugh, in the fiscal year 2023 budget, CYBERCOM requested $16.7 million to adapt electronic warfare technologies and cyber-peculiar capabilities to gain access to targeted enemy forces. With increased funding, how would you envision CYBERCOM supporting service requirements to build and expand electronic warfare capabilities to support COCOMs and their requirements to access hardened internet protocol (I.P.) tactical networks via close access radio frequency (R.F.) capabilities normally employed via electronic warfare tools and authorities?

Lieutenant General HAUGH. As Joint Force Provider for cyberspace operations, the Command monitors the capability and capacity of all units contributing to the fight in cyberspace. This includes our expeditionary cyberspace operations, which have collectively served as a force multiplier. With expanded acquisition and budget authorities starting in fiscal year 2024, USCYBERCOM will collaborate with Combatant Commands and the Services to identify requirements and solutions for RF-enabled capabilities.

QUESTIONS SUBMITTED BY SENATOR ROGER F. WICKER

NARRATIVE INTELLIGENCE

14. Senator WICKER. Lieutenant General Haugh, propaganda and foreign malign influence activities disseminated constantly on traditional media and social media by non-State actors and nation-State rivals undermines U.S. interests, exacerbates conflicts, and subverts democracy. Social media-enabled influence operations serve as a powerful force in shaping modern battlefields through activities short of kinetic warfare. The digital dimension, including, social media, and emerging domains of virtual and augmented reality change rapidly and may make it difficult for U.S. Agencies and, particularly, the Department of Defense to keep pace.

What are the key capability and resource needs (e.g. a skilled workforce, technology, or analytics) for operations in the information environment and countering foreign adversaries' malign influence campaigns against the United States population, systems, and processes?

Lieutenant General HAUGH. USCYBERCOM collaborates with partners in developing a coordinated effort to repel foreign actors' attempts to conduct malign influence activity against us. USCYBERCOM will continue to pair its skilled workforce with advanced technology and analytical capabilities. These resources will provide the synergy needed to remain ahead of foreign efforts in the information domain, while ensuring our actions protect the rights and civil liberties of U.S. citizens.

15. Senator WICKER. Lieutenant General Haugh, how are you working with colleges and universities to counter foreign malign influence against allies and U.S. institutions and systems?

Lieutenant General HAUGH. Through the Academic Engagement Network (AEN), USCYBERCOM works closely with colleges and universities to find innovative approaches to address the most pressing cyber challenges facing the Command. The National Security Agency (NSA) manages the National Centers of Academic Excellence in Cybersecurity (NCAE-C) program. There are more than 400 colleges and universities identified as NCAE-Cs, spanning 48 states, the District of Columbia,

and Puerto Rico. If confirmed, I will ensure we are leveraging both organizations' academic partnerships to counter foreign malign influence.

16. Senator WICKER. Lieutenant General Haugh, what resources do you need to counter foreign malign influence beyond additional funding?

Lieutenant General HAUGH. Most pressing is on time passage of the fiscal year 2024 defense appropriations bill. This legislation will fully enable USCYBERCOM's enhanced budget authorities. If confirmed, I will analyze USCYBERCOM's execution of our budget and authorities to determine if additional gaps remain.

QUESTIONS SUBMITTED BY SENATOR DAN SULLIVAN

NATIONAL SECURITY AGENCY HUNT FORWARD TEAMS

17. Senator SULLIVAN. Lieutenant General Haugh, a November 2022 press statement released by CYBERCOM detailed how U.S. Joint Forces, in close cooperation with the Government of Ukraine, conducted defensive cyber operations prior to Russia's invasion last year. According to CYBERCOM, hunt forward operations are purely defensive activities and are key to CYBERCOM's persistent international engagement strategy. Most recently, in early June of this year, hunt forward teams conducted their first engagements in the U.S. Southern Command (SOUTHCOM) area of responsibility (AOR). As our strategic competitors' cyber capabilities grow so must ours and those of our partners, I think hunt forward is an excellent initiative that will provide tremendous benefits to our national security. Can you describe how hunt forward teams were employed to support Ukraine?

Lieutenant General HAUGH. In response to a request for support, USCYBERCOM deployed hunt forward operators to work with our Ukrainian partners against malicious cyber activity on their networks. While hunt forward forces were on the ground, remote forces provided critical analytic and advisory support. Together, the combined forces analyzed adversary tactics and tools, sharing their findings with government and industry partners to bolster defense in both the U.S and other partner nations.

