S. HRG. 115–396

NOMINATION OF WILLIAM R. EVANINA TO BE THE DIRECTOR OF THE NATIONAL COUNTER-INTELLIGENCE AND SECURITY CENTER

HEARING

BEFORE THE

SELECT COMMITTEE ON INTELLIGENCE

OF THE

UNITED STATES SENATE

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

TUESDAY, MAY 15, 2018

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
30–120 PDF WASHINGTON : 2018

SELECT COMMITTEE ON INTELLIGENCE

[Established by S. Res. 400, 94th Cong., 2d Sess.]

RICHARD BURR, North Carolina, *Chairman*
MARK R. WARNER, Virginia, *Vice Chairman*

JAMES E. RISCH, Idaho
MARCO RUBIO, Florida
SUSAN COLLINS, Maine
ROY BLUNT, Missouri
JAMES LANKFORD, Oklahoma
TOM COTTON, Arkansas
JOHN CORNYN, Texas

DIANNE FEINSTEIN, California
RON WYDEN, Oregon
MARTIN HEINRICH, New Mexico
ANGUS KING, Maine
JOE MANCHIN III, West Virginia
KAMALA HARRIS, California

MITCH MCCONNELL, Kentucky, *Ex Officio*
CHUCK SCHUMER, New York, *Ex Officio*
JOHN MCCAIN, Arizona, *Ex Officio*
JACK REED, Rhode Island, *Ex Officio*

CHRIS JOYNER, *Staff Director*
MICHAEL CASEY, *Minority Staff Director*
KELSEY STROUD BAILEY, *Chief Clerk*

CONTENTS

MAY 15, 2018

OPENING STATEMENTS

WITNESS

SUPPLEMENTAL MATERIAL

NOMINATION OF WILLIAM R. EVANINA TO BE THE DIRECTOR OF THE NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

TUESDAY, MAY 15, 2018

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

The Committee met, pursuant to notice, at 9:31 a.m. in Room SD–106, Dirksen Senate Office Building, Hon. Richard Burr (Chairman of the Committee) presiding.

Present: Burr, Warner, Rubio, Lankford, Wyden, Heinrich, King, and Harris.

OPENING STATEMENT OF HON. RICHARD BURR, CHAIRMAN, A U.S. SENATOR FROM NORTH CAROLINA

Chairman BURR. I'd like to call this hearing to order. I'd like to welcome our witness today, Bill Evanina, President Trump's nominee to be Director of the National Counterintelligence and Security Center, or NCSC.

Bill, congratulations on your nomination. I'd like to note that you've already served honorably as Director of NCSC since June of 2014, before the position required Senate confirmation, necessitating this hearing. So, this is a little bit out of the ordinary.

I'd like to start by recognizing your family: your wife, JulieAnne, and your sons, Dominic, who's 13, and Will, who is 19 months old and currently holding down the fort at home.

[Laughter.]

I had an opportunity to meet your wife and oldest son as we had breakfast this morning, and I just want to say thank you for allowing him to serve so many years in government. And to Dominic, thank you for your dad, because he does important stuff. I want you to know that.

Our goal in conducting this hearing is to enable the committee to consider the nominee's qualifications and to allow for thoughtful deliberation by the members.

Director Evanina has provided substantive written responses to over 55 questions presented by the committee. And, today, of course, committee members will be able to ask additional questions and to hear from him in open session.

Director Evanina graduated from Wilkes University and earned a master's degree in educational leadership from Arcadia University. He has served in government for over 23 years, including service as a supervisory special agent and assistant section chief with

the Federal Bureau of Investigation, and prior to joining NCSC served as chief of counterespionage at the Central Intelligence Agency.

Director Evanina, you're being asked to lead this agency during a period of significant and wide-ranging counterintelligence threats against our Nation. I'm hopeful that, moving forward, you'll be an influential and forceful advocate for those foreign intelligence tools you believe are necessary to keep our citizens safe while protecting Americans' privacy.

