S. HRG. 118–100

OPEN HEARING: NOMINATIONS OF LT. GEN. TIMOTHY D. HAUGH TO BE DIRECTOR, NATIONAL SECURITY AGENCY, AND MICHAEL C. CASEY TO BE DIRECTOR, NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

HEARING

BEFORE THE

SELECT COMMITTEE ON INTELLIGENCE

OF THE

UNITED STATES SENATE

ONE HUNDRED EIGHTEENTH CONGRESS

FIRST SESSION

JULY 12, 2023

Printed for the use of the Select Committee on Intelligence

Available via the World Wide Web: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE

53–313 WASHINGTON : 2024

SELECT COMMITTEE ON INTELLIGENCE

(Established by S. Res. 400, 94th Cong. 2d Sess.)

MARK R. WARNER, Virginia, *Chairman*
MARCO RUBIO, Florida, *Vice Chairman*

DIANNE FEINSTEIN, California
RON WYDEN, Oregon
MARTIN HEINRICH, New Mexico
ANGUS S. KING Jr., Maine
MICHAEL F. BENNET, Colorado
ROBERT P. CASEY, Jr., Pennsylvania
KIRSTEN E. GILLIBRAND, New York
JON OSSOFF, Georgia

JAMES E. RISCH, Idaho
SUSAN M. COLLINS, Maine
TOM COTTON, Arkansas
JOHN CORNYN, Texas
JERRY MORAN, Kansas
JAMES LANKFORD, Oklahoma
MIKE ROUNDS, South Dakota

CHARLES E. SCHUMER, New York, *Ex Officio*
MITCH MCCONNELL, Kentucky, *Ex Officio*
JACK REED, Rhode Island, *Ex Officio*
ROGER F. WICKER, Mississippi, *Ex Officio*

MICHAEL CASEY, *Staff Director*
BRIAN WALSH, *Minority Staff Director*
KELSEY STROUD BAILEY, *Chief Clerk*

C O N T E N T S

JULY 12, 2023

OPENING STATEMENTS

WITNESSES

SUPPLEMENTAL MATERIAL

OPEN HEARING: ON THE NOMINATIONS OF LT. GEN. TIMOTHY D. HAUGH TO BE DIRECTOR, NATIONAL SECURITY AGENCY, AND MICHAEL CASEY TO BE DIRECTOR, NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

WEDNESDAY, JULY 12, 2023

U.S. SENATE,
SELECT COMMITTEE ON INTELLIGENCE,
Washington, DC.

The Committee met, pursuant to notice, at 2:33 p.m., in Room SH–216 in the Hart Senate Office Building, Hon. Mark R. Warner, Chairman of the Committee, presiding.

Present: Senators Warner (presiding), Rubio, Feinstein, Wyden, Heinrich, King, Bennet, Casey, Gillibrand, Ossoff, Risch, Cotton, Cornyn, Lankford, and Rounds.

OPENING STATEMENT OF HON. MARK R. WARNER, A U.S. SENATOR FROM VIRGINIA

Chairman WARNER. I'm going to call this hearing to order and want to thank you all for being here today. General Haugh, it's great to see you again. And Mike Casey, good to see you as always.

Congratulations on both of your nominations to be, respectively, the Director of the National Security Agency, or NSA, and the Director of the National Counterintelligence and Security Center, NCSC. I want to also recognize your families. I know General Haugh has got both his wife Sherie and his daughter here. And Mike has got his wife Sarah here. Although there are a series of former staff members from the SSCI, from both teams, I'm not sure whether they're here to root you on or fully disclose when we say if anyone here, you know, speak your peace or forever hold your peace—we'll see what happens at that point. But congratulations to both of you.

General Haugh is a career intelligence officer. He served for 31 years in the United States Air Force, the Joint Forces, and in the Intelligence Community. Currently, Deputy Commander of the United States Cyber Command, General Haugh previously served as Commander of the 16th Air Force, Commander of Air Force's Cyber, and Commander of Joint Force Headquarters Cyber at Joint Base San Antonio, where he was responsible for more than 44,000 personnel conducting worldwide operations.

General Haugh, you have an impressive background. You also have very big shoes to fill—as Senator Rubio and I said when we got with you yesterday—in replacing General Paul Nakasone. It

has been one of the great opportunities of my tenure, first as Vice Chair and now Chair, to work with General Nakasone. And we do wish him all the best. Obviously, as soon to be both head of the NSA and head of Cyber Command, you have enormous, enormous responsibilities. I look forward to hearing more from you about how you plan to make sure that NSA and Cyber Command are continuing to be poised to deal with a wide range of cyber issues, one of which is the China hack on Microsoft and the ramifications that has real time.

Obviously, Mike Casey, I'm not sure it's a good sign or not that so few Members from the Majority decided to show up for this hearing. But Mike needs no introduction to the Members or staff on the Committee. Former Chairman Feinstein brought over Mike from the House in 2016 and he served as staff director. When I came in as Vice Chair, I asked him to stay and then to stay on when I became Chair, and what a wild ride it has been. I think about our work with so many of the former staff who are here who worked on the bipartisan Russia investigation, which took enormous amounts of effort. And I think, generally his understated style and the fact that he knows virtually everything and everyone in the IC, has been a real asset to this Committee. And the fact that he has got the former staff director from the Republican side here is an indication, I think, of the kind of bipartisan approach that we desperately need. I think you'll be a great choice to be the Director of the NCSC.

We all know, the whole notion, in my mind, and a lot of the work on this Committee of national security is changing. It is no longer simply who has the most planes, ships, tanks, and guns. It really is—and again, this Committee has done a lot of good work on this—it is about technology competition, whether on subjects that are current interests, like AI. But it also includes quantum computing; it includes the work this Committee has done on 5G; it is a host of areas. Again, both of you will have responsibility in those domains.

Obviously, cyber becomes increasingly an enormous challenge in everything we do, not only on the national security side, but basically on the whole running of our economy. And we've got to make sure that we are well prepared, as we've seen, some of the interest we've seen in China's recent hack into Microsoft, these authoritarian regimes are not backing off in terms of the competition with us and competition with free nations around the world. Both of you are going to have responsibilities to take on this challenge, whether it be China, whether it be Russia. These are the issues that are not going away.

We also know—and this was something that again, this Committee—I'm proud of its work—took on a pretty unsexy topic a few years back: security clearance reform. We've got to make sure we continue to get the best and brightest people in an orderly process through a security clearance that both invites people in, but also does the appropriate background checks that we need to make sure the kind of incident that we had with the accused, Mr. Texeira, doesn't happen again. And again, many of us on this Committee are working on not only security clearance reform, but the whole notion of how many things are classified and how we go through

a more rational declassification process. So, I am very excited about both of your nominations. We're grateful for your potential service and for your family's willingness to be supportive. We believe that the Intelligence Community is the backbone of our national defense, and you are both going to play extraordinarily important roles, should you be confirmed. Very, very big jobs.

On a personal note, I just want to say to Mike, thank you for your help educating me in the Intelligence Committee. Thank you for your wisdom both to encourage me on some projects to take on and discourage me strongly on others. I'm grateful for that service. And I'm, well, reluctant to see you go. I think you're going to do an extraordinary job for our country going forward.

So, with that, I'll turn it over the Vice Chairman.

OPENING STATEMENT OF HON. MARCO RUBIO, A U.S. SENATOR FROM FLORIDA

Vice Chairman RUBIO. Well, thank you. But first of all, I always thank everyone that appears before us for their willingness to serve in these positions.

General, thank you for your service to our country writ large—to both of you really—because you've done that in public service in different ways. But now, your willingness to step up to these important roles. As the Chairman said, Mr. Casey is not a stranger to this Committee. And yet, despite the fact that he's so well known, I think he might even have a chance to be confirmed. So, we'll see as this plays out.

I think one of most interesting things about this hearing is it really goes to the very foundation of what this is all about—what we do in the Intelligence Community in our country. We spy on people, we spy on other countries particularly, and their leaders and their governments, and they try to spy on us. A lot of what we gain—and for the purpose of our national security, some of the most foundational intelligence this country has collected—continues to be through technical means. And that's what, General, you will be stepping up to do here. And it's critically important. It informs not just the IC and the Department of Defense. Frankly, it informs all kinds of public policy that allows them not just to see what's coming in a month or in a year, but what long-term trends could be like. Perhaps in this era, in which so much is interconnected through technical means, it is about the most foundational piece of intelligence that we collect on a regular basis and informs all the other agencies. It serves everyone in that regard.

And so, it's critically important to protect those capacities. As you know, we're coming up at the end of this year on the need to reauthorize what is basically at the heart and soul of our ability to collect on foreign targets: 702. And it's something I hope that the current Administration will prioritize their efforts to move on that, because we are running out of time here to get that done.

On the counterintelligence front, I think that's been as challenging as it's ever been for a long time. We are facing a return to an era of great power competition. It's a phrase that's thrown around a lot. I got here in 2010, when the singular focus, not just of this Committee but of the national security apparatus, was

counterterrorism. And it remains a challenge. But now it's increasingly about China and Russia, but also what's happening with North Korea, a rogue state with nuclear weapons. Iran and its ambitions. This emerging alignment of countries around the world who may not be our enemies, but who aren't going to be our allies and are looking for different ways to leverage the international stage to their advantage and play both sides.

But embedded in that is a real counterintelligence challenge for two reasons. The first is, with great power comes the ability to also do technical collection. But the other is that it's increasingly challenging for us because propaganda and disinformation and influence operations have existed in the case of every war fought in the last, you know, 5,500 years of recorded history. But never before have they been so easy to do at such a low cost. And I think that is in the realm of counterintelligence—the effort to drive messages that divide and pit Americans against each other, that seed information into our ecosystem in which free speech is protected by our Constitution, in ways designed to demoralize and undermine our willingness to fight and, in many ways, our capability to unite behind important causes. And that has to be balanced with the reality that we still need to ensure that our intelligence agencies can never be turned upon our citizens. In fact, the worst moments, the most dangerous moments in the history of our Intelligence Community have been when it was revealed that they were spying on people who were against the Vietnam War. Our political enemies are those in office—I'm not talking about now; I'm talking about the sixties, seventies, and eighties—to the point where those revelations almost destroyed our intelligence agencies in our country.

So, whether it's the foundational elements of our intelligence collected through technical means, or our ability to withstand not just great power competition in terms of counterintelligence, but the influence operations of not-so-great powers, but who have the ability to do that, whether it's through cut-outs, through different methods that they use, we face unique challenges that look very different than they did ten years ago, and that are rapidly evolving. So, you're both stepping into these roles at a critical time for our country, for the future of geopolitics.

I'm thankful for your willingness to serve and look forward to hearing your testimony and answers today.

Chairman WARNER. I thank the Vice Chairman.

General Haugh and Mr. Casey, I'm going to ask you both to stand and raise your right hands.

Do you solemnly swear to give this Committee the truth, the full truth, and nothing but the truth, so help you God?

General HAUGH. Yes.

Mr. CASEY. Yes.

Chairman WARNER. Please be seated.

I will now go about asking you the five standard questions the Committee poses to each nominee who appears before us. Actually, I'm not sure whether these five questions started with you, Mike, or with you, Chris. But all things come around. They just require a simple yes or no answer for the record.

One. Do you agree to appear before the Committee here or in other venues when invited?

General HAUGH. Yes.

Mr. CASEY. Yes.

Chairman WARNER. Two, if confirmed, do you agree to send officials from your office to appear before the Committee and designated staff when invited?

General HAUGH. Yes.

Mr. CASEY. Yes.

Chairman WARNER. Three, do you agree to provide documents and other materials requested by the Committee in order to carry out its oversight and legislative responsibilities?

General HAUGH. Yes.

Mr. CASEY. Yes.

Chairman WARNER. That's an important question. We had some challenges on that more recently.

Four, will you both ensure that your office and your staff provide such materials to the Committee when we request it?

General HAUGH. Yes.

Mr. CASEY. Yes.

Chairman WARNER. And five, do you agree to inform and fully brief to the fullest extent possible all Members of this Committee on intelligence activities and covert action, rather than only the Chair and Vice Chair?

General HAUGH. Yes.

Mr. CASEY. Yes.

Chairman WARNER. Thank you very much, General Haugh and Mr. Casey.

We'll now proceed to your opening statements, after which I'll recognize Members by seniority for five minutes each for questions.

The floor is yours, gentlemen.

STATEMENT OF LT. GEN. TIMOTHY D. HAUGH, NOMINEE TO BE DIRECTOR, NATIONAL SECURITY AGENCY

General HAUGH. Chairman Warner, Vice Chairman Rubio, and distinguished Members of the Committee. I am honored to testify today for my nomination as Director of the National Security Agency and Chief, Central Security Service. I want to thank President Biden, Secretary Austin, Director Haines, and General Milley for their trust in nominating me for these critical positions.

I'd also like to thank my bride, Sherie, who has served with me for the last 31 years. I would also like to thank our children, Michael and Chandler, who sacrificed as military children and 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. Sherie and I are incredibly grateful for their sacrifices to enable our service as a family.

I also would like to thank General Nakasone and Susan Nakasone for their service to the National Security Agency. General Nakasone has 36 years of dedicated service culminating as Director of NSA for the last five years. His commitment to both the mission and the people during a time of unparalleled global change has continued the legacy captured in the Agency's watchwords, "Defend the Nation, Secure the Future." I truly believe the Nation is defended and the future is secure 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 Army and Agency spouses and families.

I am a career intelligence officer who has served 31 years in the United States Air Force, within the Joint Force, and the Intelligence Community. My service in command and staff positions at all levels, to include multiple assignments within NSA and the cryptologic enterprise, have given me a deep appreciation of NSA's critical importance to the Nation. I am honored to have been nominated to lead NSA and serve with its incredibly talented professionals.

NSA's excellence in signals intelligence and cybersecurity create unparalleled advantage for the Nation. If confirmed, my focus will be to strengthen that advantage. As our Nation's competitors seek to reshape the international order and challenge our military advantages, we must leverage our competitive strengths: people, innovation, and partnerships.

I believe every great success starts with the people. NSA has great people and an incredible mission. To sustain that success, NSA must continue to attract diverse talent from across the Nation while also providing the environment where they can thrive and develop. If confirmed, I will ensure that whether an individual stays for a few years or dedicates their entire professional career to NSA, people will continue to be our foundation and legacy.

Technology continues to advance at an incredible rate. I have always been impressed with how NSA successfully innovates to remain on the cutting edge of technological advances. Its culture of innovation, its highly skilled workforce, and its record of success in applying artificial intelligence and advanced computing posture it well to adapt and apply the latest technologies to further advance its mission. Throughout NSA's history it has learned the great value of partnerships, a lesson significantly reinforced by recent experiences in response to Russia's unlawful invasion of Ukraine, and by initiatives to meet the near- and long-term challenges of the PRC. 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.

If confirmed, I will focus on ensuring the health and effectiveness of NSA and its world-class employees in delivering outcomes against national priorities, by delivering foreign intelligence, ensuring cybersecurity, protecting national security systems, and providing combat support to the Department of Defense. I will focus on strengthening the workforce, ensuring a culture of compliance, investing to leverage new technologies, and prioritizing threats facing the Nation, especially the pacing challenge posed by the People's Republic of China.

In closing, I am humbled and honored to be considered for these positions. The Nation faces challenges at unprecedented scale. If confirmed, I look forward to teaming with this Committee to posture ourselves to quickly seize opportunities to meet and outmaneuver those challenges.

Chairman Warner, Vice Chairman Rubio, and Members of the Committee, thank you for the opportunity to be here this afternoon. I look forward to answering your questions.

[The prepared statement of the nominee follows:]

Lieutenant General Timothy D. Haugh
SSCI Nomination Hearing – Opening Remarks
12 July 2023

Chairman Warner, Vice Chairman Rubio, and distinguished members of the Committee, I am honored to testify today for my nomination as Director of the National Security Agency, and Chief, Central Security Service.

I want to thank President Biden, Secretary Austin, Director Haines, and General Milley for their trust in nominating me for these critical positions.

I'd also like to thank my bride Sherie, who has served with me for the last 31 years. I would also like to thank our children, Michael and Chandler, who sacrificed as military children and 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. Sherie and I are incredibly grateful for their sacrifices to enable our service as a family.

I want to thank General Nakasone and Susan Nakasone for their service to the National Security Agency. General Nakasone has 36 years of dedicated service culminating as DIRNSA 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 Agency's watchwords – Defend the Nation; Secure the Future. I truly believe the nation is defended and the future is secure 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 Army and Agency spouses and families.

I am a career intelligence officer who has served 31 years in the Air Force, the Joint Force and the Intelligence Community. My service in command and staff positions at all levels, to include multiple assignments within NSA and the cryptologic enterprise, have given me a deep appreciation of NSA's critical importance to the nation. I am honored to have been nominated to lead NSA and serve with its incredibly talented professionals.

NSA's excellence in Signals Intelligence and Cybersecurity create unparalleled advantage for the nation. If confirmed, my focus will be to strengthen that advantage. As our nation's competitors seek to reshape the international order and

challenge our military advantages, we must leverage our competitive strengths – people, innovation, and partnerships.

I believe every great success starts with the people. NSA has great people and an incredible mission. To sustain that success, NSA must continue to attract diverse talent from across the nation while also providing the environment where they can thrive and develop. If confirmed, I will ensure that whether an individual stays for a few years or dedicates their entire professional career to NSA, people will continue to be our foundation and our legacy.

Technology continues to advance at an incredible rate. I have always been impressed with how NSA successfully innovates to remain on the cutting edge of technological advances. Its culture of innovation, its highly skilled workforce, and its record of success in applying artificial intelligence and advanced computing posture it well to adapt and apply the latest technologies to further advance its mission.

Throughout NSA's history it has learned the great value of partnerships, a lesson significantly reinforced by recent experiences in response to Russia's unlawful invasion of Ukraine and initiatives to meet the near and long term challenges of the People's Republic of China (PRC). 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.

If confirmed, I will focus on ensuring the health and effectiveness of NSA and its world-class employees in delivering outcomes against national priorities by delivering foreign intelligence, ensuring cybersecurity, protecting national security systems and providing combat support to the Department of Defense. I will focus on strengthening the workforce, ensuring a culture of compliance, investing to leverage new technologies, and prioritizing threats facing the nation -- especially the pacing challenge posed by the PRC.

In closing, I am humbled and honored to be considered for these positions. The nation faces challenges at unprecedented scale – if confirmed, I look forward to teaming with this committee to posture ourselves to quickly seize opportunities to meet and outmaneuver those challenges. Chairman Warner, Vice Chairman Rubio, and members of the Committee, thank you for the opportunity to be here this afternoon. I look forward to answering your questions.

STATEMENT OF MICHAEL C. CASEY, NOMINEE TO BE DIRECTOR, NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

Mr. CASEY. Mr. Chairman, Mr. Vice Chairman, Members of the Committee. I'm honored to appear before you as the nominee to be Director of the National Counterintelligence and Security Center. I'm deeply grateful to President Biden for nominating me for this position and to Director of National Intelligence Haines for her recommendation.

Like all of us, I'm only here because of the support and efforts of others. I'd like to thank in particular my parents, Robert and Carol Casey, for raising my brother, sister, and me and instilling in us a desire to do the right thing, work hard, and make a difference. My father passed away last year, but without the example he set for me throughout his life, I would not be here. My wife, Sara McLean, who's sitting behind me, and my daughter, Erin, who could not be here, have been unstinting in their support for my career. And as I've moved through this process, I really couldn't do it without them.

I'd also like to thank those Senators and Members of the House who brought me onto Capitol Hill and provided examples of what true public service really looks like. I began my service 28 years ago in the House working for Representative Carrie Meek and then Representative Vic Snyder. From them, I learned what Members dedicated to helping their constituents and making hard decisions look like.

Chairman Ike Skelton asked me to join the House Armed Services Committee and entrusted me with responsibilities far in excess of what I deserved.

Ranking Member Adam Smith, one of the smartest Members of the House, provided the constant example of how the best Members struggle with the difficult issues and do their best to make the right choices for the country.

Seven and a half years ago, Senator Feinstein asked me to join the staff of this Committee as the then-Minority Staff Director. I remain deeply grateful to her for giving me that opportunity.

And I'd like to single out Chairman Warner for thanks. He kept me on as a staff director when he ascended first to Vice Chairman and then Chairman of this Committee. As everyone here knows, he's one of the most energetic and dedicated Members of the Senate, constantly interested in pushing to find new ways to do more to help the country, often much faster than the Senate or the entire United States government is capable of handling. Thank you for never accepting that there are limits to what we accomplished if only we push a little bit more.

I've been fortunate to serve as a member of two excellent committee staffs; that is, the House Armed Services Committee and now the Senate Select Committee on Intelligence. From the moment I started until the day I left, I never stopped learning from the other staff members on HASC, who were always among the most professional and experienced staff members I've ever met. Serving as the minority staff director and now staff director of this Committee has been one of the greatest honors of my life. It's not always been a smooth ride. But the staff on both sides of the aisle

have struggled to always do it right and provide bipartisan, effective oversight of the Intelligence Community, almost always in ways that the public will never hear about but would deeply appreciate if they did.

I'd be remiss if I didn't thank the current and former Members of this Committee for their work also. Joining SSCI is often thankless, resisted by your personal offices and your campaign staff, and no one who isn't dedicated to ensuring U.S. national security would never agree to do this. Former Chairman Burr probably provided the best example of this, dedicating almost his entire time in Congress to serving on the intelligence committees, and spending untold hours with the men and women in the IC, working constantly to make the community better.

Finally, I'd like to take a moment to thank the men and women of the Capitol Police who guard the doors of the Committee and more importantly, become part of the SSCI community. The Committee couldn't function without them, and we don't remember that often enough.

I've spent my entire professional life in public service on Capitol Hill, working almost exclusively on national security issues—from the war in Iraq to Afghanistan, terrorism, Iran sanctions, covert action, and the other important matters this Committee works on but can never talk about. I'm particularly proud of the work this Committee undertook, in which I played a small part, to investigate the Russian interference in the 2016 election. When we started, I don't think we envisioned that it would take three and a half years and become a definitive counterintelligence look at that episode.

As it turned out, counterintelligence has become a growth business for this Committee and the entire country as we face an unprecedented level of threats from foreign actors. In addition to the traditional intelligence threat posed by Russia and other foreign intelligence services dedicated to sealing government secrets, a broad array of other hostile actors has emerged. China's ongoing and massive effort to steal U.S. intellectual property and that of our allies threatens the basis of our past success and economic future. North Korea has become a center of hacking for profit. And at the same time, Iran has expanded its own cyber capability, as well as showing its ability in traditional espionage. And of course, non-government groups like hackers not only steal for profit, but we've seen them rent or lend their services to governments.

These threats and many others I didn't name will only be exacerbated by emerging technology. We're already seeing how artificial intelligence can enhance malign influence efforts and potentially assist hackers in their efforts. Other technologies, like quantum or synthetic biology or autonomous systems, could have similar impacts. At the same time, those emerging technologies, and many others like advanced energy, are essential for the economy of the future and continued U.S. success in the world.

The National Counterintelligence and Security Center at ODNI sits at the center of many of the efforts to combat these threats and protect emerging technology, leading and supporting critical counterintelligence and security efforts across the IC, the United States government, and even the private sector. If I am fortunate enough to be confirmed as Director of the National Counterintelligence and

Security Center, I will seek to ensure that our Nation's counterintelligence efforts are integrated and effective; accelerate the work currently underway; and, I might add—strongly encouraged by this Committee—to reform the security clearance process, enhance ongoing efforts across the United States government to protect our supply chains—especially in the digital space, and continue the important work started by past directors of this Committee to educate the private sector and academia on the threats they face from foreign actors, and to help those private sector and academic institutions protect themselves.

Mr. Chairman, Mr. Vice Chairman, Members of the Committee, thank you again for your consideration of my nomination. I look forward to your questions.

[The prepared statement of the nominee follows:]

Statement for the Record
Michael C. Casey
Nominee for the position of the Director of the National Counterintelligence and Security Center
7 July 2023

Mr. Chairman, Mr. Vice Chairman, members of the Committee, I am honored to appear before you as the nominee to be the Director of the National Counterintelligence and Security Center.

I am deeply grateful to President Biden for nominating me for this position and to Director of National Intelligence Haines for her recommendation.

Like all of us, I am only here because of the support and efforts of others. I would like to thank in particular, my parents, Robert and Carol Casey, for raising my brother, sister, and me and instilling in us a desire to do the right thing, work hard, and make a difference. My father passed away last year, but without the example he set for me throughout his life, I would not be here.

I would also like to thank those Senators and members of the House who brought me onto Capitol Hill, and in multiple different, but important ways provided examples of what dedicated public service looks like. I began my service 28 years ago in the House, working for Representative Carrie Meek and then Representative Vic Snyder. From them I learned what members dedicated to helping their constituents and making hard decisions look like. Chairman Ike Skelton asked me to join the House Armed Services Committee and entrusted me with responsibilities far in excess of what I deserved. Ranking Member Adam Smith, one of the smartest members of the House, provided a constant example of how the best members struggle with the difficult issues and do their best to make the right choices for the country.

Seven and a half years ago, Senator Feinstein asked me to join the staff of this Committee as the then Minority Staff Director. I remain deeply grateful to her for giving me that opportunity.

I would like to especially single out Chairman Warner for thanks. He kept me on as his staff director when he ascended first to Vice Chairman and then Chairman of the committee. As everyone here knows, he is one of the most energetic and dedicated members of the Senate, constantly interested in pushing to find new ways to do more to help the country, often much faster than the Senate, or the entire US Government, is currently capable of handling. Thank you for never accepting that there are limits of what can be accomplished, if only you push a little more.

I have been fortunate to serve as a member of two excellent committee staffs—that of the House Armed Services Committee and now that of the Senate Select Committee on Intelligence. From the moment I started to the day I left, I never stopped learning from the other staff members on HASC who were always among the most professional and experienced staff members I ever met. Serving as the Minority Staff Director and now Staff Director of this committee has been one of the greatest honors of my life. It has not always been a smooth ride, but the staff, on both sides of the aisle, have struggled to always do it “right” and provide bipartisan, effective oversight of

the Intelligence Community, almost always in ways that the public will never hear about, but would appreciate deeply if they did.

I would be remiss if I did not thank the current and former members of this committee for their work also. Joining SSCI is often thankless, resisted by your personal offices and campaign staff, and no one who isn't dedicated to ensuring US national security would ever agree to do it. Former Chairman Burr probably provided the best example of this, dedicating almost his entire time in Congress to serving on the Intelligence Committees, spending untold hours with the men and women in the IC, and working constantly to make it better.

Finally, I would like to thank the men and women of the Capitol Police who guard the doors of the committee and, more importantly, become part of the SSCI community. This committee could not function without them, and we do not remember that enough.