18. Senator SULLIVAN. Lieutenant General Haugh, how might hunt forward teams be employed in Taiwan?

Lieutenant General HAUGH. Hunt forward operations bring us closer to adversary activity and are key to protecting our networks and critical infrastructure against shared threats. These operations are mutually beneficial because they bolster the security of our partners and the U.S. When invited to hunt on partner networks, our combined forces discover malicious cyber activity, imposing costs on our adversaries by exposing their tools and tradecraft, and providing advance notice of adversary tactics that enable us and our allies and partners to harden our networks against these threats.

19. Senator SULLIVAN. Lieutenant General Haugh, do you see hunt forward teams enhancing our relationships with our U.S. Indo-Pacific Command (INDOPACOM) partners?

Lieutenant General HAUGH. USCYBERCOM works by, with, and through USINDOPACOM in our collaboration with partners in the Indo-Pacific area of operations. Our partnerships represent a unique, collaborative advantage and accelerate our partners' capacity to defend against cyber espionage and strategic attacks. In order to achieve this mission, the Command establishes secure communications and information sharing with our partners. Through this foundation, we keep our partners informed and align our actions, building an environment of enduring cybersecurity. Hunt forward teams are a part of this equation.

THE ROLE OF CYBER IN DETERRING A TAIWAN INVASION

20. Senator SULLIVAN. Lieutenant General Haugh, in General Paul Nakasone's testimony for CYBERCOM's fiscal year 2024 posture hearing, he identified CYBERCOM's fourth line of effort as "developing options for full-spectrum cyberspace operations to assist combatant commanders . . . to achieve their objectives." He further noted China was "building capabilities far in excess of its defense needs." Deterring, and if necessary defeating, a Chinese invasion of Taiwan is certainly one of INDOPACOM's objectives. A key Chinese capability to conduct such an invasion is the PLAN (People's Liberation Army Navy). The Secretary of the Navy has acknowledged we cannot match the output of Chinese shipyards and the PLAN is already numerically larger than the United States Navy. The PLAN also uses civilian

RO-ROs (Roll on/Roll Off) ferry vessels to practice the same type of amphibious operations it needs to conduct to invade Taiwan. What capabilities does CYBERCOM bring to the fight to help INDOPACOM achieve its objectives, specifically deterring and defeating a PLAN amphibious invasion of Taiwan?

Lieutenant General HAUGH. The ability to command and control forces is essential to any combatant commander and will be essential to USINDOPACOM in any contingency. Securing, operating, and defending DOD Information Networks will be critical and essential role in such a scenario. Additionally, USCYBERCOM, in support of INDOPACOM and in cooperation with its allies and partners, remains focused on deterring threats. Our efforts include defending forward and providing cyberspace options to the USINDOPACOM Commander. Enhanced Budget Control will ensure that the cyber mission force is organized, trained, equipped, and ready to address the challenges of the region, giving USCYBERCOM authorities to field capabilities necessary to deter aggression.

CYBER SECURITY IN THE ARCTIC

21. Senator SULLIVAN. Lieutenant General Haugh, receding sea ice in the Arctic has brought increased opportunity for access to the Arctic Ocean and with it new potential trade routes and access to natural resources. Our partners in the region have taken notice as have Russia and the People's Republic of China (PRC), who has declared itself a near Arctic State. Additionally, over the last year, Alaska, our Nation's gateway to the Arctic, has been the site of several attempted shows of strength by Russian Bear Bombers (Tupolev Tu–95) and likely collection efforts by PRC spy balloons. Relatedly, several of our Arctic partners have either already experienced or are bracing to experience cyber threats from our strategic competitors. At the appropriate classification level, what is your understanding of the cyber threat in the Arctic?

Lieutenant General HAUGH. Russia and the PRC have demonstrated their intent and capability in the cyber domain and their interest in the Arctic. Russia's cyber capabilities are particularly concerning given the significant United States energy, telecommunications, and transportation critical infrastructure and key resources (CI/KR) in the Arctic region. Similarly, Beijing's quest for a polar "silk road" and interest in becoming a "near-Arctic State," suggests cyber espionage will be a means to augment its intelligence collection activities to influence Arctic nations.