As I've mentioned to others during this nomination hearing, I can assure you that this committee will faithfully follow its charter and conduct vigorous and real-time oversight of the intelligence community, its operations and its activities. We'll ask difficult and probing questions of you, your staff; and we expect honest, complete and timely responses. I look forward to supporting your nomination and ensuring consideration without delay.

Thank you again for being here. I look forward to your testimony.

I'll now recognize the Vice Chairman.

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

Vice Chairman WARNER. Thank you, Mr. Chairman.

I want to echo the Chairman's remarks in welcoming Bill Evanina today. Obviously, Bill, 22-year veteran of the FBI, Director of the National Counterintelligence and Security Center. As the Chairman mentioned, you've had this job for four years. But we thought it was so important that we made it Senate-confirmed, so you get to go through your first confirmation hearing process. You're obviously no stranger to this committee and all the members on the committee. You've briefed us many times, and I think you bring remarkable skills to this position.

In my questions today, I want to focus on two issues. One is security clearances. This committee has had a couple hearings on that subject, both open and closed. We all know the DNI is the government's security executive agent and you as the DNI's point person have to take the lead on that.

As you've acknowledged, and I think this committee additionally has acknowledged, the current system is broken: 740,000-person backlog, costs too much, takes too long, way too complex. We've had lots of testimony about continuous evaluation, better use of technology, trying to knock down, on the DOD side, a big amount of that backlog. I'd like this morning if you would add a little more details and provide us any update.

The second issue that I want to focus on will be your role to oversee the counterintelligence security activities across the U.S. government, particularly with regards to some of our near-peer nation-state adversaries, Russia, China, their whole-of-society approaches. I believe, particularly the challenge posed by China in terms of its acquisition of our technology secrets, and their penetration of starting at early stage companies, through the penetration of universities, and some of the companies that this committee has highlighted in the past. We're going to need to up our game on that. So I look forward to your testimony on that subject as well.

Thank you, Mr. Chairman. I look forward to the witness' testimony.

Chairman BURR. Thank you, Vice Chairman.

Bill, could I ask you to stand and raise your right hand?

Do you solemnly swear to give the committee the truth, the whole truth, and nothing but the truth, so help you God?

Mr. EVANINA. I do.

Chairman BURR. Please be seated.

TESTIMONY OF WILLIAM R. EVANINA, NOMINATED TO BE THE DIRECTOR OF THE NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

Chairman BURR. Director, before we move to your statement, I'll ask you five standard questions that the committee poses to each nominee who appears before us. They just require a simple yes-or-no answer.

Do you agree to appear before the committee here or in other venues when invited?

Mr. EVANINA. Yes.

Chairman BURR. If confirmed, do you agree to send officials from your office to appear before the committee and designated staff when invited?

Mr. EVANINA. Yes.

Chairman BURR. Do you agree to provide documents or any other materials requested by the committee in order to carry out its oversight and legislative responsibilities?

Mr. EVANINA. Yes.

Chairman BURR. Will you ensure that your office and your staff provides such materials to the committee when requested?

Mr. EVANINA. Yes.

Chairman BURR. And fifth, do you agree to inform and fully brief to the fullest extent possible all members of the committee on all intelligence activities, rather than just the Chairman and the Vice Chairman?

Mr. EVANINA. Yes.

Chairman BURR. Thank you very much.

We'll now proceed to your opening statement, after which I'll recognize members by seniority for five minutes. Bill, the floor is yours.

Mr. EVANINA. Thank you, Senator.

Chairman, Vice Chairman, members: I have issued a statement for the record which I'd like to be added to the record and I'll have some brief comments.

It's an honor to appear with you today to consider my nomination to be the first Director of the National Counterintelligence and Security Center, or NCSC. It's also an honor and privilege that this Congress has decided this position to be important enough to make it a Senate-confirmed position. I'm also honored the President and Director of National Intelligence Dan Coats have the trust and confidence in me to fulfill this position.

I would first like to express my gratitude to my family: my father John, my mother Barbara, my brother Steven, my sister Tanya, most especially my wife, JulieAnne, and my sons Dominic and Will.