I have spent my entire professional life in public service on Capitol Hill, working almost exclusively on national security issues, from the War in Iraq, to Afghanistan, terrorism, Iran sanctions, to covert action and the other important matters this committee works on, but can never talk about.

I am particularly proud of the work this committee undertook, in which I played a small part, to investigate the Russian government's efforts to interfere in the 2016 election. When we began the effort, I don't think we envisioned that it would take 3 and a half years and become the definitive counterintelligence look at that episode.

As it turns out, counterintelligence has become a growth business for this committee, and the entire country, as we face an unprecedented level of threats from foreign actors. In addition to the "traditional" intelligence threat posed by Russia and other foreign intelligence services dedicated to stealing the government's secrets, a broad array of other actors has emerged that require addressing. China's ongoing, and massive, effort to steal US intellectual property and that of our allies threatens the basis of our past success and economic future. North Korea has become a center of hacking for profit, at the same time as Iran has expanded its own cyber capability as well as shown its capability in traditional espionage. And of course, non-government groups like hackers not only steal for profit, but we have seen them rent or lend their services to hostile governments.

These threats, and the many others I did not name, will only be exacerbated by emerging technology. We're already seeing how artificial intelligence can enhance malign influence efforts and potentially assist hackers in their efforts. Other such technologies, like quantum or synthetic biology or autonomous systems, could have similar impacts. At the same time, those emerging technologies and many others, like advanced energy, are essential for the economy of the future and continued US success in the world.

The National Counterintelligence and Security Center at ODNI sits at the center of many of the efforts to combat these threats and protect emerging technology, leading and supporting critical counterintelligence and security efforts across the IC, the US government, and even the private sector. The Director of the NCSC serves as the National Intelligence Manager for

Counterintelligence and provides direct support to the DNI for the execution of the Security Executive Agent authorities across the executive branch. NCSC supports the National Insider Threat Task Force. NCSC also plays key roles in educating the private sector and the public about counterintelligence threats and works to identify and mitigate supply chain risks for the IC and the US government at large. And I would be entirely remiss if I didn't specifically call out the key role NCSC has in driving the issue of security clearance reform.

If I am fortunate enough to be confirmed as Director of the National Counterintelligence and Security Center, I will:

- Seek to enhance the important role NCSC plays in ensuring that our nation's counterintelligence efforts are integrated and effective to detect, understand, anticipate, and hopefully deter foreign intelligence efforts;
- Continue the important work begun by my predecessors and strongly encouraged by this committee to reform the security clearance process, ensuring that we can onboard personnel more quickly, implement continuous evaluation, and ensure reciprocity among US government agencies;
- Support and enhance ongoing efforts across the USG to protect our supply chains, especially in the digital space; and
- Continue the important work started by my predecessors and this committee to educate the private sector and academia on the threats they face from foreign actors and to help those private sector and academic institutions protect themselves from these threats.

Mr. Chairman, Mr. Vice Chairman, Members of the Committee—thank you again for your consideration of my nomination. I look forward to your questions.

Chairman WARNER. Thank you both for very good opening statements. I've got a couple of questions for each of you. And again, I remind Members we're going to go not by order of arrival—we're going to go by seniority in five-minute rounds, and you can go ahead and start the clock. I'll make sure I adhere to that five-minute effort—or try to.

General, I want to echo a comment that Senator Rubio made. We desperately need to get 702 reauthorized. I'm going to ask you, in your experience, how that has been a useful tool, not just in terms of the counterterrorism efforts of the decade past, but on a going-forward basis in terms of our near-peer adversaries? I think in many cases we have not done a very good job, the IC and the FBI and the Administration, in making clear that the 702 we're talking about today is very different from the 702 that was reauthorized back in 2018. There have been improvements; we need to do a better job of documenting of that.

Can you speak to the important role that Section 702 plays in terms of protecting our Nation?

General HAUGH. Yes, thank you for the question, Senator Warner. In terms of Section 702, it is a critical authority for the Intelligence Community to be able to target foreign persons overseas, to be able to collect intelligence that provides critical foreign intelligence on cybersecurity, counter-proliferation, counterterrorism, and a whole host of threats. In my experience, it's absolutely essential.

As I have reviewed products, in every product that goes to the senior leaders of our government, Section 702 has an impact. It's a critical authority. And it is also critical that as we use that very necessary authority. I have also seen, through my experience with the National Security Agency, a culture of compliance to ensure that through every execution of that authority, that the protection of civil liberties of Americans is a cornerstone of how that's executed.

Chairman WARNER. Well, I agree, and I want your commitment that when you are confirmed you will help keep the pressure on the balance of the IC and particularly our friends at the FBI. I'm not only making the case of how essential this tool is, but also the level of reforms that have been put in place.

Very briefly, because I'll make sure I can get to Mr. Casey as well on a question or two. But one of the things that we've had conversations with General Nakasone a number of times, the fact that we may not have seen from Vladimir Putin the level of all of his cyber tools. The Ukrainians have really stepped up. Companies like Microsoft help in the private sector. But in light of the fact that we've seen the recent China hack on Microsoft, how do we make sure that we stay abreast of what's going on with near-peer adversaries like China and Russia?

General HAUGH. Senator, I think first and foremost, the National Security Agency, in terms of its role of foreign intelligence and being able to inform on threats, is critical. But the power of partnerships—and as you have seen over the last few months—the work that has gone on collaboratively between SSCI, FBI, the National Security Agency, foreign partners, and also industry to produce very clear, unclassified, releasable advisories on how China

is targeting our critical infrastructure and service providers, is a good example of how to do that collaboratively—to be able to illuminate those threats that attack our economy and potentially our national security.

Chairman WARNER. Thank you. I think you mentioned this, Mike, in your opening comments, but I'm going to get it again, on the record. Should you be confirmed, will you continue to work with this Committee on our security clearance reform efforts?

Mr. CASEY. Thank you for the question, Mr. Chairman. Yes. Closely. And often.

Chairman WARNER. All right, good. We're going to hold you to that. I know the Members of the Committee and many of the folks who've worked with you here in the audience—, but I'm not sure all of the members of the public fully understand the role of the NCSC. Briefly, can you describe that, and what you think your priorities will be should you be confirmed?

Mr. CASEY. Sure. The NCSC plays an important role in developing policy, overseeing counterintelligence efforts across the United States government. So, it focuses mostly on counterintelligence. They have a Center for Security Evaluation; the Special Security Directorate, which does personnel vetting. There's a fair amount of supply chain work that they oversee and coordinate across the government. They essentially provide that function for the DNI that coordinates the IC in all matters of security across——

Chairman WARNER. And what would your goals with this entity be, should you be confirmed?

Mr. CASEY. If I'm lucky enough to be confirmed, and I think as I said in my opening statement, one, I want to ensure that our counterintelligence efforts are fully coordinated. There are a lot of players in that space. And we need to make sure we cover the waterfront in an appropriate way and evolve to meet the evolving threats. Two, to continue to work on security clearance that you've already mentioned. I think there's a great deal we can do to move that work forward. And then, three, the Director of National Intelligence has asked me to look at supply chain, particularly with regard to the cyber contents of what software the government is using, as a deep interest and concern to her.

Chairman WARNER. My final question is, and I want to make sure the press sees this for the record: We have this picture here. Is this actually a photo of you undercover? Can we validate whether this is really a picture of Mike Casey or not? I'd ask all of my——

Mr. CASEY. I don't think I can comment on this.

Chairman WARNER. Well, we'll take that under consideration when it comes to the vote.

With that, I'll turn it over the Vice Chairman.

Vice Chairman RUBIO. Maybe he has a body double just like Putin, I don't know. That's what I read in The Guardian anyway, whatever those tabloids are.

Let me start with NSA—this dual-hat issue. And we've raised that in our conversation, meaning that you're at CYBERCOM now, but now also the NSA. First, I'm just curious, to the extent that you know what the answer is, and I think you do, to what extent

does CYBERCOM now, today, currently rely on NSA personnel to execute its mission?

General HAUGH. There is a really good collaborative relationship between Cyber Command and NSA. There are NSA personnel that serve within Cyber Command. Those dollars, for every individual, are reimbursed by U.S. Cyber Command. That partnership has been incredibly complimentary to the execution of NSA's missions, and we really see that at comparative strength for our Nation to have the dual-hat leadership of both the NSA and Cyber.

Vice Chairman RUBIO. And the reason why this has come up is the issue of the delegated authorities, where U.S. Special Operations Command and Cyber Command are the only two unified military commands that can operate under NSA-delegated signals intelligence authorities. Now, while the use of these delegated authorities at SOCOM is well understood, the use of those delegated authorities at CYBERCOM—I'm not sure we could describe it or even write about it in terms of having a clear understanding.

As the Deputy Commander of Cyber Command, what's your awareness of the oversight and compliance standards used by the Command in executing the delegated signals authority?

General HAUGH. Senator, as U.S. Cyber Command does execute signals intelligence authorities. It follows every rule provided by the National Security Agency; and oversight is conducted consistent with all of the rules that govern signals intelligence, and closely coordinated with the National Security.

Vice Chairman RUBIO. I guess the fundamental question is, why does U.S. Cyber Command have raw SIGINT access when such access is limited within the broader IC? What's the argument in favor of that?

General HAUGH. Senator, the overlap between activities in cyberspace and within signals intelligence—those things are inextricably linked. And the partnership and how we've developed that, to be able to leverage the authorities, both within U.S. Cyber Command, the National Security Agency, have been a power and have really been an enabler for outcomes for the Nation. And I think as we walk through that, if confirmed, I will certainly be committed to ensuring your visibility.

Vice Chairman RUBIO. Yeah, I mean, you didn't design the infrastructure. So, we're not blaming you for it. You just have to, I think, from our perspective, it's simply that when it translates over to Cyber Command, our ability to conduct oversight over intelligence dollars and activities become severely constrained in many cases. And I think that's the problem that we're confronting on a regular basis in that regard. In the past, we've raised that concern, and I think it's one you'll wrestle with as you come into this role.

And Mr. Casey, I know you're aware of this because you've worked on it, but there is no authoritative definition for offensive counterintelligence or strategic counterintelligence. And the Committee—and you're well aware of what we've been working on in terms of a Committee report on this—thinks it's really important to establish these terms to better define the counterintelligence responsibilities within the Intelligence Community. And as you know, those recommendations are forthcoming. I think you're pretty aware of what those are going to be.

In your view, what is the best way to define offensive counterintelligence and strategic counterintelligence?

Mr. CASEY. Thank you for the question, sir.

As you note, the Committee struggled with this and they address it in a forthcoming Committee report that may be voted on in the near future. As you note, there's no government-wide definition of either, and I think the Committee staff and Committee Members struggled with a definition; ultimately didn't put it in law but suggested that the Director of National Intelligence provide one. Frankly—having some knowledge of what the Committee's definition was and some input into it—I think those definitions are pretty good.

And if it's okay with you, I'd like to just read them:

Offensive counterintelligence means clandestine counterintelligence activity conducted for national security, strategic, and counterintelligence purposes against the target having suspected or known affiliation with a foreign intelligence entity, to counter clandestine activities that threaten the United States or the national interests of the United States. And strategic counterintelligence means the processes and product of developing the context, tradecraft capabilities, knowledge, and understanding of the strategic environment, including the intentions and capabilities of foreign adversaries, and the national resources necessary to engage in counterintelligence activities to support United States national security interests, policy development, and planning processes.

I think as the Committee struggled with it, we all agreed we're not sure it's a perfect definition, but it is a pretty good working one, and there's probably some utility in having it.

Vice Chairman RUBIO. It sounds like a pretty wise definition to me. You would agree the DNI should just take it up and just implement whatever we put in that report. Right?

Mr. CASEY. Seems like an excellent thing for her to consider.

Vice Chairman RUBIO. Good. Excellent. Thank you.

Chairman WARNER. Thank you, Senator Rubio. Senator Feinstein.

Senator FEINSTEIN. Thank you. Thank you, Mr. Chairman.

I would like a moment to speak about Mike Casey, and his nomination to the Director of the National Counterintelligence and Security Center. For those Members of the Committee who might not know, I originally hired Mike Casey to be the Staff Director in January of 2016 while I was the Vice Chairman for the Committee. Mike did great work that year, overseeing several classified items, including several counterintelligence issues. And then we were lucky, Senator Warner decided to keep Mike on as Staff Director when he took over as Vice Chairman in 2017. Accordingly, we have had the ability over the past seven and a half years to observe Mike, and I find him fully qualified for the position.

Mike, well done. And I think we all look forward to your confirmation.

Let me ask this question. Can one of you give us a sense of the effectiveness of Russian cyber efforts in Ukraine, and our ability to help the Ukrainians in countering them? What else should we do?

General HAUGH. Senator, in terms of Russia's capabilities, they have certainly used a number of cyber capabilities against Ukraine.

Ukraine gets great credit in terms of how they prepared for what they have expected and experienced from Russian cyberspace. By partnering with NATO members, by partnering with various elements of the U.S. government, and also with U.S. industry, they were much more resilient to these cyber-attacks. They continue today. And we would expect that Russia will continue to use every cyber capability that they have as part of their unlawful conflict. And wherever we can provide assistance, we should continue to do that, Senator.

Senator FEINSTEIN. Thank you very much. I think that's good advice.

Thank you, Mr. Chairman.

Chairman WARNER. Thank you, Senator.

Senator Cotton.

Senator COTTON. Congratulations, gentlemen, to both of you for your nominations. Thank you for your past service and for your ongoing service.

General, we've already talked a little bit about Section 702 because it's coming up for reauthorization. You talked about how significant it is to the work of the Agency and to our national security. To put it in very plain terms, 702 is about spying on foreigners in foreign countries, right?

General HAUGH. Yes, Senator.

Senator COTTON. And the reason why it implicates America at all is that it can either be passing through an American telecommunication system, is that correct?

General HAUGH. Yes, Senator.

Senator COTTON. So, you have one Iranian bad guy in Vienna and another one in Bangkok, and they decide to use Gmail, for instance. It allows you to target, with the requested Gmail, their communications.

General HAUGH. If it's a valid foreign intelligence target, yes, Senator.

Senator COTTON. And a second reason why it might implicate America when we're dealing with foreigners and foreign soil, is that bad guy in Iran, or working for Iran around the country and maybe speaking to a bad guy here in America, as well?

General HAUGH. And if the target is the foreign target, yes, Senator.

Senator COTTON. Okay. So, this obviously has become a very heated controversy and there's some question about whether it can be reauthorized or not. But that the nub of the controversy is not that first category, I think, but the second one, right? And the prospect for what's known as reverse targeting?

General HAUGH. That is not authorized.

Senator COTTON. I understand. Can you explain to us how you go about ensuring that something that's not authorized doesn't actually happen?

General HAUGH. In my experience, Senator, there are very strong procedures for ensuring that the target of the use of 702 is a valid foreign intelligence target and that that target is overseas. There are a number of series of oversight mechanisms that I've had experience with to ensure that that not only is that always the case, but if there is a mistake, or an inadvertent action, that it's imme-

diately reported, both to Congress and to, of course, the National Security Agency.

Senator COTTON. Can you get into a little more detail in this setting about those oversight precautions to ensure those abuses don't occur? Or is that something that you're uncomfortable discussing?

General HAUGH. Well, I think, Senator, I can talk broadly in my current role about what I have seen from the National Security Agency, which is a culture of compliance—a group of Americans that want to protect their fellow Americans' civil liberties and do that in a way that's consistent with our laws, our policies, and our values. To go into the exquisite detail, Senator, what I'd request is, if confirmed, to come back to you and have a conversation.

Senator COTTON. Sure, that's fine. We're all human, mistakes happen. Sometimes abuses happen. Some of those abuses have been widely reported in the news. If such a thing happens, what mechanisms do you have in place to identify such mistakes or abuses and what kind of corrective actions are taken in those circumstances?

General HAUGH. Senator, I think that what NSA laid out with ODNI in the Transparency Report lays out just those use cases—that if there was something that has happened inadvertently, it's reported: the number of times it's occurred and ensuring that that is reported back to the court as well as to the Congress.

Senator COTTON. OK, thank you. If confirmed, I think you probably still have a little bit more work to do and probably in a classified setting with Members, not only in the Senate but in the House as well, to get 702 reauthorized.

General HAUGH. Yes, Senator.

Senator COTTON. Mr. Casey, I want to review a conclusion about the NCSC: NCSC as U.S. government lead for counterintelligence lacks a clear mission as well as sufficient and well-defined authorities and resources to effectively confront this landscape. Moreover, NCSC's placement within the Office of Director of National Intelligence may hinder its ability to scale and respond to threats in an agile manner. Despite these challenges, there is no consensus among counterintelligence officials on the way forward for the NCSC.

Are you familiar with that statement?

Mr. CASEY. I believe it came from the Committee's audits and projects team look at NCSC.

Senator COTTON. It's from our Committee and their take on the NCSC. We made 17 recommendations to try to improve NCSC. Do you agree with all those recommendations?

Mr. CASEY. Broadly, yes. I think the one that was sort of taken under advisement and to be considered was the placement—whether it should be an independent agency. There are potentially advantages to it, disadvantages to it.

Senator COTTON. Okay. All right, thank you. Well, I think our Nation vitally needs a strong and effective NCSC, especially for the threat that we face against China. And if confirmed, I hope that you'll be able to pursue and implement as many of those recommendations as possible.

Chairman WARNER. Senator Wyden.

Senator WYDEN. Thank you, Mr. Chairman. Good to see both of you and trying to keep a straight face looking at Mr. Casey, who's worked so hard and so well with us for so long. And congratulations.

Let me start with you, Mr. Haugh, if I might. With a few exceptions, NSA currently requires a probable cause determination for U.S. person queries of communications collected pursuant to Executive Order 12333. My question is, is there any reason that standard couldn't be applied to communications collected under Section 702 of FISA? And one of the reasons—and you can see the interest here in the Committee with respect to 702—I don't understand why if it works for 12333, it can't work for 702. And it would certainly provide more protection for Americans who are concerned about their privacy rights.

Your thoughts?

General HAUGH. Senator, I share your focus on protecting American civil liberties. As in my experience of working with E.O. 12333 collection, I've got a good understanding of that. What I would ask Senator, in my current role, I am not into the details of how each 702 authorization is executed. I'd ask to be able to come back if confirmed and have a conversation with you.

Senator WYDEN. Let's speed it up a little bit, though. I'd like a written answer why we couldn't have that before the vote. Can you get that to——

General HAUGH. Yes, Senator.

Senator WYDEN [continuing]. Within a week in writing?

General HAUGH. Yes, Senator. If confirmed, I will do that Senator.

Senator WYDEN. No, no. We need to have your——

General HAUGH. Yes, Senator.

Senator WYDEN [continuing]. Assessment of it before we vote within a week.

General HAUGH. Understood, Senator.

Senator WYDEN. Can you do that?

General HAUGH. Yes, Senator.

Senator WYDEN. Great, thank you. Let's talk about your role as functional manager for cyber. General Haugh, the NSA Director is the functional manager for signals intelligence, which means the director develops and implements IC-wide policies, practices, and procedures for SIGINT. Does this role extend to computer network exploitation?

General HAUGH. Senator, the overall responsibility of the SIGINT functional manager is to direct and have oversight of all SIGINT collection, processing, analysis, and reporting and dissemination of SIGINT products. And that includes computer network operations.

Senator WYDEN. You're the point guy with respect to all of those things that the public usually thinks is——

General HAUGH. So, in terms of using all of the tools of the United States SIGINT system, the Director of the National Security Agency is responsible.

Senator WYDEN. Good. On encryption, every day, it becomes more and more obvious that Americans' security, their safety, and their well-being depends on strong encryption. If you're confirmed,

will you commit that NSA will not seek to insert backdoors into or otherwise weaken encryption technology used by Americans?

General HAUGH. Senator, encryption is a critical responsibility of the National Security Agency. It's critical to defend our national security systems and our weapons systems. If confirmed, I will not weaken encryption for Americans.

Senator WYDEN. That's an important statement. So, on your watch encryption is going to be preserved?

General HAUGH. Yes, Senator.

Senator WYDEN. Very good. Let me ask one other question, if I might, on the definition of signals. General, last October there was a new Executive Order on signals, and two weeks ago the IC issued a whole array of procedures implementing that Executive Order. What's missing is any Intelligence-Community-wide definition of signals. That makes it hard to know what all these procedures actually cover? In your view, should there be an Intelligence-Community-wide definition of signals? And I know that we've had some discussion up here already about that.

General HAUGH. Yes, Senator. In terms of where the definition of signals intelligence is defined, it's defined in National Security Council Intelligence Directives, in E.O. 12333, and in the United States SIGINT systems intelligence directives. They are all very consistent in terms of what comprises SIGINT in terms of communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence. So, I think there is a common definition that is aligned across the Executive Branch.

Senator WYDEN. As you and I talked in the office, with respect to the lack of a consistent IC-wide definition, I know we'll continue that. And I look forward to particularly getting your response in writing to that question I asked about Section 702, before we vote in the Committee, and I appreciated your candor in the office.

Thank you, Mr. Chairman.

Chairman WARNER. Senator Cornyn.

Senator CORNYN. Congratulations to both of you for your nominations.

I don't think it's an overstatement to say we're living at a time of—certainly in my lifetime—unprecedented distrust of our government institutions and challenges to those institutions. Unfortunately, some of that, I think, in the case, for example, of the FBI, is justified by the abuses that occurred in recent years that we all are familiar with and been well documented. And I know Director Wray is committed to attempting to regain the public trust. And indeed, there's one thing both of you should be happy about today. And that is you're not in the House of Representatives where Director Wray is testifying today, and your name isn't Chris Wray.

But I just want to get an understanding from you, General. How can the American people be confident that these incredible tools, which you said are essential to the mission of NSA and Cyber Command—how can they be assured that these tools will not be abused to their detriment?

General HAUGH. Yes, Senator, I think it's incredibly important, if confirmed, to build a trusting confidence that for myself as a leader, that you will trust the inputs, because I know I have faith and confidence in all of the individuals of the National Security

Agency. In my experience, an incredible workforce that is focused on the protection of their fellow Americans. And they do a service to their Nation every day. And the ability for us to provide transparency on their activities is something, if confirmed, that I would like to be able to partner with this Committee on.

Senator CORNYN. And Mr. Casey, as you're well aware of the concerns about the FBI's activities, since you're going to be so involved in counterintelligence matters oversight at the DNI, I'd be interested in your views about the FBI's unique role. They are a law enforcement agency, but they're also a counterintelligence agency. And in the course of dealing with some of this lawfully-collected intelligence on foreign—on people overseas, occasionally a U.S. person's name will come up that can even potentially be used in the course of an investigation that has nothing to do with the counterintelligence matter, but other law enforcement matters.

What's your view about how we do best to try to regain the public's trust that the FBI, as the primary counterintelligence agency for the U.S. IC, isn't able to use that lawfully-collected foreign intelligence for an improper purpose against an American citizen or a U.S. person, which of course as you know, is broader than a U.S. citizen?

Mr. CASEY. Thank you for the question, Senator. First, NCSC is not an operational——

Senator CORNYN. Right.

Mr. CASEY [continuing]. Part of the government. They're very much a strategy oversight and policy——

Senator CORNYN. But you're supposed to integrate counterintelligence and security missions areas under one organizational construct.

Mr. CASEY. Correct, sir. But there are other agencies that actually carry them out.

Senator CORNYN. So, you won't be part of the operations, but you will be part of the oversight.

Mr. CASEY. Correct. And the NCSC's purpose in devising all counterintelligence strategies, plans. One, there's a heavy involvement in the Civil Liberties Office. There's a real attempt to achieve transparency and I think to your question about the FBI, as much transparency as humanly possible into how the FBI operates is probably the best way to regain the trust of the American people.

I know as Congress considers 702 reauthorization, there are a number of proposals for increasing transparency or putting limits on how that information that's collected can be used, and there's certainly work that can be done in that area.

Senator CORNYN. Well, part of the conundrum in trying to convince the American people, much less Members of Congress, about these authorities—is a lot of the information that would demonstrate the necessity of that is classified information by its nature. And I know the DNI and others have attempted to declassify certain things that they could give us the information we can use then to make the case why 702 should be reauthorized.

But I think we've got a very heavy lift on our hands, and frankly, it's going to start with the House of Representatives. We're going to have to make some changes with the FBI's authority, particu-

larly as regards U.S. citizens and U.S. persons, when they use lawfully-collected 702 information for law enforcement purposes.

But finally, let me just ask you, General, since we talked about this yesterday. You know, it's a big concern of mine, given the incredible responsibilities of Cyber Command and NSA, the global responsibilities, and all the hot spots in particular you have to prioritize. I'm worried that we are losing the war on counternarcotics efforts in Mexico and south. And I worry that we don't have the bandwidth we need for the NSA to provide the intelligence that we can then use with our partners in the region to go after the bad guys, and to cut off the flow of some of these narcotics.

Could you share with us some of your thoughts about how we might be able to augment those current authorities, or the means by which those authorities are exercised?

General HAUGH. Senator, it's an important question in terms of counternarcotics, specifically Fentanyl and what that has meant to our Nation. That is certainly a mission that is a responsibility, from a foreign intelligence perspective, of the National Security Agency to understand those threats. If confirmed, I'm committed to be able to work that and also to look for new partners to be able to collaborate with, to be able to address that threat.

Chairman WARNER. Senator Heinrich.

Senator HEINRICH. I want to start just by thanking Senator Cornyn for that last question, because I think it's a really pressing issue that deserves your focus.

Lieutenant General Haugh, this has been covered a little bit, but I want to return to it and just make sure I understand your plan for moving forward. A number of prehearing questions asked about Section 702, FISA collection, and the compliance regime that NSA has in place for its Section 702 collection authorities to ensure the protection of U.S. persons in particular. So, in your answers, you largely deferred to the current NSA leadership, stating that you have limited familiarity with the issue in your current role with CYBERCOM. And I have to say, I don't view that answer as good enough. I'm disappointed. NSA very much depends on FISA Section 702 authorities to collect the communications of critical foreign intelligence targets located outside of the United States who use our U.S. infrastructure and services to communicate.

And especially with 702's expiration looming, it would simply serve you well as the nominee to lead the NSA to demonstrate more than a limited familiarity with those procedures and compliance governing the protection of Americans' data. So, I would just ask for your commitment to expedite that process to become very familiar with that compliance regime as you seek the confirmation.

General HAUGH. Senator, I absolutely agree with you that this is the priority issue in terms of being able to understand, to a granular level of detail, how this is conducted. If confirmed, this is my first priority: to be able to understand that.

Senator HEINRICH. I'm glad to hear that.

I'm going to pop over to you, Mr. Casey, very quickly, and I certainly don't have to tell you about the importance of promoting supply chain security for increasing American competitiveness, for driving innovation. What's the role of the NCSC in preventing and

mitigating foreign, state, or even non-state actors from compromising U.S. supply chains?