[The nomination reference of Lieutenant General Timothy D. Haugh, USAF follows:]

NOMINATION REFERENCE AND REPORT

PN678

AS IN EXECUTIVE SESSION,
SENATE OF THE UNITED STATES,
May 30, 2023.

Ordered, That the following nomination be referred to the Committee on Armed Services:

The following named officer for appointment in the United States Air Force to the grade indicated while assigned to a position of importance and responsibility under title 10, U.S.C., section 601:

To Be General

Lt. Gen. Timothy D. Haugh, 5791

_____, 2023.
(Date)

Reported by Mr. Reed _____
(Signature)

with the recommendation that the nomination be confirmed.

☐ **The nominee has agreed to respond to requests to appear and testify before any duly constituted committee of the Senate.**

[The biographical sketch of Lieutenant General Timothy D. Haugh, USAF, which was transmitted to the Committee at the time the nomination was referred, follows:]

BIOGRAPHY

UNITED STATES AIR FORCE

LIEUTENANT GENERAL TIMOTHY D. HAUGH

Lt. Gen. Timothy D. Haugh is the Deputy Commander, U.S. Cyber Command, Fort George G. Meade, Maryland. USCYBERCOM directs, synchronizes and coordinates cyberspace planning and operations to defend and advance national interests in collaboration with domestic and international partners. Prior to this assignment, Lt. Gen. Haugh served as Commander, Sixteenth Air Force; Commander, Air Forces Cyber, and Commander, Joint Force Headquarters-Cyber, Joint Base San Antonio-Lackland, Texas, where he was responsible for more than 44,000 personnel conducting worldwide operations.

Lt. Gen. Haugh received his commission in 1991 as a distinguished graduate of the ROTC program at Lehigh University. He has served in a variety of intelligence and cyber command and staff assignments. The general has commanded at the squadron, group, wing, numbered air force, and joint levels and served on staffs at major command, agency and combatant command headquarters. Lt. Gen. Haugh's previous joint general officer assignments include serving as the Commander, Cyber National Mission Force, and the Director of Intelligence, U.S. Cyber Command.

EFFECTIVE DATES OF PROMOTION

Second Lieutenant
December 09, 1991

First Lieutenant
December 09, 1993

Captain
December 09, 1995

Major
September 01, 2002

Lieutenant Colonel
March 01, 2006

Colonel
August 01, 2011

Brigadier General
November 02, 2016

Major General
August 30, 2019

Lieutenant General
October 11, 2019

EDUCATION
1991 Bachelor of Arts, Russian Studies, Lehigh University, Bethlehem, Pa.
1997 Squadron Officer School, Maxwell Air Force Base, Ala.
1999 Master of Science, Telecommunications, Southern Methodist University, Dallas
2005 Master of Science, Joint Information Operations, Naval Postgraduate School, Monterey, Calif.
2010 Master of Science, National Resource Strategy with a concentration in Information Operations, Industrial College of the Armed Forces, Fort Lesley J. McNair, Washington, D.C.

ASSIGNMENTS
1. June 1992–December 1992, Student, Signals Intelligence Officer Course, Goodfellow Air Force Base, Texas
2. January 1993–September 1995, Flight Commander, 301st Intelligence Squadron, Misawa Air Base, Japan
3. October 1995–July 1998, Commander, Detachment 2, 544th Intelligence Group, Sabana Seca, Puerto Rico
4. August 1998–June 2001, Chief, Information Operations Technology Integration, Headquarters Air Intelligence Agency, Kelly AFB, Texas
5. June 2001–June 2004, Information Operations Project Officer, headquarters U.S. Air Force, the Pentagon, Arlington, Va.
6. July 2004–September 2005, Student, Naval Postgraduate School, Monterey, Calif.
7. September 2005–June 2007, Director of Intelligence, Air Force Special Operations Forces, Hurlburt Field, Fla.
8. June 2007–June 2009, Commander, 315th Network Warfare Squadron, Fort George G. Meade, Md.
9. July 2009–June 2010, Student, Industrial College of the Armed Forces, Fort Lesley J. McNair, Washington, D.C.
10. June 2010–June 2011, Chief, Intelligence, Surveillance, and Reconnaissance Division, 609th Air Operations Center, Al Udeid AB, Qatar
11. July 2011–July 2013, Commander, 318th Information Operations Group, Joint Base San Antonio-Lackland, Texas
12. July 2013–June 2014, Assistant Vice Commander, Air Force Intelligence, Surveillance, and Reconnaissance Agency, JB San Antonio-Lackland, Texas
13. June 2014–May 2016, Commander, 480th ISR Wing, Joint Base Langley-Eustis, Va.
14. June 2016–June 2017, Deputy Commander, Joint Task Force-Ares, U.S. Cyber Command, Fort George G. Meade, Md.
15. June 2017–June 2018, Director of Intelligence, U.S. Cyber Command, Fort George G. Meade, Md.
16. June 2018–August 2019, Commander, Cyber National Mission Force, Fort George G. Meade, Md.
17. August 2019–October 2019, Commander, Twenty-Fifth Air Force, JB San Antonio-Lackland, Texas
18. October 2019–August 2022, Commander, Sixteenth Air Force; Commander, Air Forces Cyber, and Commander, Joint Force Headquarters-Cyber, JB San Antonio-Lackland, Texas