Lastly, I would like to thank the women and men of the National Counterintelligence and Security Center, who are dedicated professionals, and their successes in the last few years have made NCSC the global leader in counterintelligence and security.

Mr. Chairman, I was born and raised in Peckville, Pennsylvania, a small blue-collar town just north of Scranton. There, through my family and friends, I learned the value of integrity, hard work and service to others.

One of those neighbors was Gino Merli, private first class in the U.S. Army during World War II. Mr. Merli was awarded the Medal of Honor, two Purple Hearts and a Bronze Star for his heroic activities in the Battle of the Bulge. Spending time with Mr. Merli and other role models growing up, I learned the value of character, citizenship and service, and we should never take our democracy or freedom for granted.

Mr. Chairman, I am proud to be a career public servant. I've been in Federal service for over 29 years, 22 of which as a proud member of the FBI. I've held a wide spectrum of positions in the FBI and, as you mentioned, chief of the Central Intelligence Agency's counterespionage group.

Mr. Chairman, the threat we face from our adversaries is progressive, persistent, and requires constant mitigation by our government and private sector. The most prominent and enduring nation-state intelligence threats will continue to be Russia and China. However, Iran, North Korea and others are prominent with their intent and increasing capabilities.

I believe the aggressive Russian intelligence services will continue their efforts to interfere and create distrust in our democratic processes, encourage anti-U.S. political views, and weaken our U.S. partnerships and European allies.

China's utilization of intelligence services and nontraditional collectors to advance their national development continues to place our national security at risk. The U.S. must continually and aggressively respond to China's systematic theft of U.S. technology, trade secrets, proprietary data, research and development across wide swaths of the U.S. economy. Mr. Chairman, I proffer today that our economic security is our national security.

Mr. Chairman, historically, the mitigation of these national security threats lay solely at the feet of the intelligence community and Federal law enforcement. I proffer today, that to successfully thwart the threats and the complexity that we see not only requires a whole-of-government approach, but a whole-of-country approach.

Mr. Chairman, insider threats are a pernicious intelligence vulnerability that we face every day. Although we'll never eliminate the possibility of a bad actor within our walls, we continue to strive toward enhanced technical and behavioral solutions to prevent catastrophic damage, as well as to develop creative solutions to prevent and deter this activity.

Mr. Chairman, as you and the Vice Chairman are fully aware, our government security clearance process is outdated and inefficient. It is currently undergoing a comprehensive overhaul.

We plan and will develop and implement a process that results in the expeditious onboarding of qualified U.S. citizens both into

government and in cleared industry with agility and reciprocity. At the same time, we must not reduce the quality of the investigations, to ensure that we are bringing on a quality, highly trusted workforce to protect our secrets.

If confirmed, and as the executor of the DNI's role of security executive agent, I am committed to leading this effort, in partnership with the Office of Personnel Management, the Office of Management and Budget, and Department of Defense.

Mr. Chairman, I am humbled. If confirmed, I would become the first Senate-confirmed Director representing the men and women of the NCSC. As well, I will represent the men and women who have toiled for decades in the counterintelligence security field, often without attribution and knowledge. They do so to protect our people, our data, our secrets and our Nation.

Chairman Burr, Vice Chairman Warner, members of the committee, thank you again for your consideration of my nomination. I look forward to your questions.

[The prepared statement of Mr. Evanina follows:]

STATEMENT FOR THE RECORD
WILLIAM R. EVANINA FOR CONFIRMATION HEARING BEFORE THE SENATE SELECT COMMITTEE ON INTELLIGENCE
TO BE DIRECTOR OF THE
NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER
(15 May 2018)
216 Hart Senate Office Building

Chairman Burr, Vice Chairman Warner, and Members of the Committee.

It's an honor to appear before you today as you consider my nomination to be the first Senate confirmed Director of the National Counterintelligence and Security Center (NCSC). I am grateful that the Congress has considered the position I currently hold to be sufficiently important to require Senate confirmation—an acknowledgment of the significant, and growing, challenges being addressed by NCSC to enhance our nation's security.