Mr. CASEY. Thank you for the question, Senator. It's one of the major roles that NCSC has. An entire directorate is dedicated to supply chain issues and cyber. And as I mentioned, particularly on cyber/supply chain, it's one of the DNI's highest priorities. For me, were I fortunate enough to be confirmed and move into this job, the NCSC is the lead for supply chain issues for the IC, and throughout, frankly, the United States government. Having said that, there are a lot of players in this space, and so an important part of that is coordinating the efforts, ensuring that lessons learned are shared among the agencies and sometimes with the private sector.

Senator HEINRICH. Talk a little bit about that. How do you plan to make sure that NCSC keeps ahead of advancing technology in order to provide threat awareness information to industry, and for that matter, federal and other partners?

Mr. CASEY. Thank you, Senator. First, with a caveat that as I've not been confirmed, I'm not deeply versed in the NCSC's current efforts. But I think the single biggest question is understanding what the current efforts of the United States government and various different parts of it are. DoD has a number of efforts ongoing. Other parts of NSA have efforts ongoing. I think there should be a big effort in understanding what the waterfront looks like at the moment and ensuring that we have adequately covered it. Frankly, if I'm lucky enough to be confirmed, I'd like to come back to you with a better answer on the next two or three steps we could take.

Senator HEINRICH. We'll look forward to that. Thank you very much, Chairman.

Chairman WARNER. Let me just, before I go to Senator Lankford, we have heard from Senator Cornyn, Senator Heinrich, and obviously Senator Wyden as well on 702 concerns. One of the things—we just have to do a better job as we ask our colleagues to reauthorize this critical tool and convince the American public. Again, there are many changes in terms of FBI operating procedures. But also at NSA, operating procedures that are very different than they were even a year or two ago, let alone what we reauthorized in 2018.

And we just have to do a better job of documenting that and making that case. That's an editorial comment, obviously, but for those of us who understand the importance of this tool, we've got some work to do., I do think making clear how the decrease in inadvertent contacts or the number of people that may actually receive a victim notification through a 702 tool is a case we've got to make.

Senator Lankford.

Senator LANKFORD. Mr. Chairman, thank you. Thanks to both of you, and for your service already to the country and what you've done.

General, I want to be able to zero in on some of the things that Senator Cornyn brought up as well on the counter narcotics work that's happening currently. There are a lot of threats that Americans have around the world.

There's a lot of work that needs to be done, but people feel what's happening on the streets, and 100,000 families are dealing with a

family member that died from illegal narcotics that came into the country last year. So, we feel this threat faster than we feel other threats on it. What I'm interested in is what your commitment is to be able to actually go after the information and the infrastructure that's actually bringing these drugs in that are killing Americans every single day.

General HAUGH. Senator, I agree with you. This is a national security issue. And from a National Security Agency perspective, the role of foreign intelligence to be able to understand the threat and communicate that threat to elements that can take action, that will be a priority, Senator, if confirmed.

Senator LANKFORD. Okay, I appreciate that. We'll follow up on that in the days ahead. Unfortunately, every director that's a recent director of NSA has dealt with a major security breach within the Agency. So, you get to walk in and say, okay, not on my watch. So, let me just ask you, as you approach trying to deal with how are we not going to have a security breach on your watch, what are your first thoughts about what to do different? How to be able to deal with this?

General HAUGH. Senator, the protection of our national security information is critical. Classified, in and of itself, by its very definition, if disclosed causes great harm to the Nation. So, this is paramount for leaders in the national security community. For me, I think about it in two different ways. Personal accountability. So, we need to make sure that we have the highest talent, and I'm very confident in the talent we have in the National Security Agency. We have to ensure that continues, and then we have to have technical means to ensure that we are able to be confident in the oversight and the control of classified information.

So, if confirmed, I'll review all of our current processes, and ensure that from a National Security Agency perspective, that we're doing everything we can and then we'll partner with the rest of the national security community and the Intelligence Community to ensure that we're sharing what we believe are best practices.

Senator LANKFORD. Yes, that would be helpful in the days ahead. Obviously, there's work to be done. Every director has said that. It's a challenge. You're dealing with a lot of people and a lot of complexity. And having the opportunity to be able to verify what's out there and what's not out there is important.

There's been this balance between contractors and full-time employees. It's much faster to hire a contractor; they get people in immediately and are able to take care of it. A lot of them have experience in the IC and they're able to get there quickly on it. It's hard to be able to get full-time folks that are there, and then there's different sets of rules on it. How will you strike that balance between the contractor and full-time?

General HAUGH. Senator, I do believe it's a balance, and we have to ensure that. There are things that, from a National Security Agency perspective, the workforce with the mission focus and the technical capability is a critical asset to the Nation. And having them be able to do inherently government functions and to be able to do that in a world-class way is certainly the priority in terms of being able to sustain that world-class foreign intelligence and cybersecurity that NSA provides.

Senator LANKFORD. Okay. We're going to count on that in the days ahead, as well.

You were asked a question just in the prehearing questions about describing your view about when it's appropriate to withhold pertinent and timely information from the Congressional intelligence committees. You answered appropriately: It's not appropriate to withhold information that's within the jurisdiction of a Congressional committee.

That may seem like a silly question, but the challenge that we've had around this dais, both sides of the aisle, has been that we would have a hearing in a closed-door setting. We would go through all the different issues, and then within 24 hours something would be in the New York Times that was not discussed with us, that was clearly known, and it became an issue of we just didn't ask the right question at the right time.

And it was like, I would have told you if you would have asked me directly. But we don't know whether to ask people directly. So, I think the basis of this question that was coming to you was, we don't want to have to know how to ask the magic question. If there are issues that we need to be aware of, we need to know, and it needs to be forthcoming in an opening statement from you and to say, hey, this is something that's on the horizon.

Are we still okay with that?

General HAUGH. Senator, if I'm confirmed, I commit to a partnership to ensure that you have the necessary information.

Senator LANKFORD. Thank you. We appreciate that very much, and we look forward to that partnership.

Mr. Casey, I need to know, is this nomination really a discreet way to get out from under Senator Warner's authority?

Mr. CASEY. One hundred percent, sir.

Senator LANKFORD. That was what I assumed, that was the prehearing question that had not been asked to you directly on this.

I do want to ask for just a philosophical statement from you as well, because the counterintelligence efforts—and you approach this in your opening statement as well—is you made the statement of counterintelligence efforts—I'm going to abbreviate some of it—is to deflect, understand, anticipate, and hopefully deter foreign intelligence efforts. I want to drill down on the last of them, philosophically, strategically. What does it mean to deter foreign intelligence efforts to you?

Mr. CASEY. Thank you for the question, Senator. The way I think about it is success looks like this: when we get intel that the foreign government, foreign intelligence services, went somewhere else to try to steal secrets that they thought were too hard to get here and they were too likely to get caught. And that covers a variety of efforts across the security, counterintelligence, offensive counterintelligence activities. But that when we put those things together, they just decide they can't operate here.

Senator LANKFORD. Okay, thank you. I appreciate that and appreciate your engagement, obviously, your service here to the Committee as well, and the way you've handled so many issues. As you're dealing with private industry and talking about threats that they're facing, I would encourage you to do what has been done in the past and to make sure that private industry is fully aware that

any of their cooperation, their data, is voluntary in the way they share that and engage, so that their rights are also protected because they're a victim. Not now suddenly to be victimized by their own government. Again, by having to share information in ways that are not comfortable, or PII and such. And so, there's this strange balance that you've got to be able to work to be able to help protect those companies, individuals, and American citizens as the attack is coming to private business, but also protecting the rights of those individuals as well.

Mr. CASEY. Thank you for that, Senator.

Senator LANKFORD. Thank you.

Chairman WARNER. And while I will take issue with his characterization of Mr. Casey, I would say I want to double down on your comment to General Haugh. You're going to find no better ally than this Committee. But that trust—and it's happened with many of the folks who've appeared before us—disappears if we don't ask the magic question, and we then subsequently find there was a piece of information that somebody had and didn't reveal to us when they had an opportunity.

Senator LANKFORD. One hundred percent. And may I remind you, Mr. Chairman, Mr. Casey was under oath when he answered that first question.

Chairman WARNER. Senator King.

Senator KING. Thank you, Mr. Chairman.

General, I want to focus on a word that you used four or five times in one of your first couple of answers, and that word is collaborate and collaborative. The cyber conflict is different than conflict in history. We're not talking about army against army, and air force against air force, navy against navy. We're talking about 85 percent of the target space in the private sector. So, collaboration and really a new level of trust and collaboration, it seems to me, is going to be necessary.

Is this something that you believe that in your history with the military, you will be able to transition to having that kind of relationship of trust and collaboration with the private sector, and NSA when you take over that position?

General HAUGH. Senator, this is an important issue, and I think it's been enabled both by the Congress and by the Department of Defense to have that collaboration with industry, both from U.S. Cyber Command and the National Security Agency. The ability to share directly with industry, while also teaming with our teammates in DHS and FBI, has been a really critical enabler.

NSA has been enabled by the Department to do a partnership with the defense industrial base and build a collaborative relationship to share information in both ways from a threat perspective. And NSA has also begun to provide cybersecurity services to the defense industrial base. Those are the types of partnerships that, as we see those initial indicators, those are the potential things, that if confirmed, I'll look at how do we scale that?

Senator KING. Well, I think your answer is exactly right, but the resulting product of this is a kind of collaboration that doesn't come naturally to either side, and trust has to be established. And I hope that's something that's also in your calculation. As Senator Lankford said, the companies have to feel comfortable in a trustful

way to share this information with you. I was asked a question this morning in a public forum about Ukraine and why we didn't have more cyberattacks from Russia as a result, because everyone was expecting this. Part of it, as you testified, was the Ukrainian skill working with us and the work that was done to help them defend their networks and to be more able to be resilient. But part of it, I said publicly, I think the Russians were afraid of Paul Nakasone. There's a deterrent effect that is very important. The concept that he established was called Defend Forward.

Do you subscribe to that concept that we have to have a deterrent that adversaries feel that coming against us in a cyber-attack of some kind is not a free lunch?

General HAUGH. Senator, I think we need to engage our adversaries if they're conducting activities that are malign and have a negative impact on the national security of the United States, or a negative impact on our allies and partners. And that ability to do that and the ability to put pressure on them, expose their activities, while also making our allies and partners more resilient, is absolutely critical every day so that they know that they're contested.

Senator KING. Well, and the key phrase you just used was, "they know." It's not a deterrent if they don't know it, if they don't know that we have the capability. And I think you have to be aggressive in terms of letting our adversaries know that if they attack the United States in cyberspace, there will be a proportional and hurtful response.

General HAUGH. I think, if confirmed, Senator, in the roles that I will play, it will be my role to be able to produce options that are also consequential and ensure that across how we integrate with all the other elements of our national capabilities, to be able to ensure that we do have a realistic deterrent and to be able to present that.

Senator KING. Well, I hope to see intelligence over the next several years where one of our adversaries said, we better not do this because we're afraid of that General Haugh guy. So, that's a mission.

Insider threats and counterintelligence. If I think back to our major intelligence briefs going back to Aldridge Ames and after that, we cannot possibly vet people to the point where there is a zero chance of somebody turning on their country. Therefore, you mentioned technical means, General. I was surprised, for example, in the recent case, that we didn't know when information was being exfiltrated from a classified system. Are we working on technical means to have a greater grasp of our secure information, rather than hoping that the people that we have hired will never succumb to whatever the temptation is to betray their country?

Let's start with you, Mike.

Mr. CASEY. Thank you for the question, Senator. Not sitting in the seat, I don't know all the details, but my understanding is there's a certain amount of agency by agency—different agencies have implemented different technical means to do that.

Senator KING. Well, that's a problem right there.

Mr. CASEY. Yes, Senator.

Senator KING. And you're in charge of this Center. How about some uniformity of process?

Mr. CASEY. So, my understanding is that there's a current Intelligence Community review of the recent disclosures underway at the moment. And when that's finished, my expectation, were I to be confirmed, that through the role of the involvement of the National Insider Threat Task Force, that those lessons would be shared with different agencies. And then it's a matter of essentially shaming them into getting the job done.

Senator KING. General, I hope you're going to be astride of a highly capable technical agency. I hope that it will have as one of its missions figuring out how to protect this information using, as you say, technical means.

Do you see that as part of your mission?

General HAUGH. Yes, Senator. I think overall, the National Security Agency is relied upon to provide—if it's not within the specific role of the National Manager for National Security Systems—it certainly is to provide advice on how best to use technology to protect our national security information.

Senator KING. Thank you both, gentlemen. Thank you, Mr. Chairman.

Chairman WARNER. I think those were good questions, Senator King. I do think, at least in my conversations under General Nakasone's leadership, and also, frankly, because the NSA has been the victim of so many of these issues, the notion of copying documents and walking out, they have taken corrective action the rest of the IC can learn from. I don't think, if Mr. Teixeira ends up being proven guilty, that he would have gotten away with it at the NSA.

Senator Rounds.

Senator ROUNDS. Thank you, Mr. Chairman. First of all, to both of you, thank you for your service to our country. General Haugh, it's not just you, it's your family. And when you've deployed multiple times, your family is away from you, they put up with that. And so, I want to say thank you to your family as well.

Mr. Casey, you're probably not deployed in the same way as General Haugh has been, but as several other Members have indicated, putting up with a Committee and working through the bureaucracy of Washington, D.C., for years and to do a number of successful items also says a lot about your capabilities, as well.

So, thank you to both of you.

I want to begin with General Haugh. I share the admiration that Senator King has expressed with regard to what General Nakasone has been able to accomplish. And part of this has been because he has taken on and has challenged the issues surrounding a dual-hat. I happen to be a proponent of the dual-hat approach. I think it works well. It's probably not perfect, but it's better than having separation and then having disagreements or silos in which you try to communicate back and forth.

One of the areas that I felt had been very successful was the implementation of NSPM 13, which is a classified document. It basically, in broad terms, would suggest a clear way, a quick way in which to respond to foreign threats or opportunities for cyber intervention by us. And since that was intervened or approached, it has

been an item making our cyber operations, I would consider, to be much more successful.

The question I have is, moving forward, NSPM 13, while modified slightly over the last ten years or so, is still in effect. Do you believe that you need additional capabilities, or do you see additional capabilities that are necessary to continue your mission in terms of the dual-hat approach that we expect today?

General HAUGH. Senator, in my experience, there is a really good alignment between the law and what has been produced by the Congress, by our national policy, and by the authorities that have been given to U.S. Cyber Command and the National Security Agency. So, I think what that then allows is complementary action under those sets of authorities that produce the best outcome for the Nation.

Senator ROUNDS. One of those areas, as a number of the Members here have talked about, is 702. Could you just briefly, because there's a lot of folks back home saying, what are they talking about? What is a 702? Could you briefly, in terms of the magnitude of the importance to the defense of our country, could you share in this open session a little bit about how critical and how much we use 702 authorities?

General HAUGH. Senator, I think that, first and foremost, ensuring that the American people understand that this is an authority to collect against foreign persons overseas.

Senator ROUNDS. Just, like, once every month or so?

General HAUGH. It is extensively used and it is an irreplaceable authority for the Intelligence Community.

Senator ROUNDS. Give me an example, if you could, the magnitude of the value of that program. Can you share that?

General HAUGH. I will give you an example of the products that are produced for the President's daily brief. One hundred percent of those that have SIGINT input that have 702 reflections in them.

Senator ROUNDS. It's not an item that we want to lose, so we want to make sure that we protect and that Members of the House and the Senate feel a great degree of comfort that the protection of American citizens' private information continues and is improved upon in the reauthorization. Fair statement?

General HAUGH. Yes, Senator.

Senator ROUNDS. Thank you.

Mr. Casey, I'm just curious. You've had a chance sitting here to look at a number of different opportunities that we've had to improve or to look at the execution of counterintelligence operations. And while you would not be an operator of those, you clearly would be the overseer of a lot of them and the coordinator of a lot of them.

Does the Director of the NCSC have the necessary authorities to appropriately lead the CI enterprise? And that includes assistance to our private sector.

Mr. CASEY. Thank you for the question, Senator. I think the Committee's audits and projects team had a number of suggestions for improving that. If I'm fortunate enough to be confirmed, I'd like to, frankly, take some time to look at it and get back to you.

Senator ROUNDS. I want you to go on a little bit. It seems to me that you've expressed in the past a real desire to perhaps make some repairs here. Is that a fair statement?

Mr. CASEY. That's a fair statement, sir.

Senator ROUNDS. How strongly do you believe in that? Tell me, how serious is it that this has got to be done?

Mr. CASEY. I think we've all sat here before and talked about the threats that we're facing from the PRC, from Russia, to thefts of intellectual property—where the United States is facing an across-the-board threat by a whole of society, to say nothing of terrorist hackers, the usual gamut. And it is extremely urgent that we get a system in place that works on every possible level to protect against all those threats.

Senator ROUNDS. Including those against private enterprise?

Mr. CASEY. Absolutely. And, in fact, that's been a priority of the PRC. And as I think I said in my opening statement, that threatens our current economic success in the future. And as the Chairman has pointed out more times than I can count, if the Chinese are able to, frankly, get ahead of technology, start setting the international standards, over time that locks us and Western Europe and the Japanese and South Koreans not only out of the game, but plays to our disadvantages and affects our personal freedoms.

Senator ROUNDS. Thank you. My time has expired.

Thank you, Mr. Chairman.

Chairman WARNER. Thank you, Senator Rounds. Senator Casey.

Senator CASEY. Thank you, Mr. Chairman. I want to thank both the nominees for your, as Senator Rounds said, your service to the country, your willingness to continue in service of the Nation. This Casey will not have questions for Nominee Casey at this time.

Mr. CASEY. Deeply disappointed, sir.

Senator CASEY. But we might later.

But General, I want to thank you for taking time to sit and talk, as we did. And I'm noting for the record your Lehigh University credentials, among others. We're grateful for that. I just have one comment and then two questions for you, General. One is, I won't reiterate or ask for reiteration of the questions pertaining to 702, but like so many of us, I think virtually every one of us we've seen, because of the briefings we've received, the benefit of 702. And it's a critical set of authorities for our ability to keep the Nation safe. I don't think I have to reiterate that anymore, but we have to keep making that case. But the question I had was, and I'm referencing your testimony on page two, you talked about in the third full paragraph on page two, the value of partnerships.

And you say in reference to, in particular Russia and the People's Republic of China, you say, quote: 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. End quote.

Here's a question.

Obviously, NSA has a focus on both of those nations and the threats posed by them. So, how do you plan to continue to lead that effort to adapt both the mission and the capabilities of NSA in order to focus on those two threats?

General HAUGH. Senator, in terms of how we think about partnerships, it's really the men and women of the National Security Agency, the ability to create advantage for those other interagency partners. They all perform critical roles for our Nation. But NSA is providing both foreign intelligence and cybersecurity—foundational to the other activities that we do—both within the department and within the interagency.

When we think about foreign partners sharing those common threats, how do we work with them to also ensure that our Nation is secure, but also enabling them where we have shared interest, to be able to defend against foreign activity, whether that's in cyberspace, whether it's disinformation, or it's some other coercion, and be able to provide insights and be able to enable resilience to those activities.

So, as we think about partnerships, it really is about how to make others effective, and to be able to ensure that we're doing the best thing for the national defense by leveraging our authorities, doing it in a very legal and compliant way with our laws, policies, and values.

Senator CASEY. Thank you. I know that you share the real concern we have about the threats posed by both Russia and the People's Republic of China.

Last question is this. One of the areas of focus for me on the Committee, as I've tried to do across a number of committees and jurisdictions that I serve on, is the Intelligence Community's efforts to both create more accessible facilities and implement assistive technologies in order to enable people with disabilities to contribute to the IC's mission. Talk to me about that and the efforts you can continue to undertake in that area.

General HAUGH. Senator, I think this is an area that NSA has been one of the leaders in the community, ensuring that we have the talent that can do the highly technical, very mission-focused set of activities that go on at the National Security Agency. NSA has been very successful to go across the country and to be able to tap into the talent that exists both within disabled and neurodiverse communities, to be able to do very important missions for our Nation. If confirmed, I look forward to being a part of that and to be able to continue that and continue to grow it.

Senator CASEY. Thank you, General. Thank you, Mr. Chairman.

Chairman WARNER. Thank you, Senator Casey. I appreciate you raising that last issue and thought it was appropriate to mention the community that, frankly, I had to get educated about in terms of neurodiverse and what a role they can play. I appreciate you raising that.

Senator Gillibrand.

Senator GILLIBRAND. General Haugh, thank you so much for your service. You're taking on a very big job, and we're very grateful for it.

In response to additional prehearing questions, you discussed the collateral benefits for the protection of commercial networks outside the defense industrial base, which come from NSA's engagement with the private sector.

In a time of war, do you feel confident that our civilian digital infrastructure, to include emergency services, can be sufficiently

protected by the current commercial providers? Or are there adjustments to your authorities needed to use NSA and CYBERCOM capabilities to protect things like hospital networks, public utilities, and other critical infrastructure?

General HAUGH. Senator, I think that the National Cybersecurity Strategy starts to lay out that framework in terms of how we collaborate across the U.S. government with state and local partners. And I think NSA will have a critical role to play, particularly with our teammates in DHS and the FBI, to be able to put us in the best position as a Nation to be able to do that defense. But I do believe there's work to be done.

Senator GILLIBRAND. I would imagine some of that work would include what happened in Guam most recently.

General HAUGH. And Senator, I think it's a really good example, because understanding what the threat is and now being able to inform that threat and NSA's role from the National Manager of National Security Systems will certainly be at that table to partner with all the other elements of the U.S. government with INDOPACOM as the element that's responsible, from a Department of Defense perspective, to understand the threat and then be able to work solutions collaboratively, with both the local all the way through to the other federal partners.

Senator GILLIBRAND. I think it's just a very apt example, because if the civilian-owned infrastructure is taken down, you can't complete operations, especially if it's critical infrastructure in the United States. And without the review and analysis of what risks we have and what vulnerabilities we have, we will not be prepared to protect, defend, and be able to continue to use all the infrastructure we need in the United States to project worldwide.

General HAUGH. Senator, if confirmed, I look forward to partnering with our teammates in DHS and also within the elements in the Department as we look at defense-critical infrastructure.

Senator GILLIBRAND. Thank you.

As a Member of this Committee and the Armed Services Committee, I've seen firsthand, oftentimes it is intelligence relationships and military relationships with other countries, sometimes developed confidentially, which produce some of the biggest results in our bilateral relationships. Our ability to develop robust coalitions is crucial to safeguarding our national interests. But when we operate together, sometimes we're only as strong as our weakest link.

Being mindful that we are in an open setting, can you discuss any work that you've done to date to raise the cybersecurity acumen of our partners and what types of enhanced cooperation would you like to advance, if confirmed?

General HAUGH. Senator, I do have a lot of experience in this area. Previously, I was the Commander of the Cyber National Mission Force when we initiated the Defend Forward operations, which based off authorities from Congress and then from the Executive Branch. This allowed us to now go and be able to partner with other nations, to be able to identify threats on their networks collaboratively, and really allow us to do two things simultaneously: put pressure on one of the other nation-states that we're attempt-

ing to influence that nation, and also allow them to get a deeper understanding of our tradecraft and how we do that every day.

Additionally, I think what we have seen as part of the overall coalition to support Ukraine is a collaboration of nations that has had to do that together on networks that also we had to spend significant time with European Command and NATO to ensure that those networks that we're using collaboratively with each of those partners are cybersecure.

Senator GILLIBRAND. As an example, I just visited some of our assets in Portugal, and they had a recent cyberattack that put NATO confidential materials at risk. That country still hasn't reached its two percent investment in military. One recommendation would be to really encourage our allies to choose that their investment will be in cyber-capacity or in space capacity or in new intelligence capacity that's helpful for the alliances.

Is that something you will endeavor to do?

General HAUGH. Senator, well certainly, we have a great partnership with General Cavoli today. We'll certainly work very closely with General Cavoli on what capabilities the alliance needs.

Senator GILLIBRAND. Thank you. And then last, in last year's NDAA, I established—and expanded in this year's NDAA—a scholarship program for college students to gain education in cybersecurity and digital services, with an ensuing service obligation to the Department of Defense or the IC. Do I have your commitment, if confirmed as NSA Director, you will welcome these students, once cleared, as part of your dedicated and trained workforce, and do everything you can to support the Cyber academy?

General HAUGH. Absolutely, Senator.

Senator GILLIBRAND. Thank you.

Thank you, Mr. Chairman.

Chairman WARNER. Thank you, Senator. I also think you raised a very interesting point about other ways that our NATO allies could get to those requisite investments, and, frankly, might actually be more valuable than another 50 soldiers.

Senator GILLIBRAND. Correct. Which is why I wanted to highlight it to the future NSA Director, because he can lead that effort. It's also a way to project power with countries that want to align with us, that have enormous potential, like India. So, military sales are typically the way we project power, but you can also do it through development of new capabilities in cyber, in space, in future technologies—with a different kind of industrial base.

Chairman WARNER. I think a very good point.

Senator Ossoff.

Senator OSSOFF. Thank you, Mr. Chairman. And Mr. Casey, thank you for your career of service to the Congress. Congratulations on this nomination. General Haugh, thank you for your service in the Air Force. Congratulations to you, as well.

One would have thought that after the Snowden affair hard lessons learned would have been applied consistently across DoD and the IC to prevent serious and preventable disclosures of classified information. But the recent unauthorized disclosures, allegedly by an Air guardsman in Massachusetts, suggest to me that there remains, at least in pockets of the U.S. government, significant complacency and incompetence about the protection of classified infor-

mation. So, beginning with you, General Haugh, could you please detail to the Committee how, in this role, if confirmed, you will, with intensity and precision, use both your formal authorities and your influence and example to prevent such unauthorized disclosures, which put U.S. national security at risk, in the future?

General HAUGH. Senator, protection of our classified information is paramount. If confirmed, the role that the Director of NSA plays to be the national manager of national security systems, that sets the starting point in terms of how do we secure those systems, and how do we monitor them in terms of understanding threats—as we think about foreign threats. But we do have insight in how to deal with insider threats. So, if confirmed, I pledge to work with the other elements of the IC and within the department to help support efforts to ensure that our systems are secure.

Senator OSSOFF. How about standardizing best technical practices?

General HAUGH. We'll certainly be an advocate for that. Yes, Senator.

Senator OSSOFF. Mr. Casey.