19. August 2022–present, Deputy Commander, U.S. Cyber Command, Fort George G. Meade, Md.

SUMMARY OF JOINT ASSIGNMENTS
1. June 2001–June 2004, Information Operations Project Officer, headquarters U.S. Air Force, the Pentagon, Arlington, Va., as a major
2. June 2007–June 2009, Commander, 315th Network Warfare Squadron, Fort George G. Meade, Md., as a lieutenant colonel
3. June 2010–June 2011, Chief, Intelligence, Surveillance and Reconnaissance Division, 609th Air Operations Center, Al Udeid Air Base, Qatar, U.S. Central Command, as a colonel
4. June 2017–June 2018, Director of Intelligence, U.S. Cyber Command, Fort George G. Meade, Md., as a brigadier general
5. June 2018–August 2019, Commander, Cyber National Mission Force, Fort George G. Meade, Md., as a brigadier general
6. August 2022–present, Deputy Commander, U.S. Cyber Command, Fort George G. Meade, Md., as a lieutenant general

MAJOR AWARDS AND DECORATIONS
Defense Superior Service Medal
Legion of Merit with two oak leaf clusters
Bronze Star Medal
Defense Meritorious Service Medal
Meritorious Service Medal with four oak leaf clusters
Joint Service Commendation Medal with three oak leaf clusters Air
Force Commendation Medal
Air Force Achievement Medal

EFFECTIVE DATES OF PROMOTION
Second Lieutenant Dec. 9, 1991
First Lieutenant Dec. 9, 1993
Captain Dec. 9, 1995
Major Sept. 1, 2002
Lieutenant Colonel March 1, 2006
Colonel Aug. 1, 2011
Brigadier General Nov. 2, 2016
Major General Aug. 30, 2019
Lieutenant General Oct. 11, 2019

(Current as of September 2022)

[The Committee on Armed Services requires certain senior military officers nominated by the President to positions requiring the advice and consent of the Senate to complete a form that details the biographical, financial, and other information of the nominee. The form executed by Lieutenant General Timothy D. Haugh, USAF in connection with his nomination follows:]

118th CONGRESS, 2023 -- 2024
UNITED STATES SENATE
COMMITTEE ON ARMED SERVICES
ROOM SR-228
WASHINGTON, D.C. 20510-6050

SENATE ARMED SERVICES COMMITTEE QUESTIONNAIRE
INFORMATION REQUESTED OF NOMINEES
FOR CERTAIN SENIOR MILITARY POSITIONS

INSTRUCTIONS TO THE NOMINEE: Answer all questions and provide all requested information. If more space is needed, attach an additional sheet of paper to the Questionnaire and cite the part of the Questionnaire and the question number (e.g., A-9, B-4) to which the continuation of your answer applies. Unless otherwise required, an answer of "yes", "no", or "not applicable" is appropriate.

QUESTIONNAIRE, PART A

NOTE: Information furnished in this part of the Questionnaire will be made available in Committee offices for public inspection prior to the hearing, if any, and will be entered in the hearing record, also available to the public.