In my capacity as Director of NCSC over the last several years, I've often appeared before this, and other Congressional committees. I have great respect for the importance of Congress' oversight role, and I have prided myself in keeping Congress fully and currently informed about developments within my cognizance in the counterintelligence and security field. If confirmed, I will continue this important information sharing commitment to Congress.

I am also honored and grateful that the President and the Director of National Intelligence have the trust and confidence in my ability to continue to serve our nation's counterintelligence and security enterprise.

I would first like to express my gratitude to my family; my mother Barbara, father John, brother Stephen, and sister Tanya – and particularly my wife JulieAnne, and my sons Dominic and Will, who are present with me today. Their love and support means everything to me.

I also want to thank the men and women of NCSC and ODNI, who lead and support both the counterintelligence and security mission as we have made NCSC the global leader in both mission areas.

I was born and raised in Peckville, Pennsylvania. There—through my family and neighbors—I learned the value of integrity, hard work, duty, pride in country, and service to others. One of those neighbors—who lived just a few blocks from my family's house—had a particularly strong influence on me.

Gino Merli was a Private First Class in the U.S. Army during World War II. He landed on Omaha Beach on D-Day, and later fought in the Battle of the Bulge. Mr. Merli was awarded the Medal of Honor for blocking a German advance at a U.S. Army outpost in Belgium.

When I was growing up, he advised my friends and me about the importance of character, citizenship, and service. I also learned from Mr. Merli that we should never take our freedom for granted.

Mr. Chairman, I am proud to be a career public servant. I believe that my past service has been solid preparation for the position I hold today, and for which I'm being considered for confirmation.

I've been in the federal service for over twenty-nine years—twenty-two of which were spent as a Special Agent with the Federal Bureau of Investigation (FBI). And as I've described in the Committee's questionnaire, I've held a wide spectrum of leadership roles at the FBI in the law enforcement and national security fields. I have also been the Chief of the CIA's Counterespionage Group, so I have served in the lead domestic and international CI agencies.

Mr. Chairman, I have led the organization that is now known as the National Counterintelligence and Security Center since June, 2014. If confirmed, I will continue to lead NCSC and serve as the head of counterintelligence for the U.S. Government, and as the principal counterintelligence and security advisor to the Director of National Intelligence.

The foreign intelligence threat is one of the most significant threats to our country. On February 13, Director of National Intelligence Dan Coats appeared before this Committee to provide the Intelligence Community's annual threat assessment.

I agree with DNI Coats' assessment that the United States faces a complex global foreign intelligence threat. The most prominent state intelligence threats to U.S. interests will continue to be Russia and China, based on their services' capabilities, intent, and broad operational scope.

As a nation we were not prepared for Russia's intent and action to interfere in U.S. democratic processes and institutions. I believe that the Russian intelligence services will continue their efforts to encourage anti-U.S. political views, create wedges that reduce trust and confidence in democratic processes, weaken U.S. partnerships with European allies, and undermine Western sanctions.

Until fairly recently, China's use of its intelligence services to advance its national development (thereby undermining the economic security of the U.S.) did not receive adequate attention. The U.S. must continue to respond to China's systematic theft of U.S. technology across broad swaths of the U.S. economy, which represents a critical national security threat. Our economic security IS our national security.

The most critical CI threats cut across these threat actors: influence operations, critical infrastructure, supply chain, and traditional as well as economic espionage. 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.

Advanced technology previously available mainly to leading nation-states is now increasingly available to a wide range of nation-state and non-state actors as well. For example, a growing set of threat actors are now capable of using cyber operations to remotely access traditional intelligence targets, as well as a broader set of U.S. targets including critical infrastructure and supply chain, often without attribution.

Insider threats – sometimes with the encouragement of external actors – are a pernicious intelligence threat to maintaining our secrets and our national security. Unauthorized disclosures also have a devastating impact on the men and women who serve every day to protect our secrets, our data, our systems, and our personnel.

If confirmed, I commit to the continual leadership of the Intelligence Community and the U.S. Government efforts to address these significant, and increasingly complex, global intelligence threats to the United States.