Mr. CASEY. Thank you for the question, Senator. If confirmed, the Director of NCSC also plays a role in a number of different ways in helping to prevent insider threats. So, one, the NCSC coordinates damage assessments when they're ordered to ensure that we capture what actually happened and what lessons we can learn from it. Secondly, the DNI and the AG co-chair, but the NCSC largely staffs, the National Insider Threat Task Force that's charged with sharing best practices and encouraging agencies across the government to effectively implement security.

And then finally, the personnel vetting, which NCSC is, again with DoD, helping to lead the development and roll out of Trusted Workforce 2.0 to hopefully head off some of the insiders, frankly, before they become insider threats.

Senator OSSOFF. Mr. Casey. Thank you.

How will you characterize or measure success in your role if confirmed?

Mr. CASEY. Thank you for that question, Senator. I think there's a few different ways that if I'm confirmed, I would measure success. One is the continued and hopefully successful rollout of Trusted Workforce 2.0. Second thing, I think we can do a better job of doing more coordinated outreach to the private sector and academia about the threats they're facing and ways they can mitigate it.

And finally, the ultimate way of measuring success, as I think I was alluding to with Senator Lankford, is when General Haugh gets SIGINT in from some foreign adversary that it's too hard to operate in the United States, and they're going to go somewhere else.

Senator OSSOFF. Thank you, Mr. Casey.

General Haugh, with the immense capabilities that would be at your disposal as NSA Director, of course, there emerge privacy and civil liberties concerns for American citizens. Will you pledge to be fully attentive to those concerns, both as a matter of law and as a matter of ethics and best practice, and fully candid with the Committee when we bring questions to you on that subject?

General HAUGH. Yes, Senator.

Senator OSSOFF. And General Haugh, of course, NSA Georgia, which will be a significant contributor to your efforts if confirmed, brings unique capabilities to the National Security Agency. Can you characterize the value of the contribution of the personnel at NSA Georgia and opportunities for growth you see at that facility?

General HAUGH. Yes, Senator. In terms of my current role and in my previous roles, NSA Georgia is a critical part of the United States SIGINT system, and it's also very critical to U.S. Cyber Command in terms of the forces we've aligned with Army Cyber. The specific areas that I think are unique with NSA Georgia is NSA's combat support role, and that's support to commanders in the field. NSA Georgia has been a leader, and I would expect that to continue and expand in terms of the demands to ensure that there's resilience across the United States SIGINT system, while also partnering and expanding training. The infrastructure that has now been built between the Cyber Center of Excellence and the work that NSA is doing at NSA Georgia is an opportunity for us to ensure that we've got the trained talent, both within NSA and Cyber Command, and NSA Georgia will be significant to that.

Senator OSSOFF. Thank you both for your continued willingness to serve.

Thank you, Mr. Chairman.

Chairman WARNER. Thank you, Senator Ossoff.

All right, I've got one last question. General Haugh, you're going to not be the victim of this question, but I am reinforcing what Senator Lankford brought up about being on the record. You have repeatedly indicated that you are going to continue the efforts of this Committee on security clearance reform and the whole process of security clearance. Is that correct?

Mr. CASEY. That's correct, Senator.

Chairman WARNER. Okay. One way, and remember, I will remind you, you're on the record, one way that you could make that commitment, at least in my mind, more diligent would be a commitment that you will return Jon Rosenwasser's calls within four hours, regardless of where you may be in-country, out-of-country, or anywhere else.

Mr. CASEY. If I'm fortunate enough to be confirmed, sir, I'll certainly look at that issue and get back to you within 60 days.

Chairman WARNER. I think I may borrow Senator Wyden's technique and ask you to give a fulsome response to that in writing.

Senator KING. He'll give that question all the consideration it deserves.

Mr. CASEY. Thank you, Senator King.

Chairman WARNER. Well, once again, Angus King coming to your rescue.

Well, let me let me thank both of you for your testimony and I appreciate Senator King hanging in. You both have imminent qualifications for the jobs you've been nominated for. I want to thank, as I think other Members have mentioned, the fact that your families are both here. These are tough jobs and tough careers to take on.

We appreciate and support their service, as well. And I do want to just note on a personal basis how proud I am of you, Mike, and

the fact that so many former colleagues, of their own volition and on their own time, came up here to show support for you. I think that speaks volumes.

Mr. CASEY. Thank you, Senator. I suspect they had mixed motives.

Chairman WARNER. Well, we are going to hold you on the Rosenwasser thing.

And General Haugh, I think Senator Lankford made a very good point, and you will have no better allies than this Committee on a totally bipartisan basis. But some of the most disappointing times in my tenure here have been when someone, not, say, on purpose, but for whatever reason, had information they didn't share. It then came out, and yet they'd appeared before the Committee previously.

So, leaning in, and if it needs to be on a classified setting, we will understand that. But leaning in to make sure that you share and trust us, we will be that kind of partner.

Any final comments on this? This may be a record. And I want to thank Vice Chairman Rubio for his cooperation on this.

If any Members of the Committee wish to submit questions for the record after today's hearing, please do so no later than noon on Thursday, July 13—Chris, I'm not sure you ever had a turnaround that quick—so that gives you less than 24 hours.

But I'm grateful for the Vice Chairman's cooperation to see if we can move this proceeding along.

Again, Mr. Casey and General Haugh, thank you for appearing before the Committee today. Thank you, as well, to your families. They should all be proud of you, and good luck going forward.

We are adjourned.

(Whereupon the hearing was adjourned at 4:10 p.m.)

SELECT COMMITTEE ON INTELLIGENCE

UNITED STATES SENATE

QUESTIONNAIRE FOR COMPLETION BY PRESIDENTIAL NOMINEES

SELECT COMMITTEE ON INTELLIGENCE
UNITED STATES SENATE

QUESTIONNAIRE FOR COMPLETION BY PRESIDENTIAL NOMINEES

PART A - BIOGRAPHICAL INFORMATION

1. FULL NAME: TIMOTHY D. HAUGH
   OTHER NAMES USED: N/A

2. DATE AND PLACE OF BIRTH: 11 January 1969
   CITIZENSHIP: US

3. MARITAL STATUS: Married

4. SPOUSE'S NAME: Sherie J. Haugh

5. SPOUSE'S MAIDEN NAME IF APPLICABLE: McCallus

6. NAMES AND AGES OF CHILDREN:

NAME	AGE
Redacted	

7. EDUCATION SINCE HIGH SCHOOL:

INSTITUTION	DATES ATTENDED	DEGREE RECEIVED	DATE OF DEGREE
Lehigh University	1987-1991	Bachelor of Arts in Russian Studies	1991
Southern Methodist University	1997-1999	Master of Science in Telecommunications	1999
Naval Postgraduate School	2004-2005	Master of Science in Joint Information Operations	2005
Industrial College of the Armed Forces	2009-2010	Master of Science in National Resource Strategy	2010

8. EMPLOYMENT RECORD (LIST ALL POSITIONS HELD SINCE COLLEGE, INCLUDING MILITARY SERVICE. INDICATE NAME OF EMPLOYER, POSITION, TITLE OR DESCRIPTION, LOCATION, AND DATES OF EMPLOYMENT).

EMPLOYER	POSITION/TITLE	LOCATION	DATES
U.S. Air Force	Deputy Commander, U.S. Cyber Command	Fort George G. Meade, Md	August 2022–present
U.S. Air Force	Commander, Sixteenth Air Force; Commander, Air Forces Cyber, and Commander, Joint Force Headquarters-Cyber	JB San Antonio-Lackland, Texas	October 2019–August 2022
U.S. Air Force	Commander, Twenty-Fifth Air Force	JB San Antonio-Lackland, Texas	August 2019–October 2019
U.S. Air Force	Director of Intelligence, U.S. Cyber Command	Fort George G. Meade, Md.	June 2017–June 2018
U.S. Air Force	Deputy Commander, Joint Task Force-Ares, U.S. Cyber Command	Fort George G. Meade, Md.	June 2016–June 2017
U.S. Air Force	Commander, 480th ISR Wing	JB Langley-Eustis, Va.	June 2014–May 2016
U.S. Air Force	Assistant Vice Commander, Air Force Intelligence, Surveillance, and Reconnaissance Agency	JB San Antonio-Lackland, Texas	July 2013–June 2014
U.S. Air Force	Commander, 318th Information Operations Group	JB San Antonio-Lackland, Texas	July 2011–July 2013
U.S. Air Force	Chief, Intelligence, Surveillance, and Reconnaissance Division, 609th Air Operations Center	Al Udeid AB, Qatar	June 2010–June 2011
U.S. Air Force	Student, Industrial College of the Armed Forces	Fort Lesley J. McNair, Washington, D.C.	July 2009–June 2010
U.S. Air Force	Commander, 315th Network Warfare Squadron	Fort George G. Meade, Md.	June 2007–June 2009
U.S. Air Force	Director of Intelligence, Air Force Special Operations Forces	Hurlburt Field, Fla.	September 2005–June 2007
U.S. Air Force	Student, Naval Postgraduate School	Monterey, Calif.	July 2004–September 2005
U.S. Air Force	Information Operations Project Officer, Headquarters U.S. Air Force, the Pentagon	Arlington, Va.	June 2001–June 2004
U.S. Air Force	Chief, Information Operations Technology Integration, Headquarters Air Intelligence Agency	Kelly AFB, Texas	August 1998–June 2001

U.S. Air Force	Commander, Detachment 2, 544th Intelligence Group	Sabana Seca, Puerto Rico	October 1995–July 1998
U.S. Air Force	Flight Commander, 301st Intelligence Squadron	Misawa Air Base, Japan	January 1993–September 1995
U.S. Air Force	Student, Signals Intelligence Officer Course	Goodfellow Air Force Base, Texas	June 1992–December 1992

9. GOVERNMENT EXPERIENCE (INDICATE EXPERIENCE IN OR ASSOCIATION WITH FEDERAL, STATE, OR LOCAL GOVERNMENTS, INCLUDING ADVISORY, CONSULTATIVE, HONORARY, OR OTHER PART-TIME SERVICE OR POSITION. DO NOT REPEAT INFORMATION ALREADY PROVIDED IN QUESTION 8).

   Summer Intern – PA State Representative Alvin C. Bush, Summers 1988 and 1989.

10. INDICATE ANY SPECIALIZED INTELLIGENCE OR NATIONAL SECURITY EXPERTISE YOU HAVE ACQUIRED HAVING SERVED IN THE POSITIONS DESCRIBED IN QUESTIONS 8 AND/OR 9.

    2012 Chief, Intelligence, Surveillance and Reconnaissance Division, 609th Air Operations Center, Al Udeid Air Base, Qatar, U.S. Central Command, intelligence leader for U.S. and Allied collection and targeting operations in the CENTCOM Area of Responsibility.

    2016 Deputy Commander, JTF-ARES, Fort Meade, MD; attended multiple National Security Council meetings on cyberspace operations.

    2018 Commander, CNMF, Fort Meade, MD; U.S. Cyber Command lead for Russia Small Group, interagency effort to defend 2018 elections.

11. HONORS AND AWARDS (PROVIDE INFORMATION ON SCHOLARSHIPS, FELLOWSHIPS, HONORARY DEGREES, MILITARY DECORATIONS, CIVILIAN SERVICE CITATIONS, OR ANY OTHER SPECIAL RECOGNITION FOR OUTSTANDING PERFORMANCE OR ACHIEVEMENT).

    Air Force ROTC 4-year scholarship
    Air Force Distinguished Service Medal
    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
    National Intelligence Community
    Air Force Commendation Medal
    Air Force Achievement Medal
    National Intelligence Meritorious Unit Citation

12. ORGANIZATIONAL AFFILIATIONS (LIST MEMBERSHIPS IN AND OFFICES HELD WITHIN THE LAST TEN YEARS IN ANY PROFESSIONAL, CIVIC, FRATERNAL, BUSINESS, SCHOLARLY, CULTURAL, CHARITABLE, OR OTHER SIMILAR ORGANIZATIONS).

ORGANIZATION	OFFICE HELD
Air Force Association	Member
Bethany United Methodist Church	Member

13. PUBLISHED WRITINGS AND SPEECHES (LIST THE TITLES, PUBLISHERS, BLOGS AND PUBLICATION DATES OF ANY BOOKS, ARTICLES, REPORTS, OR OTHER PUBLISHED MATERIALS YOU HAVE AUTHORED. ALSO LIST ANY PUBLIC SPEECHES OR REMARKS YOU HAVE MADE WITHIN THE LAST TEN YEARS FOR WHICH THERE IS A TEXT, TRANSCRIPT, OR VIDEO). IF ASKED, WILL YOU PROVIDE A COPY OF EACH REQUESTED PUBLICATION, TEXT, TRANSCRIPT, OR VIDEO?

If asked, I will provide a copy of each available publication, text, transcript, or video.

EVENT	LOCATION	DATE
Speaker – Cyber Commander's Forum No 12	Tallinn, Estonia	May 30 2023
Speaker - Nuclear C3 Summit	Ft Meade, MD	March 22-23 2023
Speaker - Cyber Recon	Ft Meade, MD	April 19 2023
Speaker - Commander's Conference 2022	Norfolk, VA	December 8 2022
Speaker - Senior Leader Speaking Engagement	Ft McNair, DC	November 14 2022
Speaker - FVEY Cyber Week AUS	Canberra, Australia	October 12-19 2022
Speaker - 16 AF Change of Command	San Antonio, TX	July 21 2022
Media Interview: Defense Scoop	Phone interview	July 20 2022
Media Interview: SA Express News	Phone interview	July 20 2022
Speaker - Basic Military Training Graduation	San Antonio, TX	July 14 2022
Keynote Speaker - Cyber Technology for National Security (Lincoln Labs, MIT)	Cambridge, MA	June 29 2022
Speaker - Cyber Commanders' Forum	Estonia	May 30 2022
Media Interview: Recorded Future	Phone interview	April 22 2022
MEDIA INTERVIEW: One-on-One with Recorded Futures Hot Topic: Air Force's Cyber Chief https://www.jbsa.mil/News/Photos/igphoto/2002948432/mediaid/5831905/	Virtual	April 17 2022
Podcast - Sword and Shield Podcast	San Antonio, TX	April 13 2022
Congressional Hearing - Air Force Cyber Mission Force Readiness Statement	Washington, DC	April 05 2022
Speaker - Air Combat Command Technology & Acquisition Sustainment Review	Hampton, VA	March 30 2022
Speaker - Council on Foreign Relations	Virtual	March 28 2022
Speaker - Vice General Officer Summit	Virtual	March 23 2022
Panel - AFA Cyber Ops and the Joint Fight	Orlando, FL	March 04 2022
Interview - RAND Study	San Antonio, TX	February 28 2022
Keynote Speaker - AFCEA Rocky Mountain Cyber Symposium	Colorado Springs, CO	February 23 2022
Keynote Speaker - Cyber Cup https://www.jbsa.mil/News/Photos/igphoto/2002948432/mediaid/5831905/	San Antonio, TX	February 19 2022
Speaker - Fiesta Crows Conference	San Antonio, TX	January 12 2022
Keynote Speaker - DoDIIS 16th Air Force Empowering Innovation and Partnerships	Pre-Recorded	December 5-8 2021
Keynote Speaker - 16th Air Force Changing the Battlespace Through Convergence	San Antonio, Texas	November 16 2021
Keynote: 2021 Alamo AFCEA Chapter Event (AACE)	La Cantera Resort (16641 La Cantera Pkwy, San	November 16 2021

	Antonio, TX 78256)	
Fireside Chat: 12th Annual Billington CyberSecurity Summit	Friendship Heights, MD	October 08 2021
Speaker - Billington CyberSecurity Summit https://www.youtube.com/watch?v=ZRdTw2yiLTs		October 06 2021
Keynote Speaker - Air Force Information Technology and Cyberpower Conference	Montgomery, AL	October 04 2021
Panel Member - Joint Service Academy Cybersecurity Summit - DoD Cyber Commanders: Lessons Learned from a Global Pandemic	Virtual	September 23 2021
Interview - National Defense Magazine	AFA Air Space Cyber Conference, National Harbor, MD	September 22 2021
Panel Member - Air Force Association IW Panel	National Harbor, Maryland	September 22 2021
Media Interview: FWC	AFA Air Space Cyber Conference, National Harbor, MD	September 21 2021
Media Interview: Signal Magazine	AFA Air Space Cyber Conference, National Harbor, MD	September 21 2021
Media Interview: AF Magazine	AFA Air Space Cyber Conference, National Harbor, MD	September 21 2021
Media Interview: C4ISR	AFA Air Space Cyber Conference, National Harbor, MD	September 21 2021
Speaker - Interview w/Mark Pomerleau	National Harbor, Maryland	September 20 2021
Speaker - Air Force Association (Media Roundtable)	National Harbor, Maryland	September 20 2021
Panelist: Digital Strategy Workshop Series - The National Academies of Sciences - Engineering - Medicine	Virtual	September 02 2021
Speaker - San Antonio Chamber of Commerce	The Red Berry Estate's Lakeside Ballroom (856 Gembler Road San Antonio, Texas 78219)	August 18 2021
Speaker (virtual Zoom audio segment) - Defense and Aerospace Report - 16 AF Overview	Virtual	August 09 2021
Mission Brief: San Antonio Chamber of Commerce visit to 16 AF	HQ 16 AF	July 23 2021
Keynote Speaker - Air Force Information Technology and Cyberpower Conference	Montgomery, AL	July 22 2021
Speaker - San Antonio Chamber of Commerce	San Antonio, Texas	July 20 2021
Keynote: National Defense Industrial Association JADC2 & All Domain Warfare Symposium	Texas A&M University in	July 14 2021

	College Station, TX	
Speaker - MIT Lincoln Labs Engagement - Current/Future Outlook		July 01 2021
Speaker (virtual) - Senator Cornyn Cadet Sendoff	Virtual	May 31 2021
Keynote: 16 AF visit to University of Texas San Antonio's National Security Collaboration Center	UTSA Main Campus (One UTSA Circle, San Antonio, Texas 78249)	May 20 2021
Media Interview: Aero Aerospace & Defense	Phone interview	April 14, 2021
Speaker - Sword and Shield Podcast on what Convergence means to a Cyber Wing https://podcasts.apple.com/us/podcast/sword-and-shield-podcast-ep-53-competition-in-cyberspace/id1520065733?i=1000526267802	JBSA - San Antonio	May 18 2021
Speaker (via Zoom) - San Antonio Mayor's Cyber Cup https://www.youtube.com/watch?v=OilMpTqOVoY	Virtual	March 13 2021
Speaker (via Zoom) - Rocky Mountain Cyberspace Symposium 16 AF Update and "The Other Airmen"	Virtual - Colorado Springs	March 11 2021
Keynote Speaker (via video) - San Antonio Mayor's Cup Awards / College Fair	Virtual - San Antonio	February 27 2021
Speaker - Hoover Institute Chat Series - Agile Collaboration in the Defense of the Nation	Hoover Instititue	February 26 2021
Keynote: 13O Graduation	Virtual/Recording	November 20 2020
Speaking: ALAMO ACE	San Antonio, TX	November 16-19 2020
Panelist: NDIA Panel	Virtual	October 28 2020
Keynote: Baylor Address	Det 810 Waco, TX	September 16 2020
Panelist: AFA cASC Panel Discussion	Virtual	September 14-17 2020
Media: Billington Cyber Security Article https://billingtoncybersecurity.com/air-force-must-change-the-way-it-thinks-to-win-new-age-of-information-wars/	Virtual	September 09 2020
Discussion: Business Executives for National Security	Virtual Event	September 10, 2020
Panelist: AFA Infor Warfare	Virtual	September 01 2020
Media: Airmen in the Fight: AFA Welcomes Sixteenth Air Force https://www.youtube.com/watch?v=-jutVpn7r3k	Virtual	August 13 2020
Media: Fireside Keynote with Lt General Tim Haugh Fed Supernova https://www.youtube.com/watch?v=Ce7bWIGCcxU&pp=ygUMbHQgZ2VuIGh1YWdo	Virtual	August 04 2020
Keynote Speaker: AFITIC	Virtual	August 27 2020
Speaker: Washington Capitol AFA	Washington, DC	August 13 2020
ARTICLE: 16th Air Force and Convergence for the Information War https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/Haugh_Hall_Fan_CDR%20V5N2%20Summer%202020.pdf?ver=2020-07-27-053232-357		July 27 2020

Media: Fireside Chat (Fed SuperNova)	Virtual	July 16 2020
Speaker: Aerospace Nation		July 15 2020
Speaker: CSIA Presentation		June 11 2020
Speaker: RAND Discussion		June 10 2020
Panelist: Washington Executive DoD Council	Washington, DC	June 04 2020
Keynote Speaker: CORONA	Wright Patterson, AFB	June 02 2020
Media: IW Convergence Article	Virtual	May 04 2020
KLE: San Antonio Chamber Leaders Visit	JBSA-Lackland, TX	April 27 2020
Keynote Speaker: Alamo AFCEA Luncheon	San Antonio, TX	April 21 2020
Keynote Speaker: AFA Symposium	Langley, VA	April 16 2020
Keynote Speaker: IW Symposium	Washington, DC	March 11-12 2020
Keynote Speaker: FTVA (Freedom Through Vigilance Association)	San Antonio, TX	March 21 2020
Keynote Speaker: AF Operations Research Symposium	Washington, DC	March 16 2020
Keynote Speaker: SA Cyber Cup/Mayors Cup	San Antonio, TX	February 29 2020
Keynote Speaker: Reserve Component Summit	Fort George G. Meade, Maryland	February 7-8 2020
Keynote Speaker: Rocky Mntn Cyber Symp https://www.youtube.com/watch?v=AoeBjSvkRzc	Colorado Springs, CO	February 06 2020
Keynote Speaker: Aerospace Nation	Virtual	January 19 2020
SPEAKER: 2019 AFA Hot Topic: 16 AF Mission Brief/Combined Slide with HAF	National Harbor, MD	November 11 2019
KEYNOTE: Alamo AFCEA Hot Topics: 16AF Mission Brief	JBSA Lackland, TX	November 18 2019
KEYNOTE: 16 AF NAF Standup Hot Topic: Activation of 16AF IW NAF	JBSA Lackland, TX	October 11 20219
KEYNOTE: 2019 FTVA Hot Topics: Alumni For 25th / 24th AF Contributions to ISR and AF	JBSA Lackland, TX	October 5 2019
KEYNOTE: 2019 ICCE - https://www.youtube.com/watch?v=ILcKZnwX_Rw		September 29 2019
PANELIST: 2019 AFA Symposium. Hot Topics: Cyber Effects in the MDO Environment https://www.youtube.com/watch?v=qZt2s22NukQ	National Harbor, MD	September 16-18 2019
ARTICLE: Improving Outcomes: Intelligence, Surveillance, and Reconnaissance Assessment https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-31_Issue-4/SLP-Haugh_Leonard.pdf	Maxwell AFB, AL	November 27 2017
ARTICLE: The Sadr II Movement: An Organizational Fight for Legitimacy within the Iraqi Shi'a Community Strategic Insights https://apps.dtic.mil/sti/pdfs/ADA521548.pdf		May 2005

PART B - QUALIFICATIONS

14. QUALIFICATIONS (DESCRIBE WHY YOU BELIEVE YOU ARE QUALIFIED TO SERVE AS THE DIRECTOR OF THE NATIONAL SECURITY AGENCY).

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. I have commanded intelligence units at the Squadron, Wing, and Numbered Air Force level and served as a designated Senior Intelligence Officer in Special Operations, a Combatant Command, and multiple Air Force intelligence units in garrison or deployed. Initially trained as a Signals Intelligence officer, I have served in a total of seven intelligence assignments at NSA field sites, the NSA HQ, and within the Air Force's cryptologic component. In additional cyber assignments, I have been part of combined operations with NSA that allowed me to partner with or support NSA's Cybersecurity and Signals Intelligence missions. I have been honored to serve with NSA for a majority of my career and have a deep appreciation for the incredibly talented NSA professionals that execute NSA's important missions in service of the nation.

PART C - POLITICAL AND FOREIGN AFFILIATIONS

15. POLITICAL ACTIVITIES (LIST ANY MEMBERSHIPS OR OFFICES HELD IN OR FINANCIAL CONTRIBUTIONS OR SERVICES RENDERED TO, ANY POLITICAL PARTY, ELECTION COMMITTEE, POLITICAL ACTION COMMITTEE, OR INDIVIDUAL CANDIDATE DURING THE LAST TEN YEARS).

None

16. CANDIDACY FOR PUBLIC OFFICE (FURNISH DETAILS OF ANY CANDIDACY FOR ELECTIVE PUBLIC OFFICE).

None

17. FOREIGN AFFILIATIONS

(NOTE: QUESTIONS 17A AND B ARE NOT LIMITED TO RELATIONSHIPS REQUIRING REGISTRATION UNDER THE FOREIGN AGENTS REGISTRATION ACT. QUESTIONS 17A, B, AND C DO NOT CALL FOR A POSITIVE RESPONSE IF THE REPRESENTATION OR TRANSACTION WAS AUTHORIZED BY THE UNITED STATES GOVERNMENT IN CONNECTION WITH YOUR OR YOUR SPOUSE'S EMPLOYMENT IN GOVERNMENT SERVICE.)

A. HAVE YOU OR YOUR SPOUSE EVER REPRESENTED IN ANY CAPACITY (E.G. EMPLOYEE, ATTORNEY, OR POLITICAL/BUSINESS CONSULTANT), WITH OR WITHOUT COMPENSATION, A FOREIGN GOVERNMENT OR AN ENTITY CONTROLLED BY A FOREIGN GOVERNMENT? IF SO, PLEASE FULLY DESCRIBE SUCH RELATIONSHIP.

No

B. HAVE ANY OF YOUR OR YOUR SPOUSE'S ASSOCIATES REPRESENTED, IN ANY CAPACITY, WITH OR WITHOUT COMPENSATION, A FOREIGN GOVERNMENT OR AN ENTITY CONTROLLED BY A FOREIGN GOVERNMENT? IF SO, PLEASE FULLY DESCRIBE SUCH RELATIONSHIP.

No

C. DURING THE PAST TEN YEARS, HAVE YOU OR YOUR SPOUSE RECEIVED ANY COMPENSATION FROM, OR BEEN INVOLVED IN ANY FINANCIAL OR BUSINESS

TRANSACTIONS WITH, A FOREIGN GOVERNMENT OR ANY ENTITY CONTROLLED BY A FOREIGN GOVERNMENT? IF SO, PLEASE PROVIDE DETAILS.

No

D. HAVE YOU OR YOUR SPOUSE EVER REGISTERED UNDER THE FOREIGN AGENTS REGISTRATION ACT? IF SO, PLEASE PROVIDE DETAILS.

No

18. DESCRIBE ANY LOBBYING ACTIVITY DURING THE PAST TEN YEARS, OTHER THAN IN AN OFFICIAL U.S. GOVERNMENT CAPACITY, IN WHICH YOU OR YOUR SPOUSE HAVE ENGAGED FOR THE PURPOSE OF DIRECTLY OR INDIRECTLY INFLUENCING THE PASSAGE, DEFEAT, OR MODIFICATION OF FEDERAL LEGISLATION, OR FOR THE PURPOSE OF AFFECTING THE ADMINISTRATION AND EXECUTION OF FEDERAL LAW OR PUBLIC POLICY.