BIOGRAPHICAL INFORMATION TO BE MADE PUBLIC

1. **Name (Include any former names you have used):** Timothy D. Haugh

2. **Position to which nominated:** Director, National Security Agency/Chief, Central Security Service/Commander, United States Cyber Command

3. **Date of nomination:**

4. **Government experience (List any advisory, consultative, honorary, and other part-time service or positions with Federal, State, or local governments, other than those listed in the service record extract provided to the Committee by the applicable agency/department/board):** None

5. **Business relationships (List all positions currently held as an officer, director, trustee, partner, proprietor, agent, representative, or consultant of any corporation, firm, partnership, or other business enterprise, and of any educational or other institution):** None

6. **Memberships (List all memberships and offices that you currently hold, as well as any memberships and offices you have previously held, in professional, fraternal, scholarly, civic, business, charitable, and other organizations):**
- Air Force Association, Member (active) - I enjoy no benefits as a result of my membership
- Armed Forces Communications and Electronics Association, Member (inactive) - I enjoy no benefits as a result of my membership
- Institute of Electrical and Electronics Engineers, Member (inactive) - I enjoy no benefits as a result of my membership
- Christ United Methodist Church, Member (active) - I enjoy no benefits as a result of my membership

7. **Honors and awards (List all scholarships, fellowships, honorary degrees, honorary society memberships, and any other special recognition received for outstanding service or achievements, in addition to those listed in the service record extract and biographical provided to the Committee by the agency or department):**
- Distinguished Graduate, Air Force ROTC, Lehigh University
- Honors Graduate, B.A., Russian Studies, Lehigh University
- Distinguished Graduate, Squadron Officer School, Maxwell AFB, AL

COMMITMENTS IN FURTHERANCE OF CONGRESSIONAL OVERSIGHT

NOTE: In order to exercise their legislative and oversight responsibilities, it is important that this Committee, its subcommittees, and other appropriate committees of Congress timely receive testimony, briefings, reports, records—including documents and electronic communications, and other information from the executive branch. A simple "yes" or "no" response is appropriate.

8. **Do you agree, if confirmed, and on request, to appear and testify before this Committee, its subcommittees, and other appropriate Committees of Congress?** Yes.

9. **Do you agree, if confirmed, and when asked before this Committee, its subcommittees, or other appropriate Committees of Congress to give your personal views, even if those views differ from the position of the Administration?** Yes.

10. **Do you agree, if confirmed, to provide this Committee, its subcommittees, other appropriate Committees of Congress, and their respective staffs such witnesses and briefers, briefings, reports, records—including documents and electronic communications, and other information, as may be requested of you, and to do so timely?** Yes.

11. **Do you agree, if confirmed, to consult with this Committee, its subcommittees, other appropriate Committees of Congress, and their respective staffs, regarding your basis for any delay or denial in providing testimony, briefings, reports, records—including documents and electronic communications, and other information requested of you?** Yes.

12. **Do you agree, if confirmed, to keep this Committee, its subcommittees, other appropriate Committees of Congress, and their respective staffs apprised of new information that materially impacts the accuracy of testimony, briefings, reports, records—including documents and electronic communications, and other information you or your organization previously provided?** Yes.

13. **Do you agree, if confirmed, and on request, to provide this Committee and its subcommittees with records and other information within their oversight jurisdiction, even absent a formal Committee request?** Yes.

14. **Do you agree, if confirmed, to respond timely to letters to, and/or inquiries and other requests of you or your organization from individual Senators who are members of this Committee?** Yes.

15. **Do you agree, if confirmed, to ensure that you and other members of your organization protect from retaliation any military member, federal employee, or contractor employee who testifies before, or communicates with this Committee, its subcommittees, and any other appropriate committee of Congress?** Yes.

[The nominee responded to Parts B-E of the committee questionnaire. The text of the questionnaire is set forth in the Appendix to this volume. The nominee's answers to Parts B-E are contained in the committee's executive files.]

SIGNATURE AND DATE

I hereby state that I have read and signed Parts A and B of the foregoing Senate Armed Services Committee Questionnaire, and that the information provided therein, and in any document appended thereto, is, to the best of my knowledge and belief, current, accurate, and complete.

TIMOTHY D. HAUGH
Lieutenant General, USAF

[The nomination of Lieutenant General Timothy D. Haugh, USAF was reported to the Senate by Chairman Reed on June 13, 2023, with the recommendation that the nomination be confirmed. The nomination was confirmed by the Senate on December 19, 2023.]

○