As the Director of NCSC, and as prescribed in your legislation which created my role, I am responsible for leading and supporting the counterintelligence and security activities of the U.S. Intelligence Community, the U.S. Government, and U.S. private sector entities at risk from intelligence collection by foreign adversaries.

And I would like to emphasize that NCSC safeguards privacy and civil liberties, and practices appropriate transparency in all counterintelligence and security programs to ensure accountability to Congress and the American people.

Mr. Chairman, as you, the Vice Chairman, and all Members of this Committee are keenly aware, our government's security clearance process is outdated and inefficient, and requires a comprehensive overhaul. Currently, there are 4 million Americans deployed around the globe – in over 100 agencies and departments – who possess a security clearance. We must develop and implement a business process that results in the expeditious onboarding of highly qualified citizens – both in the U.S. government and cleared industry – with agility and complete reciprocity. At the same time, we must not reduce the quality of the investigations to ensure we are hiring a highly trusted workforce that will protect our nation's secrets. If confirmed, as the executor of the DNI's role as the Security Executive Agent, I am committed to leading this important government-wide effort. In partnership with Office of Personnel Management, Office of Management and Budget, and the Department of Defense I commit to provide this committee by the end of the year a comprehensive plan for vetting a trusted workforce in a modernized manner employing a robust Continuous Evaluation program and

maximizing technology. I also commit to working with your committee to develop metrics which will effectively evaluate progress and provide a baseline to hold agencies and departments accountable.

Additionally, within 30 days of this hearing the DNI will issue guidance to departments and agencies clarifying, aligning, and modifying the 2012 federal investigative standards.

Mr. Chairman, I'd like to conclude my remarks by sharing a story that illustrates the commitment to public service that I, along with my colleagues at the National Counterintelligence and Security Center share.

One year ago, NCSC staff traveled to the National Archives to renew our Oath of Office as federal employees. We assembled in the National Archives' Exhibit Hall where our nation's foundational documents—the Constitution, the Bill of Rights, and the Declaration of Independence—are on display. To me, these are sacred documents, and this was the most fitting place to renew our Oath and commitment to the laws of this great nation.

As federal civil servants, we pledge our loyalty to the Constitution and the rule of law. Our service to the American people is defined by scrupulous adherence to the law and the ideas and ideals embodied in these important documents.

I am honored to lead the NCSC workforce. I am also humbled that, if confirmed, I would become the first Senate confirmed Director to specifically represent the men and women of that organization who have toiled behind the scenes in the global counterintelligence and security arenas for decades protecting our nation. Our success in protecting our nation's security is based on teamwork in a hard-working, respectful, collaborative, and professional work environment with our partners throughout the government and private sector.

Public service is a tremendous honor as well as an enormous public trust. And as intelligence professionals, we are custodians of our nation's secrets. We have a special responsibility to our fellow citizens. All of us are firmly committed to serving the American people and abiding by the

Constitution and the rule of law. If confirmed, I will remain committed to these essential goals.

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

Chairman BURR. Bill, thank you very much for that testimony. The Chair would recognize himself, and then the Vice Chairman and then members by seniority for up to five minutes of questions.

Bill, we've talked about it before: Leaks of classified information put sensitive sources and methods at risk and cause irreparable damage to our national security. Congress took action accordingly in the FISA Amendments Reauthorization Act of 2017 by imposing enhanced penalties on those convicted of unauthorized disclosures.

If confirmed, how do you plan to address insider threats and the security of sensitive and classified information?

Mr. EVANINA. Mr. Chairman, thank you for that question. And I would concur that the unauthorized disclosure of classified information is not only traumatic to the secrets that we lose as a country, but they're also harmful and insidious to the men and women who serve to protect them every day.

If confirmed, I will continue to work with my Federal law enforcement partners, both at the FBI and Department of Justice, to enhance not only the investigations, but the penalties for such unauthorized disclosures, as well as with the intelligence community, to enhance their ability to identify unauthorized disclosures within their walls and provide the most effective and efficient monitoring and provide information where that information—to the Department of Justice and the FBI for prosecution.