None

PART D - FINANCIAL DISCLOSURE AND CONFLICT OF INTEREST

19. DESCRIBE ANY EMPLOYMENT, BUSINESS RELATIONSHIP, FINANCIAL TRANSACTION, INVESTMENT, ASSOCIATION, OR ACTIVITY (INCLUDING, BUT NOT LIMITED TO, DEALINGS WITH THE FEDERAL GOVERNMENT ON YOUR OWN BEHALF OR ON BEHALF OF A CLIENT), WHICH COULD CREATE, OR APPEAR TO CREATE, A CONFLICT OF INTEREST IN THE POSITION TO WHICH YOU HAVE BEEN NOMINATED.

None

20. DO YOU INTEND TO SEVER ALL BUSINESS CONNECTIONS WITH YOUR PRESENT EMPLOYERS, FIRMS, BUSINESS ASSOCIATES AND/OR PARTNERSHIPS, OR OTHER ORGANIZATIONS IN THE EVENT THAT YOU ARE CONFIRMED BY THE SENATE? IF NOT, PLEASE EXPLAIN.

N/A

21. DESCRIBE THE FINANCIAL ARRANGEMENTS YOU HAVE MADE OR PLAN TO MAKE, IF YOU ARE CONFIRMED, IN CONNECTION WITH SEVERANCE FROM YOUR CURRENT POSITION. PLEASE INCLUDE SEVERANCE PAY, PENSION RIGHTS, STOCK OPTIONS, DEFERRED INCOME ARRANGEMENTS, AND ANY AND ALL COMPENSATION THAT WILL OR MIGHT BE RECEIVED IN THE FUTURE AS A RESULT OF YOUR CURRENT BUSINESS OR PROFESSIONAL RELATIONSHIPS.

None

22. DO YOU HAVE ANY PLANS, COMMITMENTS, OR AGREEMENTS TO PURSUE OUTSIDE EMPLOYMENT, WITH OR WITHOUT COMPENSATION, DURING YOUR SERVICE WITH THE GOVERNMENT? IF SO, PLEASE PROVIDE DETAILS.

No

23. AS FAR AS CAN BE FORESEEN, STATE YOUR PLANS AFTER COMPLETING GOVERNMENT SERVICE. PLEASE SPECIFICALLY DESCRIBE ANY AGREEMENTS OR UNDERSTANDINGS, WRITTEN OR UNWRITTEN, CONCERNING EMPLOYMENT AFTER LEAVING GOVERNMENT SERVICE. IN PARTICULAR, DESCRIBE ANY AGREEMENTS, UNDERSTANDINGS, OR OPTIONS TO RETURN TO YOUR CURRENT POSITION.

I have no agreements or understandings concerning employment following government service.

24. IF YOU ARE PRESENTLY IN GOVERNMENT SERVICE, DURING THE PAST FIVE YEARS OF SUCH SERVICE, HAVE YOU RECEIVED FROM A PERSON OUTSIDE OF GOVERNMENT AN OFFER OR EXPRESSION OF INTEREST TO EMPLOY YOUR SERVICES AFTER YOU LEAVE GOVERNMENT SERVICE? IF YES, PLEASE PROVIDE DETAILS.

No

25. IS YOUR SPOUSE EMPLOYED? IF YES AND THE NATURE OF THIS EMPLOYMENT IS RELATED IN ANY WAY TO THE POSITION FOR WHICH YOU ARE SEEKING CONFIRMATION, PLEASE INDICATE YOUR SPOUSE'S EMPLOYER, THE POSITION, AND THE LENGTH OF TIME THE POSITION HAS BEEN HELD. IF YOUR SPOUSE'S EMPLOYMENT IS NOT RELATED TO THE POSITION TO WHICH YOU HAVE BEEN NOMINATED, PLEASE SO STATE.

No

26. LIST BELOW ALL CORPORATIONS, PARTNERSHIPS, FOUNDATIONS, TRUSTS, OR OTHER ENTITIES TOWARD WHICH YOU OR YOUR SPOUSE HAVE FIDUCIARY OBLIGATIONS OR IN WHICH YOU OR YOUR SPOUSE HAVE HELD DIRECTORSHIPS OR OTHER POSITIONS OF TRUST DURING THE PAST FIVE YEARS.

NAME OF ENTITY	POSITION	DATES HELD	SELF OR SPOUSE

None

27. LIST ALL GIFTS EXCEEDING $100 IN VALUE RECEIVED DURING THE PAST FIVE YEARS BY YOU, YOUR SPOUSE, OR YOUR DEPENDENTS. (NOTE: GIFTS RECEIVED FROM RELATIVES AND GIFTS GIVEN TO YOUR SPOUSE OR DEPENDENT NEED NOT BE INCLUDED UNLESS THE GIFT WAS GIVEN WITH YOUR KNOWLEDGE AND ACQUIESCENCE AND YOU HAD REASON TO BELIEVE THE GIFT WAS GIVEN BECAUSE OF YOUR OFFICIAL POSITION.)

None

28. LIST ALL SECURITIES, REAL PROPERTY, PARTNERSHIP INTERESTS, OR OTHER INVESTMENTS OR RECEIVABLES WITH A CURRENT MARKET VALUE (OR, IF MARKET VALUE IS NOT ASCERTAINABLE, ESTIMATED CURRENT FAIR VALUE) IN EXCESS OF $1,000. (NOTE: THE INFORMATION PROVIDED IN RESPONSE TO SCHEDULE A OF THE DISCLOSURE FORMS OF THE OFFICE OF GOVERNMENT ETHICS MAY BE INCORPORATED BY REFERENCE, PROVIDED THAT CURRENT VALUATIONS ARE USED.)

DESCRIPTION OF PROPERTY	VALUE	METHOD OF VALUATION

See executive branch personnel public financial disclosure report (OGE Form 278e)

29. LIST ALL LOANS OR OTHER INDEBTEDNESS (INCLUDING ANY CONTINGENT LIABILITIES) IN EXCESS OF $10,000. EXCLUDE A MORTGAGE ON YOUR PERSONAL RESIDENCE UNLESS IT IS RENTED OUT, AND LOANS SECURED BY AUTOMOBILES, HOUSEHOLD FURNITURE, OR APPLIANCES. (NOTE: THE INFORMATION PROVIDED IN RESPONSE TO SCHEDULE C OF THE DISCLOSURE FORM OF THE OFFICE OF GOVERNMENT ETHICS MAY BE INCORPORATED BY REFERENCE, PROVIDED THAT CONTINGENT LIABILITIES ARE ALSO INCLUDED.)

NATURE OF OBLIGATION	NAME OF OBLIGEE	AMOUNT

See executive branch personnel public financial disclosure report (OGE Form 278e)

30. ARE YOU OR YOUR SPOUSE NOW IN DEFAULT ON ANY LOAN, DEBT, OR OTHER FINANCIAL OBLIGATION? HAVE YOU OR YOUR SPOUSE BEEN IN DEFAULT ON ANY LOAN, DEBT, OR OTHER FINANCIAL OBLIGATION IN THE PAST TEN YEARS? HAVE YOU OR YOUR SPOUSE EVER BEEN REFUSED CREDIT OR HAD A LOAN APPLICATION DENIED? IF THE ANSWER TO ANY OF THESE QUESTIONS IS YES, PLEASE PROVIDE DETAILS.

No

31. LIST THE SPECIFIC SOURCES AND AMOUNTS OF ALL INCOME RECEIVED DURING THE LAST FIVE YEARS, INCLUDING ALL SALARIES, FEES, DIVIDENDS, INTEREST, GIFTS, RENTS, ROYALTIES, PATENTS, HONORARIA, AND OTHER ITEMS EXCEEDING $200. (COPIES OF U.S. INCOME TAX RETURNS FOR THESE YEARS MAY BE SUBSTITUTED HERE, BUT THEIR SUBMISSION IS NOT REQUIRED.)

	2018	2019	2020	2021	2022
SALARIES	Redacted				
DIVIDENDS					
TOTAL					

32. IF ASKED, WILL YOU PROVIDE THE COMMITTEE WITH COPIES OF YOUR AND YOUR SPOUSE'S FEDERAL INCOME TAX RETURNS FOR THE PAST THREE YEARS?

Yes

33. LIST ALL JURISDICTIONS IN WHICH YOU AND YOUR SPOUSE FILE ANNUAL INCOME TAX RETURNS.

Federal only (Pasco County, Florida resident)

34. HAVE YOUR FEDERAL OR STATE TAX RETURNS BEEN THE SUBJECT OF AN AUDIT, INVESTIGATION, OR INQUIRY AT ANY TIME? IF SO, PLEASE PROVIDE DETAILS, INCLUDING THE RESULT OF ANY SUCH PROCEEDING.

No

35. IF YOU ARE AN ATTORNEY, ACCOUNTANT, OR OTHER PROFESSIONAL, PLEASE LIST ALL CLIENTS AND CUSTOMERS WHOM YOU BILLED MORE THAN $200 WORTH OF SERVICES DURING THE PAST FIVE YEARS. ALSO, LIST ALL JURISDICTIONS IN WHICH YOU ARE LICENSED TO PRACTICE.

N/A

36. DO YOU INTEND TO PLACE YOUR FINANCIAL HOLDINGS AND THOSE OF YOUR SPOUSE AND DEPENDENT MEMBERS OF YOUR IMMEDIATE HOUSEHOLD IN A BLIND TRUST? IF YES, PLEASE FURNISH DETAILS. IF NO, DESCRIBE OTHER ARRANGEMENTS FOR AVOIDING ANY POTENTIAL CONFLICTS OF INTEREST.

No

37. IF APPLICABLE, LIST THE LAST THREE YEARS OF ANNUAL FINANCIAL DISCLOSURE REPORTS YOU HAVE BEEN REQUIRED TO FILE WITH YOUR AGENCY, DEPARTMENT, OR BRANCH OF GOVERNMENT. IF ASKED, WILL YOU PROVIDE A COPY OF THESE REPORTS?

2020, 2021, 2022 – I will provide if asked.

PART E - ETHICAL MATTERS

38. HAVE YOU EVER BEEN THE SUBJECT OF A DISCIPLINARY PROCEEDING OR CITED FOR A BREACH OF ETHICS OR UNPROFESSIONAL CONDUCT BY, OR BEEN THE SUBJECT OF A COMPLAINT TO, ANY COURT, ADMINISTRATIVE AGENCY, PROFESSIONAL ASSOCIATION, DISCIPLINARY COMMITTEE, OR OTHER PROFESSIONAL GROUP? IF SO, PLEASE PROVIDE DETAILS.

No

39. HAVE YOU EVER BEEN INVESTIGATED, HELD, ARRESTED, OR CHARGED BY ANY FEDERAL, STATE, OR OTHER LAW ENFORCEMENT AUTHORITY FOR VIOLATION OF ANY FEDERAL STATE, COUNTY, OR MUNICIPAL LAW, REGULATION, OR ORDINANCE, OTHER THAN A MINOR TRAFFIC OFFENSE, OR NAMED AS A DEFENDANT OR OTHERWISE IN ANY INDICTMENT OR INFORMATION RELATING TO SUCH VIOLATION? IF SO, PLEASE PROVIDE DETAILS.

No

40. HAVE YOU EVER BEEN CONVICTED OF OR ENTERED A PLEA OF GUILTY OR NOLO CONTENDERE TO ANY CRIMINAL VIOLATION OTHER THAN A MINOR TRAFFIC OFFENSE? IF SO, PLEASE PROVIDE DETAILS.

No

41. ARE YOU PRESENTLY OR HAVE YOU EVER BEEN A PARTY IN INTEREST IN ANY ADMINISTRATIVE AGENCY PROCEEDING OR CIVIL LITIGATION? IF SO, PLEASE PROVIDE DETAILS.

No

42. HAVE YOU BEEN INTERVIEWED OR ASKED TO SUPPLY ANY INFORMATION AS A WITNESS OR OTHERWISE IN CONNECTION WITH ANY CONGRESSIONAL INVESTIGATION, FEDERAL, OR STATE AGENCY PROCEEDING, GRAND JURY INVESTIGATION, OR CRIMINAL OR CIVIL LITIGATION IN THE PAST TEN YEARS? IF SO, PLEASE PROVIDE DETAILS.

No

43. HAS ANY BUSINESS OF WHICH YOU ARE OR WERE AN OFFICER, DIRECTOR, OR PARTNER BEEN A PARTY TO ANY ADMINISTRATIVE AGENCY PROCEEDING OR CRIMINAL OR CIVIL LITIGATION RELEVANT TO THE POSITION TO WHICH YOU HAVE BEEN NOMINATED? IF SO, PLEASE PROVIDE DETAILS. (WITH RESPECT TO A BUSINESS OF WHICH YOU ARE OR WERE AN OFFICER, YOU NEED ONLY CONSIDER PROCEEDINGS AND LITIGATION THAT OCCURRED WHILE YOU WERE AN OFFICER OF THAT BUSINESS.)

No

44. HAVE YOU EVER BEEN THE SUBJECT OF ANY INSPECTOR GENERAL INVESTIGATION? IF SO, PLEASE PROVIDE DETAILS.

In August 2016, the Air Force received an IG compliant from a civilian under my command following disciplinary action. The complaint was investigated by SAF/IG and determined to be an unsubstantiated complaint.

PART F - SECURITY INFORMATION

45. HAVE YOU EVER BEEN DENIED ANY SECURITY CLEARANCE OR ACCESS TO CLASSIFIED INFORMATION FOR ANY REASON? IF YES, PLEASE EXPLAIN IN DETAIL.

No

46. HAVE YOU BEEN REQUIRED TO TAKE A POLYGRAPH EXAMINATION FOR ANY SECURITY CLEARANCE OR ACCESS TO CLASSIFIED INFORMATION? IF YES, PLEASE EXPLAIN.

2023 – National Security Agency
2016 – Air Force Office of Special Investigations
2007 – Air Force Office of Special Investigations

47. HAVE YOU EVER REFUSED TO SUBMIT TO A POLYGRAPH EXAMINATION? IF YES, PLEASE EXPLAIN.

No

PART G - ADDITIONAL INFORMATION

48. DESCRIBE IN YOUR OWN WORDS THE CONCEPT OF CONGRESSIONAL OVERSIGHT OF U.S. INTELLIGENCE ACTIVITIES. IN PARTICULAR, CHARACTERIZE WHAT YOU BELIEVE TO BE THE OBLIGATIONS OF THE DIRECTOR OF THE NATIONAL SECURITY AGENCY AND THE INTELLIGENCE COMMITTEES OF THE CONGRESS, RESPECTIVELY, IN THE OVERSIGHT PROCESS.

Foundational to our democracy and in adherence with the Constitution, Congress has an essential role in oversight of the executive branch. Specifically, the Intelligence Committees provide oversight of U.S. intelligence activities; ensuring compliance with the law and enabling public trust and confidence in the Intelligence Community. The Director of the National Security Agency must be a leader trusted by Congress to provide timely, accurate, and complete reports on intelligence activities, expenditure of resources and issues or incidents impacting the Agency. Ultimately, the Director of the National Security Agency is responsible for setting a culture of compliance and the Intelligence Committees of Congress provide oversight to ensure intelligence activities are resourced and conducted consistent with the laws, policies, and values of the United States of America.

49. EXPLAIN YOUR UNDERSTANDING OF THE RESPONSIBILITIES OF THE DIRECTOR OF THE NATIONAL SECURITY AGENCY.

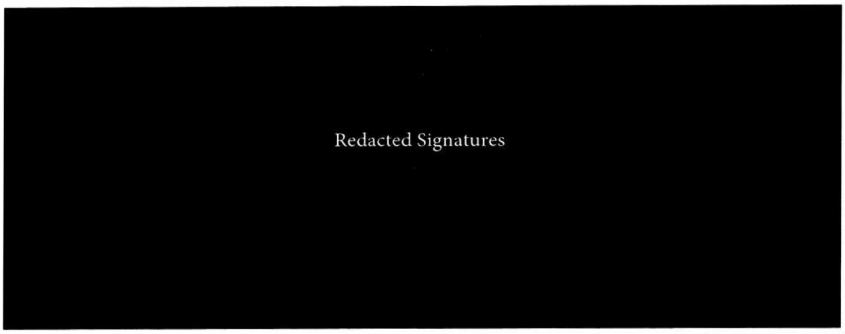
NSA is the U.S. government lead for cryptology and performs both Signals Intelligence and Cybersecurity missions. The Director of the National Security Agency has three primary roles: 1. As the SIGINT Functional Manager, serves as the U.S. government's executive agent for Signals Intelligence; 2. As the National Manger for National Security Systems serves as the U.S. government focal point for cryptography and cybersecurity for national security systems; and 3. Serves as a Combat Support Agency for the Department of Defense.

The Director of the National Security Agency is also the Chief of the Central Security Service, which includes the elements of the armed forces, Army, Navy, Air Force, Marines, Coast Guard, and Space force, which conduct cryptologic activities with NSA.

The Director of the National Security Agency is also the Commander, U.S. Cyber Command, responsible to execute combatant commander responsibilities as designated in law and policy.

AFFIRMATION

I, **LIEUTENANT GENERAL TIMOTHY D. HAUGH**, DO SWEAR THAT THE ANSWERS I HAVE PROVIDED TO THIS QUESTIONNAIRE ARE ACCURATE AND COMPLETE.



_____

SELECT COMMITTEE ON
INTELLIGENCE

UNITED STATES SENATE

Additional Prehearing Questions for

Lieutenant General Timothy D. Haugh

Upon his nomination to be Director of the National Security Agency

Responsibilities of the Director of the National Security Agency

QUESTION 1: The role of Director of the National Security Agency (DIRNSA) has been performed differently depending on what the President has requested from the position. What do you see as your role as DIRNSA, if confirmed to this position? How do you expect it to be different than that of your predecessor?

QUESTION 2: The congressional intelligence committees have supported the Intelligence Community's (IC's) evaluation of dual-hatting the Commander of U.S. Cyber Command and DIRNSA positions.

a. Which DIRNSA roles and responsibilities would be affected by a cessation of the dual-hat regime?

b. Which roles and responsibilities as the Commander of U.S. Cyber Command would be affected by a cessation of the dual-hat regime?

c. What in your view are the positive and negative aspects of a dual-hat regime? Please provide details in supporting your position, and include assessments of structure, budgetary procedures, and oversight of NSA, as well as U.S. Cyber Command.

QUESTION 3: What is your view on the dual-track supervision of NSA by the Secretary of Defense and the Director of National Intelligence?

QUESTION 4: How will you balance the four discrete responsibilities you will have to execute as the Director of NSA, the Chief of the Central Security Service, the Commander of U.S. Cyber Command, and the National Manager for National Security Systems?

QUESTION 5: Please describe which of those roles do you believe is most important, and why. Please provide supporting details in your answer.

QUESTION 6: Please describe the specific experiences you have had in your professional career that will enable you to serve effectively as the Director of the NSA. In addition, what lessons have you drawn from the experiences of current and former DIRNSAs?

QUESTION 7: If confirmed as DIRNSA, what steps will you take to improve the integration, coordination, and collaboration between NSA and the other IC agencies?

QUESTION 8: If confirmed as DIRNSA, how will you ensure that the tasking of NSA resources and personnel to support U.S. Cyber Command do not negatively impact NSA's ability to perform and fulfill core missions?

QUESTION 9: If confirmed as DIRNSA, how will you ensure that U.S. Cyber Command operations and mission do not impact NSA operations and mission?

Keeping the Congressional Intelligence Committees Fully and Currently Informed

QUESTION 10: Please describe your view of the NSA's obligation to respond to requests for information from Members of Congress.

QUESTION 11: Does NSA have a responsibility to correct the record, if it identifies occasions where inaccurate information has been provided to the congressional intelligence committees?

QUESTION 12: Please describe your view on when it is appropriate to withhold pertinent and timely information from the congressional intelligence committees.

Functions and Responsibilities of the National Security Agency

QUESTION 13: What do you consider to be the most important missions of the NSA?

QUESTION 14: How well do you think the NSA has performed recently in each of these missions?

QUESTION 15: If confirmed, what missions do you expect to direct the NSA to prioritize over others?

QUESTION 16: Every previous dual-hatted Director of NSA has experienced at least one major security incident under their leadership. What steps will you take to ensure this trend does not continue?

National Security Threats and Challenges Facing the Intelligence Community

QUESTION 17: What, in your view, are the current principal threats to national security most relevant to the NSA?

QUESTION 18: What role do you see for the NSA, in particular, and the IC, as a whole, with respect to the ongoing challenge of ubiquitous encryption as it pertains to foreign intelligence?

QUESTION 19: Do you believe that the IC needs additional statutory authorities to address the proliferation of ubiquitous commercial encryption?

Foreign Intelligence Surveillance Act

QUESTION 20: Title VII of the Foreign Intelligence Surveillance Act (FISA) will sunset on December 31, 2023, including what is commonly known as Section 702. If Section 702 authorities were to end or even be diminished, what would be the impact on national security?

QUESTION 21: Please describe why it necessary for NSA to have the ability to perform U.S. person queries of information acquired pursuant to Section 702 of FISA. What would the implications be in NSA was required to seek a warrant and probable cause prior to performing such queries?

QUESTION 22: Please clarify what is meant by "incidental collection." Can the IC use this collection to target U.S. persons? If not, what value does incidental collection have in the NSA's ability to protect our national security from counterterrorism and counterintelligence threats?

QUESTION 23: Please describe the compliance regime that the NSA has in place for its Section 702 collection authorities.

QUESTION 24: What compliance regime does U.S. Cyber Command have in place to ensure proper access to Section 702 collection?

Cybersecurity

QUESTION 25: What role do you see for the NSA in defensive cybersecurity policies or actions? What role do you see for NSA in supporting any U.S. Government offensive cybersecurity policies or actions?

QUESTION 26: What should be the NSA's role in helping to protect U.S. commercial computer networks that are not part of the defense industrial base?

QUESTION 27: What cyber threat information (classified or unclassified) should be shared with U.S. private sector entities, particularly critical infrastructure entities, to enable them to protect their networks from possible cyberattacks?

QUESTION 28: Should NSA publish finished cybersecurity intelligence products? Why or why not?

NSA Capabilities

QUESTION 29: What are your views concerning the quality of intelligence collection conducted by the NSA, and what is your assessment of the steps that have been taken to date to improve that collection?

QUESTION 30: If confirmed, what additional steps would you pursue to improve intelligence collection and what benchmarks will you use to judge the success of future collection efforts by the NSA?

QUESTION 31: What is your assessment of the quality of current NSA intelligence analysis?

QUESTION 32: If confirmed, what additional steps would you take to improve intelligence analysis, and what benchmarks will you use to judge the success of future NSA analytic efforts?

QUESTION 33: What is your view of strategic analysis and its place within the NSA? Please include your views about what constitutes such analysis, what steps should be taken to ensure adequate strategic coverage of important issues, and what finished intelligence products NSA should produce.

QUESTION 34: What are your views on the role of foundational research to NSA's mission?

NSA Personnel

QUESTION 35: What is your view of the principles that should guide the NSA in its use of contractors, rather than full-time government employees, to fulfill intelligence-related functions?

a. Are there functions within the NSA that are particularly suited for the use of contractors?

b. Are there some functions that should never be conducted by contractors, or for which use of contractors should be discouraged or require specific DIRNSA approvals?

c. What consideration should the NSA give to the cost of contractors versus government employees?

d. What does the NSA need in order to achieve an appropriate balance between government civilians, military personnel, and contractors?

QUESTION 36: What is your assessment of the personnel accountability system in place at the NSA?

QUESTION 37: What actions, if any, should be considered to ensure that the IC has a fair process for handling personnel accountability, including serious misconduct allegations?

Security Clearance Reform

QUESTION 38: What are your views on the security clearance process?

QUESTION 39: If confirmed, what changes, if any, would you seek to make to this process?

QUESTION 40: Should civilians, military, and contractor personnel be held to the same security clearance and adjudication standards for access to NSA facilities, computer systems, and information?

Management of the National Security Agency

QUESTION 41: In what ways can DIRNSA achieve sufficient independence and distance from political considerations to serve the nation with objective and dispassionate intelligence collection and analysis?

a. If confirmed, how will you ensure this independence is maintained?

b. What is your view of DIRNSA's responsibility to inform senior Administration policy officials or their spokespersons when the available intelligence either does not support or contradicts public statements they may have made?

QUESTION 42: How would you resolve a situation in which the assessments of your analysts are at odds with the policy aspirations of the administration?

QUESTION 43: What are your views of the current NSA culture and workforce?

a. What are your goals for NSA's culture and workforce?

b. If confirmed, what are the steps you plan to take to achieve these goals?

c. How will you strengthen the relationship between the civilian and military members of the NSA workforce?

Transparency

QUESTION 44: Do you believe that intelligence agencies need some level of transparency to ensure long-term public support for their activities?

QUESTION 45: If confirmed, what would be your approach to transparency?

Disclosures of Classified Information

QUESTION 46: In your view, does the NSA take appropriate precautions to protect classified information and prevent, deter, investigate, and punish unauthorized disclosures of classified information?

QUESTION 47: If confirmed, how will you ensure that appropriate and necessary precautions to protect classified information are maintained and improved, if necessary?

QUESTION 48: If confirmed, how would you manage the following issues:

a. The vulnerability of NSA information systems to harm or espionage by trusted insiders;

b. The vulnerability of NSA information systems to outside penetration;

c. The readiness of NSA to maintain continuity of operations;

d. The ability of NSA to adopt advanced information technology efficiently and effectively; and

e. The NSA's recruitment and retention of skilled STEM and information technology professionals, including contractor personnel.

QUESTION 49: How do you think that individuals who mishandle, intentionally or unintentionally, classified information should be dealt with?

SELECT COMMITTEE ON INTELLIGENCE

UNITED STATES SENATE

Post-hearing Questions For

Lieutenant General Timothy D. Haugh

upon his nomination to be

Director of the National Security Agency

QUESTIONS FOR THE RECORD

From Vice Chairman Rubio

General Oversight

1. How will you ensure that the Committee maintains current and full awareness of the National Security Agency's (NSA's) activities and intelligence reporting?

   If confirmed, I will be committed to keeping the congressional intelligence committees fully and currently informed of NSA's intelligence activities, as it is not appropriate to withhold information that is within the jurisdiction of any congressional committee. I, and my delegates, will provide the information necessary to keep the Committee currently and fully aware, to include following established procedures for briefing the most sensitive matters.