Chairman BURR. Good.

Foreign counterintelligence threats to our government supply chain continue to increase and China has become a big part of these threats. In your experience in counterintelligence both at NCSC and in your prior positions at CIA and the Bureau, how has China's counterintelligence threat grown? And what should we be concerned with?

Mr. EVANINA. Thank you, Mr. Chairman. I do believe China is one of the gravest concerns that we have moving forward as a Nation with respect to our economic security. China's utilization of a whole-of-government approach towards the United States to increase their economic and military development is problematic.

The utilization of nontraditional collectors here in the United States—engineers, scientists, students in school—and their ability to, from a cyber-enabled perspective, identify and attract unclassified data from our research facilities, continues to allow the U.S. to not only lose positions, jobs, research and funding, as well as provide first-to-market capability to the Chinese and take our ingenuity and proprietary data and trade secrets away.

Chairman BURR. In your response to the committee's questions, you stated that some of the greatest challenges to NCSC include conducting effective and sustained outreach to Federal partners, research labs and the private sector, as well as securing funding for supply-chain risk management. What are the plans for improving our government's supply-chain risk management?

Mr. EVANINA. Thank you, Mr. Chairman. Supply-chain mitigation efforts are nothing new to the U.S. However, in the last couple years they've become increasingly problematic via awareness. What NCSC does is provide that sliver of counterintelligence aspect to the who and why is implementing and mitigating our supply chain, our adversaries. And we provide and work in partnership with the

non-Title 50 organizations, General Services Administration, the labs, the weapons labs, DOE labs, to provide awareness and what the threat is emanating from our adversaries, to help them mitigate, from their perspective, and protect their data from leaving their facilities.

Chairman BURR. I thank you for that, and I want to encourage you that in the role of Director please continue to focus on that greatly. This committee has been extremely involved in supply chain concerns that we have, and it seems to slip through the cracks from a jurisdictional standpoint in Congress and, for that fact, in government.

Vice Chairman.

Vice Chairman WARNER. Thank you, Mr. Chairman.

Bill, I'm going to start with clearance reform. I think you'll recall when we had the hearings, bipartisan complete agreement the system is broken. It's 740,000-plus on the backlog. This is a security risk. This is an economic risk in terms of our ability then to brief companies.

I was very concerned that we invited all the relevant parties to testify. OMB chose not to. I would like you to give us an update on whether OMB is on the team now in trying to make this a priority.

And we'd had some discussion that that large-number backlog, you were going to be able to cut a dramatic amount of that backlog back in a relatively short timeline. Can you give us an update on that?

Mr. EVANINA. Thank you, Vice Chairman Warner.

Yes. As a matter of fact, I think subsequent to our beginning this process back in March, in our Trusted Workforce 2.0 initiative, with our partners, Office of Management and Budget, OPM and DOD, as well as a host of other organizations and departments, we have been working diligently to provide this committee and the government with two specific things. Number one, a dramatic reduction to the backlog; and number two, the development of a new business process of how we will vet qualified citizens in the U.S. in an agile, expeditious manner, at the same time making sure they're trusted.

With respect to your question on the backlog, we currently are in the final stages of a paper for the DNI to issue that's being coordinated through the intergovernmental process right now, which I believe, with some dramatic changes to how we currently do the business process of investigations, once implemented, will probably get us to a position we could estimate probably a 20 percent reduction to backlog within six months.

Vice Chairman WARNER. Only 20 percent in six months? That's a little less ambitious than I think we discussed earlier. And is OMB part of the process at this point?

Mr. EVANINA. OMB is a major part of the process. Again, the four main individuals are OMB, OPM, DOD and ODNI.

Vice Chairman WARNER. Well, and will these new business processes include reciprocity and common standards between government and our contractors?

Mr. EVANINA. Yes, sir.

Vice Chairman WARNER. Again, my hope would be, since I understand a lot of these were on the Secret level, the DOD has said there was an ability to take, I thought, a much greater percentage of that backlog down with administrative action.