2. Will you commit to us that you will be responsive to Committee requests for briefings and meetings, and ensure that we are notified in a timely manner of significant activities within our jurisdiction?

   Yes, I commit to being responsive to Committee requests and ensuring timely notifications of significant activities within the Committee's jurisdiction.

3. If asked by the Committee, will you provide the sourcing behind the NSA's finished products and assessments?

   If confirmed, I commit to accommodating the Committee's need for information in order for the Committee to perform its critical oversight function.

4. If asked by the Committee, will you provide the raw reporting that underpins IC finished products and assessments?

   If confirmed, I commit to accommodating the Committee's need for information in order for the Committee to perform its critical oversight function.

5. Do you commit to ensuring that this Committee has access to all intelligence activities under your purview?

If confirmed, I commit to keeping the Committee fully and currently informed of all of NSA's intelligence activities.

6. As the Deputy Commander of U.S. Cyber Command (CYBERCOM), what steps have you taken to grow the Command to be a self-sufficient organization? What more is needed to be done to have an independent organization?

   As Deputy Commander, I have worked to ensure that CYBERCOM is properly resourced and manned and enabled to operate in conjunction with others under delegations of authority, mission direction, and policy guidance necessary for effectiveness in the domain. I reinforce clear guidance in the planning process to develop options that draw first upon CYBERCOM capabilities and authorities while also working effectively in concert with NSA, the interagency and partners. I have been an advocate across the Department and with the Services to address shortfalls in readiness, manning, and training of the cyber mission forces and am also an advocate for expanded intelligence support to cyber to enhance our mission effectiveness. If confirmed, I will continue to work toward further improvements for CYBERCOM in readiness, training, and capability development, as well as seeking to apply enhanced budget control responsibilities to improve the Department's efficiency and coherence in its acquisition and cyber investments. The overlapping nature of the intelligence and cyber operating domains with the other warfighting domains is such that I believe the best outcomes for the Nation cannot be achieved separately and independently by any one organization. CYBERCOM can bring the best results for the Nation in close operating relationship with NSA, other mission organizations within the Department, the IC, the interagency, the private sector, and foreign partners.

7. Given the multiple organizations you will be leading, if confirmed, how can you assure us that NSA will receive focused leadership and attention, particularly given your legacy leadership role with CYBERCOM?

   If confirmed, I will be responsible and accountable for the mission effectiveness of both organizations. Such responsibility and accountability will naturally drive me to

give full and proper attention to NSA. My current leadership role with CYBERCOM and my familiarity and knowledge of its leadership, its mission, strengths and weaknesses means that I will be well positioned to comfortably delegate and direct its activities efficiently; enabling time management and focus necessary to NSA's global enterprise.

8. How do you intend to advance NSA's relationship with other large Intelligence Community agencies, notably the Central Intelligence Agency (CIA), Defense Intelligence Agency (DIA), National Geospatial-Intelligence Agency (NGA), National Reconnaissance Office (NRO), and Federal Bureau of Investigation (FBI)?

   Interagency collaboration is paramount for NSA's mission success. If confirmed, I will further assess the current status of NSA's relationships with each of the noted agencies, and partner with other agency heads to identify further opportunities to improve integration and collaboration across the IC.

9. Do you believe NSA's defensive cybersecurity mission is appropriately resourced? What changes do you intend to make as to how that mission is executed?

   NSA devotes an entire directorate to the Agency's cybersecurity mission to ensure NSA is postured to contribute to the protection of National Security Systems (NSS), the DoD, the Defense Industrial Base (DIB), and other customers of the Agency's cybersecurity products and services, which includes the dissemination of cyber threat intelligence. If confirmed, I will assess the resource posture and mission execution of NSA's defensive cybersecurity mission.

From Senator Wyden

Definition of Signals Intelligence

1. During your hearing, you testified that:

   "In terms of where the definition of signals intelligence [is] defined, it's defined in National Security Council Intelligence Directives, in E.O. 12333 and in the United States SIGINT systems intelligence directives. They are all very consistent in terms

of what comprises SIGINT in terms of communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence. So, I think there is a common definition that is aligned across the executive branch."

Please identify precisely the definition of signals intelligence that you believe applies across the executive branch.

The definition of signals intelligence applicable to NSA is found in DoDM S-5240.01-A (the SIGINT Annex) that, at Section 1.2, defines SIGINT to include, individually or in combination, communications intelligence (COMINT), electronic intelligence (ELINT), and foreign instrumentation signals intelligence (FISINT).

Reverse Targeting

1. During his confirmation process, now former Assistant Attorney General for National Security John Demers was asked about the prohibition on reverse targeting in Section 702 of the Foreign Intelligence Surveillance Act (FISA). He responded:

"As I understand it, determining whether a particular known U.S. person has been reverse targeted through the targeting of a Section 702 target necessitates a fact specific inquiry that would involve consideration of a variety of factors. For example, as the Privacy and Civil Liberties Oversight Board noted in its 2014 report, if a Section 702 tasking resulted in substantial reporting by the Intelligence Community regarding a U.S. person, but little reporting about the Section 702 target, that might be an indication that reverse targeting may have occurred."

During his confirmation process, current General Counsel for the Office of the Director of National Intelligence Christopher Fonzone was asked about this formulation. He responded: "My understanding of how IC entities make reverse-targeting determinations aligns with the view that Assistant Attorney General Demers expressed during his confirmation process – i.e., that such determinations are fact-specific and necessitate the evaluation of a variety of factors."

Does your understanding of the framework for determining whether reverse targeting has occurred comport with that of Mr. Demers and Mr. Fonzone?

If yes, how should NSA implement this process, with regard to targeting under both Section 702 of FISA and E.O. 12333?

My understanding of whether reverse targeting has occurred comports with that of Mr. Demers and Mr. Fonzone. Reverse targeting is strictly prohibited at NSA under both Section 702 of FISA and E.O. 12333. NSA reinforces this prohibition on reverse targeting through training, which is mandatory for all analysts with access to SIGINT data. Additionally, my understanding is that the Department of Justice reviews 100% of NSA's Section 702 targeting requests and reviews Section 702-derived serialized reporting containing U.S. person identities.

From Senator Lankford

Iran's Capabilities

The Iranian regime, the world's leading state sponsor of terror, continues to pose grave threats to U.S. interests and persons globally.

1. If confirmed, how do you plan to prioritize and tackle Iranian regime threats against the U.S., our interests, and our allies?

   Threats to our Nation's security are numerous – Iran continues to attempt to coerce the region with both conventional and cyber weapons. I have seen firsthand that NSA effectively aligns its collection activities with the National Intelligence Priorities Framework, while maintaining agility to respond to changes in priorities, mission requirements, shifts in target technology and crises. I would continue this method of prioritization if confirmed.

2. To fully address these Iranian regime threats, especially those in the cyber realm, do you believe that NSA requires new authorities?

If confirmed, I will assess two factors – the first, the full spectrum of Iranian threats and related challenges faced by the IC; the second, how NSA makes use of its current authorities. This will allow for a more comprehensive evaluation on whether additional authorities would be beneficial.

Response to Hearing Question Posed by Senator Ron Wyden (D-OR)
SSCI Nomination Hearing – Lieutenant General Timothy D. Haugh
12 July 2023

QUESTION: With a few exceptions, the National Security Agency (NSA) currently requires a probable cause determination for U.S. person queries of communications collected pursuant to E.O. 12333. Is there any reason that standard could not be applied to U.S. person queries of communications collected under Section 702 of FISA?

RESPONSE:

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.

E.O. 12333 and FISA Section 702 are distinct collection authorities with different governing procedures to address differences in the privacy and civil liberties concerns unique to each authority. The procedures governing these authorities have been carefully crafted through a thoughtful, deliberative process that resulted in approval by the Attorney General after consultation with the Director of National Intelligence for E.O. 12333 and by multiple judges on the Foreign Intelligence Surveillance Court (FISC) over the course of many years for 702. I understand that under the Attorney General-approved guidelines for E.O. 12333, a probable cause standard applies to a prescribed subset of U.S. person queries into E.O. 12333 data. I also understand that the FISC-approved standard for queries into FISA Section 702 data (including U.S. person queries) is that they must be reasonably likely to retrieve foreign intelligence information. I understand that there are technical, operational, and legal reasons for the differences and that each of these standards has been carefully considered at the time of adoption, and, with regards to the FISC-approved standard for queries into FISA Section 702 data, that standard is carefully considered by the FISC at every 702 renewal. In my opinion, the Attorney General and FISC have approved appropriate procedures for each of these authorities. Further, each set of procedures is well tailored to protect privacy and civil liberties in the distinct contexts presented by the unique characteristics and limitations of the data acquired pursuant to each authority. I do not believe that the E.O. 12333 U.S. person query standards could be applied effectively to data collected under FISA Section 702 authority without impairing NSA's ability to identify timely and actionable foreign intelligence.

Further, it is my understanding that E.O. 12333 activities are governed by the SIGINT Annex, which permits U.S. person queries in a range of circumstances. Certain, but not all, U.S. person queries in 12333 data require a finding by the Attorney General that there is probable cause to believe that the U.S. individual is an agent of a foreign power. Other types of U.S. person queries in 12333 can be approved internally by NSA personnel, with varying requirements and limitations. The applicable standard depends on the circumstances of the query, and the type of 12333 data being queried. For example, no probable cause determination is required if the pool of data to be queried is limited to the communications of certain foreign intelligence targets, or when the subject of the query is the victim of a foreign cyber attack, a hostage, or has given consent. Importantly, no U.S. person queries into 12333 data require a

separate finding of probable cause from the FISC; all such determinations are conducted within the Executive Branch, or may be based on existing FISC decisions on FISA applications

With respect to FISA Section 702, information acquired through the compelled assistance of U.S.-based electronic communications service providers is tailored and precise—specific to the communications of non-U.S. persons located outside of the United States who are expected to communicate foreign intelligence as defined by the specific intelligence topics that are authorized in certifications approved by the FISC. NSA's Section 702 Querying Procedures account for this precision and permit the use of U.S. person queries that are reasonably likely to retrieve foreign intelligence information. NSA recognizes the sensitivity associated with the use of U.S. person query terms to review Section 702-acquired information and has deployed specialized training, technology, and policy protections to ensure that it uses U.S. person query terms compliantly. All such queries are subject to review by the Department of Justice, and any errors in the use of U.S. person query terms must be reported to the FISC.

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 in several ways. First, 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. Second, it is unclear what would be the required showing under a blanket requirement for probable cause. For the limited examples of U.S. person queries into E.O. 12333 data that require a probable cause determination by the Attorney General, the standard is probable cause to believe that the U.S. person is an agent of a foreign power. However, for many of the permissible query purposes under 702 - like many of the permissible query purposes under E.O. 12333 - that standard could not be met. For example, U.S. persons who have been taken hostage, who are the victims of malicious cyber activity, or who are being targeted by a hostile foreign intelligence service are not agents of a foreign power. If NSA were required to demonstrate probable cause to believe they are, then NSA would lose the ability to run the very queries that are most essential to protecting victims of foreign intelligence threats. For all of these reasons, it is my view that the carefully crafted procedures that have been approved by the Attorney General for E.O. 12333 and by the FISC for Section 702 strike the right balance in supporting the government's ability to detect and counter vital national security threats while protecting the privacy and civil liberties of Americans.

As noted at the outset, this position is based on my current understanding. I also understand that the Administration and the 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. I commit to further engagement with the Senator on this and other important matters.

SELECT COMMITTEE ON INTELLIGENCE

UNITED STATES SENATE

QUESTIONNAIRE FOR COMPLETION BY PRESIDENTIAL NOMINEES

SELECT COMMITTEE ON INTELLIGENCE
UNITED STATES SENATE

QUESTIONNAIRE FOR COMPLETION BY PRESIDENTIAL NOMINEES

PART A - BIOGRAPHICAL INFORMATION

1. FULL NAME: Michael Colin Casey
   OTHER NAMES USED: N/A

2. DATE AND PLACE OF BIRTH: Poughkeepsie. NY
   CITIZENSHIP: US

3. MARITAL STATUS: Married

4. SPOUSE'S NAME: Sara McLean

5. SPOUSE'S MAIDEN NAME IF APPLICABLE: N/A

6. NAMES AND AGES OF CHILDREN:

NAME	AGE
Redacted	

7. EDUCATION SINCE HIGH SCHOOL:

INSTITUTION	DATES ATTENDED	DEGREE RECEIVED	DATE OF DEGREE
Miami University, Oxford OH	Aug 1987-Dec 1988	None	
University of Kentucky	Jan 1989-May 1992	BA	May 1992
Georgetown University	Aug 1993-Dec 1994	MA	31 July 1995

8. EMPLOYMENT RECORD (LIST ALL POSITIONS HELD SINCE COLLEGE, INCLUDING MILITARY SERVICE. INDICATE NAME OF EMPLOYER, POSITION, TITLE OR DESCRIPTION, LOCATION, AND DATES OF EMPLOYMENT).

EMPLOYER	POSITION/TITLE	LOCATION	DATES
Loews Theaters	Head Projectionist	Lexington, KY	1990-1993
Georgetown University	Student Security	Washington DC	1993-1994

Rep. Ben Casein	Intern		Washington DC	1995
Rep. Carrie Meek	LC		Washington DC	1995-1997
Rep. Vic Snyder	LA/LD		Washington DC	1997-2007
House Armed Services Committee	PSM		Washington DC	2007-2016
Senate Select Committee on Intelligence		Staff Director	Washington DC	2016 to present

9. GOVERNMENT EXPERIENCE (INDICATE EXPERIENCE IN OR ASSOCIATION WITH FEDERAL, STATE, OR LOCAL GOVERNMENTS, INCLUDING ADVISORY, CONSULTATIVE, HONORARY, OR OTHER PART-TIME SERVICE OR POSITION. DO NOT REPEAT INFORMATION ALREADY PROVIDED IN QUESTION 8).

Please see question 8

10. INDICATE ANY SPECIALIZED INTELLIGENCE OR NATIONAL SECURITY EXPERTISE YOU HAVE ACQUIRED HAVING SERVED IN THE POSITIONS DESCRIBED IN QUESTIONS 8 AND/OR 9.

I have broad and deep knowledge of both intelligence matters and the activities of the Department of Defense from my 7+ years as staff director of SSCI as well as my 9+ years with HASC. As SSCI Staff Director, I am afforded deep knowledge of extremely sensitive IC operations and investigations. My time at HASC provided a similar vantage point to observe Department of Defense operations.

11. HONORS AND AWARDS (PROVIDE INFORMATION ON SCHOLARSHIPS, FELLOWSHIPS, HONORARY DEGREES, MILITARY DECORATIONS, CIVILIAN SERVICE CITATIONS, OR ANY OTHER SPECIAL RECOGNITION FOR OUTSTANDING PERFORMANCE OR ACHIEVEMENT).

N/A

12. ORGANIZATIONAL AFFILIATIONS (LIST MEMBERSHIPS IN AND OFFICES HELD WITHIN THE LAST TEN YEARS IN ANY PROFESSIONAL, CIVIC, FRATERNAL, BUSINESS, SCHOLARLY, CULTURAL, CHARITABLE, OR OTHER SIMILAR ORGANIZATIONS).

ORGANIZATION	OFFICE HELD	DATES
School Without Walls PTA	None	2021-Present

13. PUBLISHED WRITINGS AND SPEECHES (LIST THE TITLES, PUBLISHERS, BLOGS AND PUBLICATION DATES OF ANY BOOKS, ARTICLES, REPORTS, OR OTHER PUBLISHED MATERIALS YOU HAVE AUTHORED. ALSO LIST ANY PUBLIC SPEECHES OR REMARKS YOU HAVE MADE WITHIN THE LAST TEN YEARS FOR WHICH THERE IS A TEXT, TRANSCRIPT, OR VIDEO). IF ASKED, WILL YOU PROVIDE A COPY OF EACH REQUESTED PUBLICATION, TEXT, TRANSCRIPT, OR VIDEO?

Published Material

"Why the 2 MTW Must Go." Published in Revising the Two MTW Force Shaping Paradigm. Edited by Steven Metz. Published by the Strategic Studies Institute, US Army War College. April 2001. Accessed on 1 April 2023 at: https://publications.armywarcollege.edu/wp-content/uploads/2022/11/1598.pdf

Speeches

While I have spoken in front of a number of audiences, mostly about how the SSCI or HASC functions or similar matters, I am unaware of any transcripts or recordings of such talks.

PART B - QUALIFICATIONS

14. QUALIFICATIONS (DESCRIBE WHY YOU BELIEVE YOU ARE QUALIFIED TO SERVE AS THE DIRECTOR OF THE NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER).

I currently serve as the Staff Director for the Senate Select Committee on Intelligence. I have been in this position, or its equivalent of Minority Staff Director. for over seven years. In this position, I coordinate the committee's staff as we assist the Committee Members in their oversight functions. Because of this unique position, I am afforded exceptional access to IC operations, collection, and investigations. During this period, I co-led a three and a half year investigation into how the Russian government and affiliated entities attempted to interfere with the 2016 Presidential election, an investigation that provided deep insight into the nation's counterintelligence enterprise.

Prior to my time at SSCI, I spent over 9 years as a professional staff member, including serving as the Policy Lead for the Minority for several of those years. In that capacity I oversaw a great deal of the Department of Defense's operations in the Middle East, Europe, Africa and other locations. This afforded me deep insight into how the national security apparatus of the United States functions, including interagency relations and relations with foreign governments.

My time in these positions has afforded me the opportunity develop solid relationships with many leaders across the IC and large parts of the government.

PART C - POLITICAL AND FOREIGN AFFILIATIONS

15. POLITICAL ACTIVITIES (LIST ANY MEMBERSHIPS OR OFFICES HELD IN OR FINANCIAL CONTRIBUTIONS OR SERVICES RENDERED TO, ANY POLITICAL PARTY, ELECTION COMMITTEE, POLITICAL ACTION COMMITTEE, OR INDIVIDUAL CANDIDATE DURING THE LAST TEN YEARS).

Contributions

- John Kerry for President, 07/29/2004, $250
- Obama for America, 06/25/2008, $250
- Obama Victory Fund, 09/25/2012, $250
- Obama for America, 09/25/2012, $250
- Hillary for America, 03/09/2016, $250
- ActBlue, 10/30/2018, $100
- ActBlue, 10/30/2018, $10
- Richard Bew for Congress, 03/27/2019, $250
- Biden Victory Fund, 08/16/2020, $250
- Biden for President, 08/16/2020, $250

16. CANDIDACY FOR PUBLIC OFFICE (FURNISH DETAILS OF ANY CANDIDACY FOR ELECTIVE PUBLIC OFFICE).

None

17. FOREIGN AFFILIATIONS

(NOTE: QUESTIONS 17A AND B ARE NOT LIMITED TO RELATIONSHIPS REQUIRING REGISTRATION UNDER THE FOREIGN AGENTS REGISTRATION ACT. QUESTIONS 17A, B, AND C DO NOT CALL FOR A POSITIVE RESPONSE IF THE REPRESENTATION OR TRANSACTION WAS AUTHORIZED BY THE UNITED STATES GOVERNMENT IN CONNECTION WITH YOUR OR YOUR SPOUSE'S EMPLOYMENT IN GOVERNMENT SERVICE.)

A. HAVE YOU OR YOUR SPOUSE EVER REPRESENTED IN ANY CAPACITY (E.G. EMPLOYEE, ATTORNEY, OR POLITICAL/BUSINESS CONSULTANT), WITH OR WITHOUT COMPENSATION, A FOREIGN GOVERNMENT OR AN ENTITY CONTROLLED BY A FOREIGN GOVERNMENT? IF SO, PLEASE FULLY DESCRIBE SUCH RELATIONSHIP.

No

B. HAVE ANY OF YOUR OR YOUR SPOUSE'S ASSOCIATES REPRESENTED, IN ANY CAPACITY, WITH OR WITHOUT COMPENSATION, A FOREIGN GOVERNMENT OR AN ENTITY CONTROLLED BY A FOREIGN GOVERNMENT? IF SO, PLEASE FULLY DESCRIBE SUCH RELATIONSHIP.

No

C. DURING THE PAST TEN YEARS, HAVE YOU OR YOUR SPOUSE RECEIVED ANY COMPENSATION FROM, OR BEEN INVOLVED IN ANY FINANCIAL OR BUSINESS TRANSACTIONS WITH, A FOREIGN GOVERNMENT OR ANY ENTITY CONTROLLED BY A FOREIGN GOVERNMENT? IF SO, PLEASE PROVIDE DETAILS.

No

D. HAVE YOU OR YOUR SPOUSE EVER REGISTERED UNDER THE FOREIGN AGENTS REGISTRATION ACT? IF SO, PLEASE PROVIDE DETAILS.

No

18. DESCRIBE ANY LOBBYING ACTIVITY DURING THE PAST TEN YEARS, OTHER THAN IN AN OFFICIAL U.S. GOVERNMENT CAPACITY, IN WHICH YOU OR YOUR SPOUSE HAVE ENGAGED FOR THE PURPOSE OF DIRECTLY OR INDIRECTLY INFLUENCING THE PASSAGE, DEFEAT, OR MODIFICATION OF FEDERAL LEGISLATION, OR FOR THE PURPOSE OF AFFECTING THE ADMINISTRATION AND EXECUTION OF FEDERAL LAW OR PUBLIC POLICY.

None

PART D - FINANCIAL DISCLOSURE AND CONFLICT OF INTEREST

19. DESCRIBE ANY EMPLOYMENT, BUSINESS RELATIONSHIP, FINANCIAL TRANSACTION, INVESTMENT, ASSOCIATION, OR ACTIVITY (INCLUDING, BUT NOT LIMITED TO, DEALINGS WITH THE FEDERAL GOVERNMENT ON YOUR OWN BEHALF OR ON BEHALF OF A CLIENT), WHICH COULD CREATE, OR APPEAR TO CREATE, A CONFLICT OF INTEREST IN THE POSITION TO WHICH YOU HAVE BEEN NOMINATED.

None

20. DO YOU INTEND TO SEVER ALL BUSINESS CONNECTIONS WITH YOUR PRESENT EMPLOYERS, FIRMS, BUSINESS ASSOCIATES AND/OR PARTNERSHIPS, OR OTHER ORGANIZATIONS IN THE EVENT THAT YOU ARE CONFIRMED BY THE SENATE? IF NOT, PLEASE EXPLAIN.

I have no such business connections to sever

21. DESCRIBE THE FINANCIAL ARRANGEMENTS YOU HAVE MADE OR PLAN TO MAKE, IF YOU ARE CONFIRMED, IN CONNECTION WITH SEVERANCE FROM YOUR CURRENT POSITION. PLEASE INCLUDE SEVERANCE PAY, PENSION RIGHTS, STOCK OPTIONS, DEFERRED INCOME ARRANGEMENTS, AND ANY AND ALL COMPENSATION THAT WILL OR MIGHT BE RECEIVED IN THE FUTURE AS A RESULT OF YOUR CURRENT BUSINESS OR PROFESSIONAL RELATIONSHIPS.

None

22. DO YOU HAVE ANY PLANS, COMMITMENTS, OR AGREEMENTS TO PURSUE OUTSIDE EMPLOYMENT, WITH OR WITHOUT COMPENSATION, DURING YOUR SERVICE WITH THE GOVERNMENT? IF SO, PLEASE PROVIDE DETAILS.

No

23. AS FAR AS CAN BE FORESEEN, STATE YOUR PLANS AFTER COMPLETING GOVERNMENT SERVICE. PLEASE SPECIFICALLY DESCRIBE ANY AGREEMENTS OR UNDERSTANDINGS, WRITTEN OR UNWRITTEN, CONCERNING EMPLOYMENT AFTER LEAVING GOVERNMENT SERVICE. IN PARTICULAR, DESCRIBE ANY AGREEMENTS, UNDERSTANDINGS, OR OPTIONS TO RETURN TO YOUR CURRENT POSITION.

I have no plans at this time.

24. IF YOU ARE PRESENTLY IN GOVERNMENT SERVICE, DURING THE PAST FIVE YEARS OF SUCH SERVICE, HAVE YOU RECEIVED FROM A PERSON OUTSIDE OF GOVERNMENT AN OFFER OR EXPRESSION OF INTEREST TO EMPLOY YOUR SERVICES AFTER YOU LEAVE GOVERNMENT SERVICE? IF YES, PLEASE PROVIDE DETAILS.

At various times in the past, corporations, lobbying firms, or advisory firms have expressed an interest in hiring me at some point. None of these have resulted in any agreement or offer of employment or future plans of the same.

25. IS YOUR SPOUSE EMPLOYED? IF YES AND THE NATURE OF THIS EMPLOYMENT IS RELATED IN ANY WAY TO THE POSITION FOR WHICH YOU ARE SEEKING CONFIRMATION, PLEASE INDICATE YOUR SPOUSE'S EMPLOYER, THE POSITION, AND THE LENGTH OF TIME THE POSITION HAS BEEN HELD. IF YOUR SPOUSE'S EMPLOYMENT IS NOT RELATED TO THE POSITION TO WHICH YOU HAVE BEEN NOMINATED, PLEASE SO STATE.

Sara is employed as an attorney with the US Department of Justice. Her duties there have nothing to do with the position of Director of the National Counterintelligence and Security Center

26. LIST BELOW ALL CORPORATIONS, PARTNERSHIPS, FOUNDATIONS, TRUSTS, OR OTHER ENTITIES TOWARD WHICH YOU OR YOUR SPOUSE HAVE FIDUCIARY OBLIGATIONS OR IN WHICH YOU OR YOUR SPOUSE HAVE HELD DIRECTORSHIPS OR OTHER POSITIONS OF TRUST DURING THE PAST FIVE YEARS.

NAME OF ENTITY	POSITION	DATES HELD	SELF OR SPOUSE

27. LIST ALL GIFTS EXCEEDING $100 IN VALUE RECEIVED DURING THE PAST FIVE YEARS BY YOU, YOUR SPOUSE, OR YOUR DEPENDENTS. (NOTE: GIFTS RECEIVED FROM RELATIVES AND GIFTS GIVEN TO YOUR SPOUSE OR DEPENDENT NEED NOT BE INCLUDED UNLESS THE GIFT WAS GIVEN WITH YOUR KNOWLEDGE AND ACQUIESCENCE AND YOU HAD REASON TO BELIEVE THE GIFT WAS GIVEN BECAUSE OF YOUR OFFICIAL POSITION.)

None

28. LIST ALL SECURITIES, REAL PROPERTY, PARTNERSHIP INTERESTS, OR OTHER INVESTMENTS OR RECEIVABLES WITH A CURRENT MARKET VALUE (OR, IF MARKET VALUE IS NOT ASCERTAINABLE, ESTIMATED CURRENT FAIR VALUE) IN EXCESS OF $1,000. (NOTE: THE INFORMATION PROVIDED IN RESPONSE TO SCHEDULE A OF THE DISCLOSURE FORMS OF THE OFFICE OF GOVERNMENT ETHICS MAY BE INCORPORATED BY REFERENCE, PROVIDED THAT CURRENT VALUATIONS ARE USED.)

DESCRIPTION OF PROPERTY	VALUE	METHOD OF VALUATION

See OGE 278e

29. LIST ALL LOANS OR OTHER INDEBTEDNESS (INCLUDING ANY CONTINGENT LIABILITIES) IN EXCESS OF $10,000. EXCLUDE A MORTGAGE ON YOUR PERSONAL RESIDENCE UNLESS IT IS RENTED OUT, AND LOANS SECURED BY AUTOMOBILES, HOUSEHOLD FURNITURE, OR APPLIANCES. (NOTE: THE INFORMATION PROVIDED IN RESPONSE TO SCHEDULE C OF THE DISCLOSURE FORM OF THE OFFICE OF GOVERNMENT ETHICS MAY BE INCORPORATED BY REFERENCE, PROVIDED THAT CONTINGENT LIABILITIES ARE ALSO INCLUDED.)

NATURE OF OBLIGATION	NAME OF OBLIGEE	AMOUNT

None

30. ARE YOU OR YOUR SPOUSE NOW IN DEFAULT ON ANY LOAN, DEBT, OR OTHER FINANCIAL OBLIGATION? HAVE YOU OR YOUR SPOUSE BEEN IN DEFAULT ON ANY LOAN, DEBT, OR OTHER FINANCIAL OBLIGATION IN THE PAST TEN YEARS? HAVE YOU OR YOUR SPOUSE EVER BEEN REFUSED CREDIT OR HAD A LOAN APPLICATION DENIED? IF THE ANSWER TO ANY OF THESE QUESTIONS IS YES, PLEASE PROVIDE DETAILS.

No

31. LIST THE SPECIFIC SOURCES AND AMOUNTS OF ALL INCOME RECEIVED DURING THE LAST FIVE YEARS, INCLUDING ALL SALARIES, FEES, DIVIDENDS, INTEREST, GIFTS, RENTS, ROYALTIES, PATENTS, HONORARIA, AND OTHER ITEMS EXCEEDING $200. (COPIES OF U.S. INCOME TAX RETURNS FOR THESE YEARS MAY BE SUBSTITUTED HERE, BUT THEIR SUBMISSION IS NOT REQUIRED.)

	2018	2019	2020	2021	2022
SALARIES					
FEES					
ROYALTIES					
DIVIDENDS					
INTEREST					
GIFTS					
RENTS					
OTHER					
TOTAL					

Please see tax returns submitted to the committee

32. IF ASKED, WILL YOU PROVIDE THE COMMITTEE WITH COPIES OF YOUR AND YOUR SPOUSE'S FEDERAL INCOME TAX RETURNS FOR THE PAST THREE YEARS?

I have submitted copies of our returns

33. LIST ALL JURISDICTIONS IN WHICH YOU AND YOUR SPOUSE FILE ANNUAL INCOME TAX RETURNS.

Washington DC

34. HAVE YOUR FEDERAL OR STATE TAX RETURNS BEEN THE SUBJECT OF AN AUDIT, INVESTIGATION, OR INQUIRY AT ANY TIME? IF SO, PLEASE PROVIDE DETAILS, INCLUDING THE RESULT OF ANY SUCH PROCEEDING.

No

35. IF YOU ARE AN ATTORNEY, ACCOUNTANT, OR OTHER PROFESSIONAL, PLEASE LIST ALL CLIENTS AND CUSTOMERS WHOM YOU BILLED MORE THAN $200 WORTH OF SERVICES DURING THE PAST FIVE YEARS. ALSO, LIST ALL JURISDICTIONS IN WHICH YOU ARE LICENSED TO PRACTICE.

N/A

36. DO YOU INTEND TO PLACE YOUR FINANCIAL HOLDINGS AND THOSE OF YOUR SPOUSE AND DEPENDENT MEMBERS OF YOUR IMMEDIATE HOUSEHOLD IN A BLIND TRUST? IF YES, PLEASE FURNISH DETAILS. IF NO, DESCRIBE OTHER ARRANGEMENTS FOR AVOIDING ANY POTENTIAL CONFLICTS OF INTEREST.

No. All of our financial holdings, other than checking and savings accounts and the like, are in mutual funds or similar funds managed by Vanguard.

37. IF APPLICABLE, LIST THE LAST THREE YEARS OF ANNUAL FINANCIAL DISCLOSURE REPORTS YOU HAVE BEEN REQUIRED TO FILE WITH YOUR AGENCY, DEPARTMENT, OR BRANCH OF GOVERNMENT. IF ASKED, WILL YOU PROVIDE A COPY OF THESE REPORTS?

I have filed annual disclosures with the US Senate since 2017. Yes

PART E - ETHICAL MATTERS

38. HAVE YOU EVER BEEN THE SUBJECT OF A DISCIPLINARY PROCEEDING OR CITED FOR A BREACH OF ETHICS OR UNPROFESSIONAL CONDUCT BY, OR BEEN THE SUBJECT OF A COMPLAINT TO, ANY COURT, ADMINISTRATIVE AGENCY, PROFESSIONAL ASSOCIATION, DISCIPLINARY COMMITTEE, OR OTHER PROFESSIONAL GROUP? IF SO, PLEASE PROVIDE DETAILS.

No

39. HAVE YOU EVER BEEN INVESTIGATED, HELD, ARRESTED, OR CHARGED BY ANY FEDERAL, STATE, OR OTHER LAW ENFORCEMENT AUTHORITY FOR VIOLATION OF ANY FEDERAL STATE, COUNTY, OR MUNICIPAL LAW, REGULATION, OR ORDINANCE, OTHER THAN A MINOR TRAFFIC OFFENSE, OR NAMED AS A DEFENDANT OR OTHERWISE IN ANY INDICTMENT OR INFORMATION RELATING TO SUCH VIOLATION? IF SO, PLEASE PROVIDE DETAILS.

No

40. HAVE YOU EVER BEEN CONVICTED OF OR ENTERED A PLEA OF GUILTY OR NOLO CONTENDERE TO ANY CRIMINAL VIOLATION OTHER THAN A MINOR TRAFFIC OFFENSE? IF SO, PLEASE PROVIDE DETAILS.

When I was 17, I was convicted of trespassing. I believe the record was sealed and/or expunged when I turned 18

41. ARE YOU PRESENTLY OR HAVE YOU EVER BEEN A PARTY IN INTEREST IN ANY ADMINISTRATIVE AGENCY PROCEEDING OR CIVIL LITIGATION? IF SO, PLEASE PROVIDE DETAILS.

No

42. HAVE YOU BEEN INTERVIEWED OR ASKED TO SUPPLY ANY INFORMATION AS A WITNESS OR OTHERWISE IN CONNECTION WITH ANY CONGRESSIONAL INVESTIGATION, FEDERAL, OR STATE AGENCY PROCEEDING, GRAND JURY INVESTIGATION, OR CRIMINAL OR CIVIL LITIGATION IN THE PAST TEN YEARS? IF SO, PLEASE PROVIDE DETAILS.

I was interviewed by the Department of Justice in the investigation of Jim Wolfe a former employee of the Senate Select Committee on Intelligence. The interview consisted of questions about my duties with the committee and Mr. Wolfe's service with the committee.

43. HAS ANY BUSINESS OF WHICH YOU ARE OR WERE AN OFFICER, DIRECTOR, OR PARTNER BEEN A PARTY TO ANY ADMINISTRATIVE AGENCY PROCEEDING OR CRIMINAL OR CIVIL LITIGATION RELEVANT TO THE POSITION TO WHICH YOU HAVE BEEN NOMINATED? IF SO, PLEASE PROVIDE DETAILS. (WITH RESPECT TO A BUSINESS OF WHICH YOU ARE OR WERE AN OFFICER, YOU NEED ONLY CONSIDER PROCEEDINGS AND LITIGATION THAT OCCURRED WHILE YOU WERE AN OFFICER OF THAT BUSINESS.)

No

44. HAVE YOU EVER BEEN THE SUBJECT OF ANY INSPECTOR GENERAL INVESTIGATION? IF SO, PLEASE PROVIDE DETAILS.

No

PART F - SECURITY INFORMATION

45. HAVE YOU EVER BEEN DENIED ANY SECURITY CLEARANCE OR ACCESS TO CLASSIFIED INFORMATION FOR ANY REASON? IF YES, PLEASE EXPLAIN IN DETAIL.

No

46. HAVE YOU BEEN REQUIRED TO TAKE A POLYGRAPH EXAMINATION FOR ANY SECURITY CLEARANCE OR ACCESS TO CLASSIFIED INFORMATION? IF YES, PLEASE EXPLAIN.

No

47. HAVE YOU EVER REFUSED TO SUBMIT TO A POLYGRAPH EXAMINATION? IF YES, PLEASE EXPLAIN.

No

PART G - ADDITIONAL INFORMATION

48. DESCRIBE IN YOUR OWN WORDS THE CONCEPT OF CONGRESSIONAL OVERSIGHT OF U.S. INTELLIGENCE ACTIVITIES. IN PARTICULAR, CHARACTERIZE WHAT YOU BELIEVE TO BE THE OBLIGATIONS OF THE DIRECTOR OF NCSC AND THE INTELLIGENCE COMMITTEES OF THE CONGRESS, RESPECTIVELY, IN THE OVERSIGHT PROCESS.

The National Security Act requires that the intelligence community keep the Congress fully and currently informed. As Staff Director for SSCI, I very much value this obligation, a position I will maintain if confirmed as Director of the NCSC. The Director of the NCSC should strive to provide Congress complete, accurate, and timely information about the successes and the failures of the mission center so that Congress can undertake it's important job of oversight. If confirmed, I would seek to engage often with members of Congress and the staff of SSCI, HPSCI, and the appropriations committees so that they would be fully informed as they consider legislation and the annual budget submission.

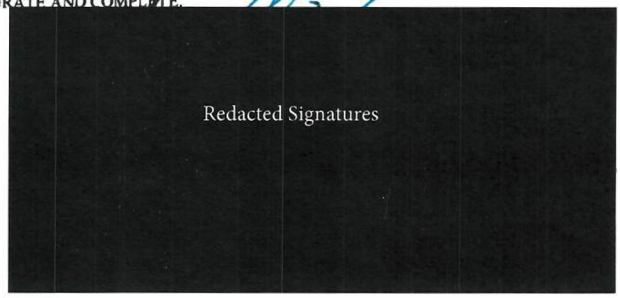
49. EXPLAIN YOUR UNDERSTANDING OF THE RESPONSIBILITIES OF THE DIRECTOR OF NCSC.

The D/NCSC serves as the head of counterintelligence for the United States government, including helping to set priorities and develop resource plans and strategies, such as the National Counterintelligence Strategy. The D/NCSC also serves as the principal advisor to the DNI for counterintelligence and personnel security policy across the US Government. The D/NCSC also leads outreach to the private sector about foreign risks.

AFFIRMATION

I, **Michael Colin Casey**, DO SWEAR THAT THE ANSWERS I HAVE PROVIDED TO THIS QUESTIONNAIRE ARE ACCURATE AND COMPLETE.

20 JUNE 2023
(Date)



TO THE CHAIRMAN, SELECT COMMITTEE ON INTELLIGENCE:

In connection with my nomination to be the Director of the National Counterintelligence and Security Center, I hereby express my willingness to respond to requests to appear and testify before any duly constituted committee of the Senate.

Redacted Signature

Date: 22 June 2023

**SELECT COMMITTEE
ON INTELLIGENCE**

UNITED STATES SENATE

**Additional Questions for
Mr. Michael C. Casey upon His Nomination to be
Director of the National Counterintelligence and Security
Center**

Responsibilities of the Director of the National Counterintelligence and Security Center

QUESTION 1: What is your understanding of the unique role of the National Counterintelligence and Security Center (NCSC) within the Intelligence Community (IC)?

NCSC leads and supports the U.S. Government's (USG) counterintelligence (CI) and security activities critical to protecting our nation. This includes providing CI outreach to U.S. private sector entities at risk of foreign intelligence penetration and issuing public warnings regarding intelligence threats to the United States. Within the IC, the Director of NCSC is the mission manager for CI, serving as the National Intelligence Manager for Counterintelligence (NIM-CI) and the principal substantive advisor to the Director of National Intelligence (DNI) on all aspects of CI.

Additionally, NCSC supports the DNI's execution of her Security Executive Agent (SecEA) authorities across the Executive Branch, including the IC, to protect our national security interests by ensuring the reliability and trustworthiness of those to whom we entrust our nation's secrets and assign to sensitive positions. Pursuant to *Executive Order (EO) 13587*, NCSC also supports the National Insider Threat Task Force, on behalf of the DNI, to strengthen insider threat programs across the USG and prevent the compromise of classified information.

QUESTION 2: What is your understanding of the specific statutory responsibilities of the Director of the NCSC?

Under the *Counterintelligence Enhancement Act of 2002*, the Director of NCSC serves as the head of national CI for the USG. In this role, the Director of NCSC is responsible for leading NCSC in:

- Producing the *National Threat Identification and Prioritization Assessment*;
- Producing and implementing the *National Counterintelligence Strategy*;
- Overseeing and coordinating the production of strategic analyses of CI matters, including the production of CI damage assessments and assessments of lessons learned from CI activities;

- Developing priorities for CI investigations, operations, and collection;

- Carrying out and coordinating surveys of the vulnerabilities of the USG and the private sector to intelligence threats to identify the areas, programs, and activities that require protection from such threats;

- Advocating for research and development programs and activities of the USG and the private sector to direct attention to the needs of the CI community;

- Developing policies and standards for training and professionalizing the workforce, and developing and managing the conduct of joint training exercises; and,

- Performing CI outreach, including consulting with the private sector to identify vulnerabilities from foreign intelligence activities.

The Director also oversees NCSC's coordination of the development of CI budgets and resource allocation plans. Furthermore, under the *CI and Security Enhancements Act of 1994*, the Director of NCSC serves as the chairperson of the National CI Policy Board.

Additionally, under *Section 103F* of the *National Security Act*, the Director of NCSC is tasked to perform not only the duties set forth under the *CI Enhancement Act of 2002*, but also such duties prescribed by the Director of National Intelligence. Under *Section 119B* of the *National Security Act*, the DNI designated NCSC as a National Intelligence Center to align CI and security functions in a single organization. In support of its role as a National Intelligence Center, NCSC is responsible for leading and supporting the integration of the USG's CI and security activities, providing outreach to federal and private sector entities, and issuing public warnings regarding intelligence threats to the United States.

There are also numerous instances where NCSC supports the DNI in her execution of her statutory responsibilities. A primary example of this is NCSC's role as the primary staff element supporting the DNI's Security Executive Agent (SecEA) functions. In this role, NCSC helps to oversee many personnel security functions related to eligibility to access classified

information and to hold a sensitive position, to include: overseeing the national security background investigation and adjudication programs; developing and issuing policies and procedures, including those that support reciprocal recognition; and arbitrating and resolving disputes among agencies.

NCSC, on behalf of the DNI, is therefore required to ensure continuous performance improvement in personnel security processes. This includes building the capacity of the background investigative workforce and implementing modernized continuous vetting techniques, as appropriate.

QUESTION 3: Have you discussed with Director Haines her specific future expectations of you, and her future expectations of the NCSC as a whole? If so, please describe these expectations.

The DNI and I have spoken multiple times about the future of the NCSC. Director Haines has expressed that her key objectives for NCSC include:

- Enhancing NSCS's work on the key fundamentals that underlie the work of the IC such as completing and improving the ongoing clearance modernization and move to Trusted Workforce 2.0;
- Building on past successes in NCSC's work on understanding and helping to mitigate the supply chain vulnerabilities for the IC and the entire United States Government;
- Ensuring that the United States Government has the right CI programs needed to protect its work, particularly in the digital space; and
- Helping to continue to convey to the private sector and academia the threats posed by foreign actors, particularly China, and helping those actors grow the programs and expertise needed to protect themselves.

NCSC Mission

QUESTION 4: What do you believe are the greatest challenges facing NCSC?

The evolving CI threat landscape and the growth of NCSC's mission requirements means that NCSC must build on a number of existing efforts in order to ensure that it is effectively postured against the adapting threat

environment will be an enduring challenge.

NCSC will need to build on prior efforts to include:

- Identifying stakeholders and outlining stakeholders' USG and security roles and responsibilities, and clarifying stakeholders' relationships with NCSC.

- Ensuring that NCSC's various roles and missions are properly prioritized and not duplicating the work of other parts of the IC or other agencies who might be better postured to carry out that work.

- Leveraging the IC in protecting non-USG entities that foreign intelligence entities target for their research, technologies, data, and intellectual property.

- Assisting NT50 agencies to establish "CI awareness" and/or security programs to ensure that USG data and sensitive information are identified and protected.

QUESTION 5: Please explain your vision for the NCSC, including your views on its current and future priorities and what the organization should look like five years from now.

My vision is for NCSC to be the nation's premier source for CI and security expertise and a trusted mission partner in protecting America against foreign and other adversarial threats. NCSC is currently updating the *National CI Strategy* that focuses on prioritizing specific goals that will make America less vulnerable to foreign intelligence threats.

To implement the vision, if confirmed, I would:

- Leverage the interagency and ensure the CI community is moving in an integrated way to accomplish goals that include:

    - Detecting, understanding, and anticipating foreign intelligence threats;

    - Deterring foreign intelligence activities and capabilities;

- Protecting U.S. interests; and,

- Building CI capabilities, partnerships, and resilience.

- Advocate for resources and budgetary authority to support requirements for the IC and NT50 agencies that align resources to priorities designed to counter risks from foreign and other adversarial intelligence threats.

- Build resilience in the private sector and academia to advance outreach, education, and awareness by making resources available that assist with the development of insider threat and mitigation programs.

- Advance security priorities and support efforts to mitigate supply chain risks, issue security standards that address evolving threats, and establish technical capabilities that complement the CI and security communities to advance their missions.

NCSC currently devotes significant time and effort to raising awareness of foreign intelligence threats. I envision that in five years NCSC will continue to provide focused, sustained leadership in key areas such as: protecting our economic security by mitigating the theft of intellectual property and critical technologies; harnessing and mitigating the promise and risks posed by cutting edge technology available to both the United States and our adversaries; and, putting personnel security and insider threat programs in place to maintain a trusted workforce.

QUESTION 6: What specific benchmarks should be used to assess the NCSC's performance?

NCSC uses many benchmarks to assess progress against the following goals outlined in its *National CI Strategy* and personnel vetting performance plans.

- NCSC gauges the effectiveness of its governance by assessing progress against strategic priorities and by taking an integrated approach to CI and security. NCSC engages across the community by chairing various boards such as the National CI Policy Board, the IC Security Directors' Board, and the CI Strategy and Resource Board.

- NCSC evaluates this in the annual production of the *State of the CI Mission* which provides an assessment of the CI community's progress against priorities, initiatives, and challenges. The *State of the CI Mission* is also used to inform the CI community's prioritization of resource needs for outyears.

- NCSC also reviews benchmarks for security programs to measure their effectiveness. NCSC issued *Performance Management Guidelines* and the *Federal Personnel Vetting Performance Management Standards* to modernize outcomes for measuring efficiency and effectiveness of vetting programs. NCSC's forthcoming issuance of the *Federal Personnel Vetting Performance Management Implementation Guidance* will establish near-term and future targets for performance measures. Collectively, these security policies will facilitate uniform measurement, assessment, and reporting of key vetting processes to ensure consistency, fairness, and the protection of civil liberties.

- NCSC evaluates the effectiveness of its outreach efforts in terms of deployed capabilities, usage, and demand for upgraded capabilities, and user testimonials. NCSC also attempts to understand the extent to which outreach has changed stakeholder behaviors, increased collaboration among stakeholders, and empowered stakeholders to enhance their own security and resilience.

- To measure the health and welfare of NCSC internally, NCSC points to the successful recruitment and retention of highly qualified CI and security officers to serve in NCSC, responsible stewardship of human and financial capital, stellar employee climate survey results, and the success of groundbreaking initiatives such as our *Cross-the-Line* program that cross-fertilizes expertise across the Center and allows for professional growth.

CI Threats

QUESTION 7: What in your view are the most critical CI threats that are currently confronting the United States?

The United States faces a growing range of intelligence threats from an expanding set of actors. Russia and China represent major traditional intelligence threats to the

United States with well-resourced, technically sophisticated intelligence services determined to gain sensitive U.S. information and thwart U.S. collection and operations. Regional actors such as Iran and North Korea, and non-state actors such as terrorist groups, transnational criminal organizations, and hackers/hacktivists are growing in intent and capability. These actors also are increasing their collaboration with one another, enhancing their skills, expanding their geographic reach, and magnifying the threat to the United States.

This expanding array of Foreign Intelligence Entities (FIE) are targeting our data, technology, and talent to erode our military and economic advantage, threatening the critical infrastructure that keeps our economy and society functioning, influencing U.S. public opinion and government policies, and undermining our democracy and societal cohesion. FIE are adopting cutting-edge technologies—from advanced cyber tools to unmanned systems to enhanced technical surveillance equipment—that improve their capabilities and challenge our defenses. Much of this technology is available commercially, providing a shortcut for previously unsophisticated foreign intelligence entities to become significant threats.

U.S. adversaries also increasingly view data as a strategic resource and a collection priority. They are focused on acquiring and analyzing data—from personally identifiable information on U.S. citizens, to commercial and government data—that can make their espionage, influence, kinetic and cyber-attack operations more effective, advance their exploitation of the U.S. economy, and give them strategic advantage over the United States.

QUESTION 8: What would be your top priorities for the NCSC, in terms of the CI threats facing the United States?

NCSC's top priorities are to mitigate and counter a range of foreign intelligence threats to U.S. interests at home and abroad. Hostile intelligence services and non-state actors are becoming more capable and have access to more tools. They seek to access government systems and infrastructure, undermine the private sector through commercial espionage, infringe on the privacy of U.S. citizens through data theft, and shape U.S. policy and public opinion through influence operations.

I anticipate these priorities will be reflected in the forthcoming *National CI Strategy* and, if confirmed, I would look forward to reviewing the strategy and ensuring the Committee is kept apprised of its development. We must better anticipate foreign

intelligence threats and work together across the IC, the broader federal government, and with our partners to counter these harmful intelligence activities and degrade FIE capabilities.

Our strength as a nation rests upon a number of strategic advantages that we must help protect and defend, including our people, our democratic institutions, our critical technology, infrastructure, and supply chains. We must invest in the future to develop the capability and capacity to meet these challenges and protect America's strategic advantage. We must reinvigorate our CI community, build and enable strong partnerships, and increase collaboration to build resilience against current and future foreign intelligence threats.

QUESTION 9: What actions would you plan to take to ensure that each of your identified priorities is satisfied?

I understand through the forthcoming *National CI Strategy*, NCSC intends to drive the direction and alignment of CI priorities and activities. NCSC will leverage the strengths of each federal department or agency within their respective missions and authorities, and in coordination with the CI community, will baseline current activities and identify shortfalls and gaps. These shortfalls and gaps will then be addressed through the strategy's implementation plan to provide future direction, investment, and resource shifts needed to ensure the successful implementation of the strategy.

QUESTION 10: In your opinion, what CI threats, if any, have been overlooked or underestimated?

The top evolving and not fully understood or fully addressed challenge involves the comprehensive national security, data security, and counterespionage laws of the People's Republic of China (PRC). These laws state that the PRC government may access private information, compel PRC citizens in China and overseas to assist PRC intelligence services, and arbitrarily detain or arrest foreigners in China for suspected espionage activities. I do not believe that the United States has fully grappled with the implications of this comprehensive system.

We also cannot underestimate the threat posed by FIEs, especially China and Russia and those groups who assist them, to our critical infrastructure, particularly the financial, power, water, communications, and transportation sectors. Each of these

sectors has a large, relatively vulnerable footprint. Their supporting personnel, networks, and other infrastructure are here in the United States, posing additional legal, coordination, collection, and other challenges for the IC. Any disruption in these sectors could impact our economy, military readiness, and the U.S. population overall. FIEs will look to exploit these nodes during a time of conflict or crisis.

The convergence and disruptive potential of several advanced technologies—including AI, quantum computing, biotechnology, autonomous systems, semiconductors and telecommunications—may have unanticipated impacts across multiple critical sectors such as healthcare, energy, agriculture, and advanced manufacturing. The CI community will face numerous challenges as these technologies develop, ranging from the collection and exploitation of sensitive personal and other data to the disruption of key technical and lifeline sector supply chains to increased adversary capabilities to influence U.S. and global financial markets.

QUESTION 11: What in your view is the appropriate role of NCSC in conducting direct informational outreach to U.S. National Labs, universities, and private sector start-ups and other entities vis-à-vis their appeal as high-value targets for economic espionage?

NCSC has a critical role to play in conducting outreach to private sector, academic, and research entities. The purpose of NCSC's outreach is to educate these entities on foreign intelligence threats to their organizations, provide them with best practices for mitigation, and help them build resilience to protect their critical assets.

Working with other federal partners, NCSC has been conducting extensive outreach for years to entities in U.S. emerging technology sectors, as well as U.S. National Labs, universities, and other research institutions. NCSC conducts its outreach through both classified and unclassified threat briefings, dissemination of written products and videos, national communications campaigns, and through enduring partnerships with industry, academia, state and local entities, foreign allies, and other stakeholders.

Given its limited staff and resources, it is critical for NCSC to continue to partner

with USG agencies in its outreach efforts. I would also highlight the opportunities provided by the "China Roadshows" hosted by the Chairman and Vice Chairman of SSCI, which have allowed NCSC, with other partners, to engage with the private sector at the C-Suite level. By working together, NCSC and its partners unify messaging, deconflict engagement efforts, and broaden the scope of their outreach efforts. NCSC will continue to align its outreach activities with the goals and objectives of the *National CI Strategy of the United States* and will capture metrics on its outreach activities to measure effectiveness and achieve optimal impact for resources spent.

I would also note that over time, I expect NCSC's, and other federal entities', engagement with the private sector to evolve. As more private sector entities are aware of the threat posed by China and other actors, their questions will naturally become more focused on "what can we do" and less about the nature of the threat. NCSC is, I believe, well positioned to continue to highlight best practices to bring together government and private sector partners to combat the evolving threat.

QUESTION 12: Please describe the CI threat resulting from the presence of thousands of foreign nationals from adversary countries at our National Labs and the risks this threat poses to U.S. national security.

The nature of the foreign intelligence threat to our National Labs has changed over the past decades. State actors increasingly are exploiting our culture of openness and collaboration to acquire information on United States research and development, new technologies, and to advance their military capabilities, modernize their economies, and weaken U.S. global influence. While we gain expertise, insight, and valuable skills by maintaining our commitment to a transparent and open innovation ecosystem, we learned that foreign adversaries are taking advantage of the access we have provided to legitimate, talented foreign scientists and academics.

Congressional Oversight

QUESTION 13: *The National Security Act of 1947, Section 102A (50 U.S.C. § 3024)* provides that the DNI "…shall be responsible for ensuring that national intelligence is provided… to the Senate and House of Representatives and the committees thereof," and will "…develop and determine an annual consolidated National Intelligence Program [(NIP)] budget."

a. What do you understand to be the obligation of the DNI and the Director of the NCSC in support of the DNI to keep the congressional intelligence committees fully and currently informed about matters relating to compliance with the Constitution and laws?

As Director Haines has stated, the DNI, per Section 502 of the *National Security Act*, has a clear legal responsibility to inform the Congressional Intelligence Committees of issues of compliance with the Constitution and laws, and to report any illegal intelligence activities. As a long-time and current congressional staffer, I have a tremendous appreciation for the value and necessity of the committee's oversight responsibilities, and fully agree with Director Haines' statement. Should I be confirmed as the Director of NCSC, I commit to keeping the committees informed of any such violations that occur under my authority.

b. What are the Director of the NCSC's specific obligations under section 102A, including as to the NIP budget?

The Director of NCSC has an obligation to support the DNI's role in overseeing the programming and execution of the NIP budget. Additionally, the Director of NCSC is charged with providing such information the DNI requests for determining the NIP budget. Additionally, under the *CI Enhancement Act of 2002*, the Director of NCSC, in coordination with the DNI, is responsible for coordinating the development of budgets and resource allocation plans for CI programs and activities, as well as ensuring that the budget and resource allocation plans address CI objectives and priorities.

Intelligence Community CI Offices and Reforms

QUESTION 14: Please describe your authorities over the CI offices within the IC.

While NCSC does not have operational authority over CI offices in the IC, NCSC may promulgate guidance for IC CI programs. Additionally, by setting strategic priorities for CI investigations, operations, and collection, NCSC guides implementation of CI programs within the IC. NCSC also conducts oversight of IC CI offices through its evaluation of their implementation of the National CI

Strategy.

QUESTION 15: Do you see any need for modifications to the statutory role or authorities of the Director of the NCSC? If so, please explain.

The United States faces daunting threats from FIEs that seek to undermine our economic strength, steal our most sensitive information, and weaken our defenses. The growing impact of those activities demands knowledge repositories, strategic orchestration of CI activities across the USG, and greater outreach efforts to engage and disrupt FIE threats.

To address these issues, if confirmed, I intend to work regularly with the ODNI to identify possible adjustments in NCSC authorities to clarify its mission and functions where needed.

Finally, I would note that the Committee's Audits and Projects Team conducted a study of NCSC last year that highlighted several potential changes to the authorities of NCSC. If confirmed as the Director of the NCSC, I would look to work through those recommendations with the DNI and the committee.

NCSC Analysis

QUESTION 16: What unique role does NCSC's strategic CI analysis play as compared to the analysis produced by other IC components?

NCSC serves a unique role within the IC by producing the *National Threat Identification and Prioritization Assessment (NTIPA)*, as required in the *CI Enhancement Act of 2002*. The *NTIPA* establishes the President's national CI priorities, helps policymakers understand the principal FIE objectives and targets, and describes the intelligence threats that could harm the United States. The *NTIPA* provides a baseline for U.S. CI requirements to guide the analytic, collection, operational, and security activities of the IC, and many other NCSC products—including the *National CI Strategy and the CI Production Guidance*—flow from it. In addition, NCSC's National CI Officers lead several interagency initiatives to drive collection, analysis, and operations to identify and counter foreign intelligence entities and protect America's strategic advantage.

In addition to analytic guidance, NCSC contributes to interagency CI risk assessments that integrate IC-coordinated threat information, vulnerability data, and mitigation strategies to assess specific CI risks to the United States. These include embassy site assessments, supply chain risk assessments, and damage assessments related to unauthorized disclosures. Since many of these threats also impact our allied partners, NCSC produces releasable versions of these products, as appropriate.

QUESTION 17: What is the NCSC's role in coordinating and publishing the IC's CI assessments?

As directed by the DNI, and in consultation with appropriate elements of the departments and agencies of the USG, NCSC oversees and coordinates the production of strategic analyses of CI matters, including the production of CI damage assessments and assessments of lessons learned from CI activities. The *NTIPA* reflects the culmination of contributions from and in coordination with the IC, many USG departments and agencies, and other components within ODNI. This document reflects the greatest concerns the IC and U.S. decision makers have about the current foreign intelligence threat landscape, and focuses the CI community's efforts against a range of foreign intelligence threats. Since many of these threats also impact our allies, NCSC produces releasable versions of *NTIPA* products as well.

State and Local Governments

QUESTION 18: What is NCSC's role in producing and disseminating intelligence for state, local, and tribal partners, including information as it relates to insider threats?

a. How is that role different than that of the Federal Bureau of Investigation (FBI) and the Department of Homeland Security (DHS)?

b. What is your understanding of the amount and nature of cooperation among NCSC, FBI, and DHS?

NCSC does not have a direct role in producing or disseminating finished intelligence for state, local, and tribal partners, including those that may relate to insider threats. NCSC partners with IC agencies that are authorized to produce and

disseminate intelligence at this level, such as FBI and DHS, in the production of bulletins, advisories, and appropriate threat warning information designed to inform and empower partners at this level. These entities are authorized to provide threat warnings and have authorities to produce finished intelligence as well.

NCSC also works directly with Executive Branch agencies to: share best practices for countering foreign intelligence and insider threats; and develop web-based platforms to raise threat awareness by creating and disseminating unclassified advisories, bulletins, and guidance that address insider threat topics. NCSC continues to collaborate with ODNI's Federal, State, Local, Tribal, and Territorial (FSLTT) Partnerships Group to address FSLTT insider threat-related equities.

National Intelligence Manager for CI

QUESTION 19: What is your vision of the Director of the NCSC in the role of National Intelligence Manager for CI?

As mission manager for the CI community, if confirmed, my vision is for NCSC to lead innovative CI and security solutions, further integrate CI and security disciplines into IC business practices, and effectively resource such efforts. To do this, we would drive integrated CI activities to anticipate and advance our understanding of evolving FIE threats and U.S. security vulnerabilities. We would drive development and implementation of new capabilities to preempt, deter, and disrupt FIE activities and insider threats, and advance CI and security to protect our people, missions, technologies, information, and infrastructure from FIEs and insider threats. We would continue enhancing the exchange of FIE threat and security vulnerability information among key partners and stakeholders at all levels to promote and prioritize coordinated approaches to mitigation. In carrying out these activities, my goal would be to create a more proactive CI and security posture in the United States, employing all instruments of national power to prevent regional and emerging threat actors from gaining leverage over the U.S.

QUESTION 20: What is the Director of the NCSC's role in developing the *National Intelligence Priorities Framework* with regard to CI?

The Director of NCSC, as the National Intelligence Manager for CI, fulfills the duties of the NIPF Intelligence Topic Expert for CI. The Director is charged with integrating the CI community's efforts across intelligence functions, disciplines,

and activities in an attempt to achieve unity of effort and effect. One of the most important tools for accomplishing those tasks is the *NIPF*. The Director uses the *NIPF* process to prioritize collection and analysis against FIE threats against the United States and codify our approach for the coming year.

The Director of NCSC convenes the CI community and oversees the drafting of the CI *NIPF* topic's priorities to integrate, and prioritize our efforts. NCSC last completed this effort in March of this year, when the Center and subject matter experts from all relevant intelligence agencies and departments came together to review FIE threats and recommended to the DNI a reprioritization to accurately reflect the CI threat level of each foreign intelligence actor. This periodic review helps the IC determine the state of collection and analysis against FIEs, develop integrated strategies to address collection and analytic gaps, and evaluate responsiveness and success in closing those gaps.

QUESTION 21: What is the Director of the NCSC's role in providing guidance on resource allocation with regard to particular CI capabilities and platforms?

The Director of NCSC provides guidance on resource allocation regarding CI capabilities and platforms through the *National CI Strategy* and subsequent implementation plan, as well as through the broader IC's *Consolidated Intelligence Guidance*. In addition, the Director works within established budgetary processes to impact changes required to address CI and security priorities in the NIP and evaluate IC program resource allocations against the *National CI Strategy*'s goals and objectives.

QUESTION 22: What is the Director of the NCSC's role in providing guidance with regard to the allocation of resources among and within IC elements?

The Director of NCSC provides guidance on the allocation of CI and security resources through the Intelligence Planning, Programming, Budgeting, and Execution (IPPBE) process. The Director also advocates directly to the IC CFO and ODNI for resources for the CI and security mission and evaluates whether IC programs are meeting their expected accomplishments. The Director's resource allocation recommendations are informed by NCSC's continuous direct interaction with IC elements and ODNI leadership. NCSC also relies on documents such as the *National CI Strategy* and the *Unifying Intelligence Strategy for CI*, as well as the *Consolidated Intelligence*

Guidance to communicate CI and security priorities to the IC. Using these documents as a guide, NCSC advocates for IC element CI and security resource requests through the IPPBE process.

QUESTION 23: Given resource constraints, how should the Director of NCSC identify unnecessary or less critical programs and seek to reallocate funding?

The Director of NCSC identifies critical and less critical programs through evaluation of CI and security programs and by developing a clear sense of IC priorities through direct interaction with IC and ODNI leadership. Working closely with IC partners, the Director participates in the entire budget process and routinely makes recommendations on strategic CI and security resource priorities, evaluates IC program requests, advocates for CI and security resources, and makes recommendations on resource alignments.

While the Director of NCSC does not have directive authority over funds reallocation, the Director effectively communicates CI and security-related priorities through documents such as the *NTIPA*, the *National CI Strategy*, the *National Intelligence Strategy*, and other CI and security-related policies and guidance so that departments and agencies can align their resources to the identified priorities. NCSC actively shapes the resource environment by routinely reviewing and recommending CI and security-related resource requests as a part of the IPPBE process as well as leveraging its CI and Resource Strategy Board to refine enterprise mission requirements and priorities.

QUESTION 24: What are the most important CI gaps or shortfalls across the IC?

We need to better understand how FIEs exploit the increasing availability of commercial intelligence tools and services to increase their capabilities and cooperate with other state and non-state actors to exploit our vulnerabilities. To increase our understanding and pivot to a more proactive CI posture, the IC must drive integration, action, and resources across the CI community to outmaneuver and constrain FIEs, protect America's strategic advantages, and invest in the future to develop the capabilities and resilience needed to meet the current threats and challenges and those to come.

FIEs seek to collect information from virtually all USG departments and agencies, state and local governments, cleared defense contractors, commercial firms across numerous sectors, think tanks, academic institutions, and more. FIEs are pursuing not only classified information, but also vast troves of unclassified material that can support their political, economic, R&D, military, and influence goals, and their attempts to target U.S. persons, supply chains, and critical infrastructure. We must continue to build trust and increase collaboration with government partners across the federal, state, and local levels as well as in academia and private industry to sensitize these sectors to the growing threats posed by FIEs and develop practical approaches for information sharing and threat mitigation.

We face an increasingly complex technology landscape that requires the modernization of not only of our collective systems, but also requires an equally skilled workforce. We must develop a technically proficient CI workforce trained in key areas such as cyber, critical infrastructure, supply chain risk management, malign investment, and economic security.

Insider Threats and Unauthorized Disclosures

QUESTION 25: What is the role of the NCSC in preventing insider threats and unauthorized disclosures?

EO 13587 established the National Insider Threat Task Force (NITTF), which is co-chaired by the DNI and the Attorney General and is staffed by NCSC and FBI personnel.

The NITTF developed *National Policy and Minimum Standards* to establish a national baseline necessary for USG insider threat programs. The NITTF provides technical and programmatic guidance to Executive Branch departments and agencies, conducts training and workforce professionalization, and disseminates best practices across the USG.

Since its inception in 2011 the NITTF has provided independent assessments of departments and agencies insider threat programs to gauge compliance with the minimum standards and to provide policymakers with a status of the enterprise. NCSC continues to focus on evolving its NITTF framework to measure effectiveness, maturity, and efficiency.

NCSC also maintains significant roles and responsibilities within the IC to deter, detect, and report unauthorized disclosures of classified information. Pursuant to *ICD 701, Unauthorized Disclosures of Classified National Security Information*, NCSC provides guidance and oversight to IC elements on CI and security matters related to unauthorized disclosures of classified information, maintains a repository of notifications from IC elements regarding any loss or compromise of classified intelligence, and reports to the DNI on a semiannual basis data regarding the occurrence of unauthorized disclosures, trends, actions taken, and status.

QUESTION 26: How does NCSC work with the FBI's National Insider Threat Task Force to deter, detect, and mitigate insider threats?

Pursuant to *EO 13587*, the National Insider Threat Task Force is co-chaired by the U.S. Attorney General and the DNI and is staffed by NCSC and FBI. The NITTF's work impacts Executive Branch departments and agencies by deterring, detecting, and mitigating insider threats. Countering insider threats requires a collaborative effort across the government to develop effective strategies and programs. Through these efforts, the NITTF trains and assists agencies in managing insider threat programs. NITTF and the FBI continue to support the USG and partners to mature established insider threat programs.

QUESTION 27: What is your plan to ensure success in preventing insider threats and unauthorized disclosures?

NCSC is taking a multi-pronged approach to ensuring success, including through its management and oversight of implementing the *National Insider Threat Maturity Framework*, the National Operations Security Program (OPSEC), and the IC's Unauthorized Disclosure Program. The NITTF's ongoing initiative to conduct program reviews of USG insider threat programs focuses on compliance with the established Minimum Standards for Executive Branch Insider Threat Programs, and on reviewing federal programs to measure their effectiveness. The NITTF works with agencies to address vulnerabilities in their programs to further enhance program effectiveness. This initiative is designed to detect, deter, and prevent future insider threats.

NCSC continues to improve the IC's approach to protect against unauthorized disclosures as it provides guidance and oversight to IC elements on CI and security matters related to unauthorized disclosures, helping them to deter, detect, and report

unauthorized disclosures of classified information. Pursuant to *ICD 701, Unauthorized Disclosures of Classified National Security Information*, NCSC maintains a repository of notifications from IC elements regarding any loss or compromise of classified intelligence and reports to the DNI on a semiannual basis, data regarding the occurrence of unauthorized disclosures, trends, actions taken, and status.

Acquisition and Supply Chain Risk Management

QUESTION 28: What is the role of the NCSC in preventing and mitigating foreign state and non-state actors from compromising the supply chains upon which the USG relies for its products and services?

NCSC works with USG Supply Chain Risk Management and cyber offices to help them assess and mitigate efforts to compromise USG and industry supply chains. NCSC also collaborates with the USG cyber community and the IC to provide CI and security perspectives on foreign intelligence and other threat actors' cyber capabilities. NCSC facilitates interagency fora and platforms for the sharing of risk information and best practices.

QUESTION 29: What is your plan to increase NCSC's success in preventing and mitigating foreign state and non-state actors from compromising the supply chains upon which the USG relies for its products and services? How do you measure and define "success" in this context?

NCSC intends to expand industry outreach on CI supply chain threats and risk management best practices to further enhance understanding and acceptance of the shared risk environment of modern global supply chains.

Feedback from stakeholders and demand for new capabilities from academia, private industry, allies, and the USG informs NCSC's measurements for success. Success would be bolstered by the introduction of stronger contractual language during USG acquisitions, proactive engagement that identifies vulnerabilities and mitigations up-front, and increased investment in CONUS-based manufacturing of critical technology components.

QUESTION 30: How do you intend to use NCSC's resources and organizational mandate to fight against the licit and illicit acquisition of U.S. sensitive and advanced technology by foreign actors?

NCSC's role in the whole-of-government effort against the licit and illicit acquisition of U.S. sensitive and advanced technology by foreign actors is to integrate, deconflict, educate, and champion the CI community's efforts. Further, NCSC has a role in identifying the variety of tools, capabilities, and partners across government that should be connected to provide much more comprehensive protection for our most vital technologies and capabilities. Additionally, the CI community will continue expanding outreach efforts to highlight the known vulnerabilities in the U.S. science and technology (S&T) infrastructure to industry, government labs, and others developing cutting-edge technologies. The CI community will continue to identify and share best practices for security and espionage awareness.

Providing threat awareness information to our partners and allies helps them make informed decisions about how to improve their security and CI postures. NCSC works closely with the National Labs to facilitate robust training and threat awareness. For example, NCSC recently introduced the "Safeguarding Science" toolkit on its public-facing website. The initiative is designed to raise awareness of the spectrum of risk in emerging technologies and to help our stakeholders in these fields—such as semiconductor and quantum—develop their own programs to protect research and innovation. NCSC partnered in this initiative with several USG organizations—including the National Science Foundation, Office of Science and Technology Policy, and National Institute of Standards and Technology—to provide tangible mitigation options against theft, abuse, misuse, and exploitation of U.S. scientific, academic, and emerging technology sectors. NCSC is also addressing these issues in the forthcoming *National CI Strategy*.

NCSC's outreach and engagement will foster the development of an informed, empowered scientific community that will be best positioned to assess emerging, advanced technologies and their applications (such as AI and quantum computing), design measures to guard against the potential misuse or theft of these technologies, and encourage information exchanges with the national security community. As a result, the IC will be better postured to proactively identify security challenges. NCSC is also addressing this issue in the forthcoming *National CI*

Strategy.

NCSC Personnel and Resources

QUESTION 31: Do you believe that NCSC currently has an appropriate level of personnel and resources? If not, please specify the areas that are lacking and NCSC's current plans to address those areas.

At this time I do not know. If confirmed, I will evaluate NCSC's personnel and resource levels to ensure NCSC is staffed to provide CI and security leadership and support to the USG, conduct outreach to appropriate U.S. private sector entities, and issue public warnings regarding intelligence threats to the United States.

As the threat environment evolves, I will leverage the ODNI planning and budgeting process to ensure NCSC has the technically trained and experienced personnel and resources to meet mission requirements.

Professional Experience

QUESTION 32: Please describe specifically how your experiences would enable you to serve as the Director of NCSC.

I have spent the last 28 years working in Congress overseeing departments and agencies of the United States government that are involved in national security. For the last seven and a half years, I have served first as the Minority Staff Director and then the Staff Director for the Senate Select Committee on Intelligence. In these roles, I helped, with my counterpart, to lead the staff of the committee in overseeing all aspects of the USIC. I also, again, with my counterpart at the time, helped direct the staff of the committee's investigation into Russia's attempt to interfere in the 2016 election. This three and a half year effort involved considerable exposure to, and engagement with, all the various CI elements of the USIC. Further, as part of my daily job responsibilities as the SSCI staff director, I have personal and direct engagement with multiple CI entities in the IC on issues of concern.

Prior to joining the SSCI staff, I was employed for 9 years at the House Armed Services Committee, where I oversaw multiple areas of DOD operations. While not as directly as involved in CI, I was frequently exposed to CI, insider threat, and supply chain risks and programs of the Department of Defense.

To be clear, I am not, unlike the past acting and confirmed Director of the NCSC, an FBI agent. However, and with all due respect to those individuals, each of whom I believe did an excellent job in that role, I believe that my background suits me for this new role, if I am fortunate enough to be confirmed. I have had a broad exposure to the IC and the entire USG national security operations. I have had long, and often in depth, engagement with CI professionals across the IC. As the Staff Director of the SSCI, I have experience in running a staff of over 40 people. Additionally, the role of Staff Director of the committee has frequently required the ability to navigate multiple competing interests, among members, other committees of the Senate, HPSCI, the IC, and the White House, among others, to enact legislation and complete projects, which has direct parallels to how NCSC must navigate the IC and multiple agencies involved in the CI mission. And, as evident by my professional experience, I have a deep appreciation for the oversight responsibilities of the committee and the necessity for partnering with the committee to ensure NCSC meets its mission requirements.

113

SELECT COMMITTEE ON INTELLIGENCE

UNITED STATES SENATE

Post-hearing Questions For

Michael Casey

upon his nomination to be

Director of the National Counterintelligence and Security Center

in the Office of the Director of National Intelligence

QUESTIONS FOR THE RECORD

From Vice Chairman Rubio

National Counterintelligence and Security Center (NCSC) Mission

1. This Committee's Audits and Projects team conducted an 18-month investigation of NCSC's functions and capabilities. In 2022, our Committee held an open hearing to build on this investigation and better establish NCSC's counterintelligence (CI) role and contributions within the Intelligence Community. Our Committee-passed Intelligence Authorization Act for Fiscal Year 2024 codifies the NCSC's mission as one that "shall include organizing and leading strategic planning for counterintelligence activities of the United States Government by integrating instruments of national power as needed to counter foreign intelligence activities."

   Would corresponding statutory definitions for "offensive counterintelligence" and "strategic counterintelligence" further clarify roles and responsibilities within the counterintelligence enterprise? Why or why not?

   During my engagements with NCSC officers, they have expressed appreciation for the Committee's ongoing efforts to codify NCSC's mission. A statutory definition for "strategic counterintelligence" would more clearly delineate and further establish NCSC's role to effectively lead the integration and alignment of national CI mission areas across the US Government. This definition would further enable NCSC to develop and lead strategic CI for the nation, and to guide the conduct of the interagency's strategic CI activities. A definition of "offensive counterintelligence" would likewise have some benefit, as there are seven IC elements with the requisite authorities to conduct offensive CI activities. Although these seven elements and their corresponding offensive CI capabilities are known across the IC, a statutory definition of "offensive CI" would help to further clarify those roles and responsibilities within the entire CI enterprise. It would also help departments and agencies outside the IC to understand the offensive CI capabilities that could be brought to bear in the collective defense of our nation.

2. NCSC and the Federal Bureau of Investigation's (FBI's) Counterintelligence Division have encountered ambiguity and conflicting guidance with regard to CI mission roles and responsibilities.

Which organization do you believe is the interagency lead for Counterintelligence: FBI or NCSC? What is the basis for your position?

Since its creation, NCSC (and ONCIX previously) has provided strategic guidance to the CI Community writ large, knitting together the efforts of CI Community agencies engaged in the full gamut of IC efforts, including collection, analysis, priorities, and resources to accomplish common goals. As I noted, the Federal Bureau of Investigation is a fundamental part of the CI Community and manages numerous CI investigative, analytic, and other resources in the domestic space. The Federal Bureau of Investigation identifies and counters intelligence threats, anchored by law enforcement and other authorities outlined in statute and other policies. In this role, the Federal Bureau of Investigation has always relied upon effective interagency ties and collaboration to accomplish its mission.

If confirmed, how do you plan to work with the FBI's Counterintelligence Division to deconflict roles and responsibilities and to ensure our counterintelligence priorities are met?

If confirmed, I will work closely with the Federal Bureau of Investigation's Counterintelligence Division to ensure counterintelligence priorities are met. The Federal Bureau of Investigation's Counterintelligence program is a fundamental part of the broader CI Community and central to addressing CI threats in CONUS. I will regularly engage with my Federal Bureau of Investigation counterparts, as my predecessors have. I anticipate the Assistant Director of the Federal Bureau of Investigation's Counterintelligence Division will be one of my key interlocutors and among the first calls I make when assessing CI Community resource needs, identifying emerging threats, and responding to policy concerns. I will also commit to continued partnership between NCSC and National Counterintelligence Task Force (NCITF) as NCSC sets strategic plans for CI activities, and NCITF plays an integral role in their implementation. I also commit to participating in government outreach efforts, as appropriate, as NCSC works to raise awareness of foreign intelligence threats. Also, NCSC has several Federal Bureau of Investigation officers on staff, and I will leverage their CI expertise and ability to reach back to the Federal Bureau of Investigation to ensure maximum transparency between our organizations.

China and Counterintelligence Threats

Foreign counterintelligence threats to our nation are only increasing. China is the largest threat we face in this regard and the challenges are wide ranging from supply chains to U.S. technology and intellectual property through its recruitment and academic programs.

1. What are the most critical current counterintelligence threats that China poses, both broadly speaking, and specifically to our supply chain?

   Among the wide ranging, persistent, and long-term intelligence threats China poses to U.S. national and economic security, some of the most critical CI threats include the PRC's efforts to collect classified U.S. national security information; to steal intellectual property and proprietary economic information; and to conduct foreign malign influence efforts against the U.S. Specific to China's intelligence threats to our supply chain, the PRC's efforts to dominate global supply chains and gain access to U.S. Government, military, and industry supply chains are especially noteworthy. The PRC's intelligence services collect and exploit any and all information they can gain on U.S. supply chains as the PRC is well-aware of U.S. dependence on global supply chains.

2. If confirmed, what are your plans for improving our government's supply chain risk management?

   If confirmed, I will ensure that NCSC continues to support integration of supply chain risk management capabilities and processes into the operations of the Federal Government by sharing threat awareness and best practices. Congress established the DNI's Supply Chain and Counterintelligence Risk Management Task Force, which the DNI named Director NCSC to chair. I plan to lead Task Force interagency members in sharing information about vulnerabilities and risk mitigation to help protect the multifaceted aspects of the U.S. government supply chain.

3. If confirmed, what are your plans for addressing the counterintelligence threats from China and our adversary's ability to steal U.S. technology and intellectual property?

   If confirmed, I will continue to lead and integrate the CI community's work to prioritize our response to the intelligence threat from China; raise awareness of the threat to critical technologies and intellectual property; and ensure that all those who might be targets know how to mitigate the threat.

From Senator Lankford

Politicizing Background Investigations

1. This year, the Biden Administration proposed potential revisions to the current SF-86 "Questionnaire for National Security Positions" background investigation form including amending Section 29 "Association Record," to include affiliation with "domestic violent extremist [*sic*] organizations." This language is, of course, already covered in the broad "Affiliations" question in Section 29 regarding membership in an "organization dedicated to terrorism" or "dedicated to the use of violence or force to overthrow the U.S. government."

   How can we be sure that expanding this definition will not politicize the issuance of security clearances?

   I understand that revisions to the SF-86 are designed to modify information collection to enhance an adjudicative determination. Question 29 focuses on those who engage in unlawful activities designed to either overthrow the U.S. Government or challenge a U.S. authoritative entity through illegal behaviors. It is my understanding that clarifying that this question pertains to terrorism regardless of whether it originates internationally or domestically allows for information collection that may be relevant in rendering a trust determination and that the revision to Question 29 seeks to identify those who engage in illegal activities to better assess the characteristics of a trusted individual to include reliability, judgment, integrity, and conduct, not to identify personal beliefs, political views, or other expressions that – if weighed in making security clearance determinations – could politicize security clearance issuances.