And then, on a going-forward basis I would hope that we would see a reduction greater than 20 percent. That would only take us down—you know, if we moved from 740,000 to half a million, that still doesn't do very well if we're at the end of this calendar year.

Mr. EVANINA. Senator, I agree with you and concur. I think some of the contingencies will be predicated upon the transfer of the MBIB inventory to DOD and how that impacts the planned mitigation efforts. We do not have an effective algorithm for that at this moment, but we are excited. That 20 percent is probably a conservative number.

Vice Chairman WARNER. On the question of counterintelligence with China, again, a number of members on this committee have raised concerns about certain of the Chinese telecom companies and their penetration into the American market. I was actually pleased that the President acted on one of those companies, ZTE.

Now, it appears that that is simply a bargaining chip in negotiations with China. I don't think that is the appropriate way. If this is a security threat, it is a security threat and needs to be dealt with as such, not as a bargaining chip in terms of greater trade negotiations. My concern as well is that we are asking purchasers of equipment at local government, private sector, we're asking others who are in the venture community and others to understand the threat of China, but I don't believe we can fully brief that threat if they don't have appropriate security clearances within their own institutions—again, another challenge that comes out of the backlog issue.

How will we be able to move aggressively on having a standardized brief to universities, tech companies, VCs on the real threat of China? That brief I think will have to be some parts classified, as well as unclassified. Do you want to address that?

Mr. EVANINA. Vice Chairman, I would concur. And I think over the last two years we've made a lot of progress with our interagency partners, the FBI and DHS, in promulgating such advice and awareness and threat to not only academia and industry, with respect to the threat from China and other nation-states who are pernicious in their stealing our proprietary data and trade secrets. We will continue to do that and work with the associations.

And I concur with your point that I think private-sector leadership, that is at the CEO level, needs to be a little bit more active in terms of obtaining security clearances so that that information that is classified can get to them in a more effective and efficient manner.

Chairman BURR. Senator Wyden.

Senator WYDEN. Thank you, Mr. Chairman.

I want to pick up, Mr. Evanina, on the Vice Chairman's point with respect to ZTE specifically. And thank you for the visit we had in our office. I thought it was very helpful.

Now, in 2012, the House Intelligence Committee issued a nonclassified bipartisan report on national security issues posed by the Chinese telecom companies, and one of them was ZTE. The report

concluded that the risks associated with ZTE's provision of equipment to U.S. critical infrastructure could undermine American national security interests. Do you agree with that bipartisan report?

Mr. EVANINA. Senator Wyden, I do.

Senator WYDEN. Okay. Now, they recommended that the United States should view with suspicion the continued penetration of the U.S. telecommunications market by ZTE. Do you agree with that?

Mr. EVANINA. Yes.

Senator WYDEN. Now, I appreciate the response. The President's comment over the weekend about ZTE I think obviously raises extraordinary national security questions, as well as economic policy concerns. So, if you're confirmed, I hope you're going to stand up to the White House on this issue.

Let me ask something with respect to where things stand now. What are the national security implications of giving ZTE sanctions relief?

Mr. EVANINA. Well, Senator Wyden, I'm not particularly up to speed with the sanctions with regard specifically to ZTE. I will say that the intelligence community and Federal law enforcement is on the record with this committee and the American people with respect to the threat posed by China Telecom.

Senator WYDEN. But as a general proposition, giving sanctions relief to a company like this, where there has been a bipartisan, non-classified report, as a general proposition that strikes me as a mistake from a counterintelligence standpoint, from a cyber-security standpoint, from an economic policy standpoint. So just tell me, as a general proposition, whether you would agree with that.

Mr. EVANINA. Well, Senator, I would agree that we will continue to provide the policymakers in this body with the relevant intelligence information to have effective policy——

Senator WYDEN. That's not the question I'm asking. Set aside ZTE. As a general proposition, does that raise the concerns I mentioned—economics, national security, cyber-security? Seems to me it's pretty low-hanging fruit here to say yes.

Mr. EVANINA. Well, Senator, again I'm not up to speed with the sanctions per se with your reference. So I would have to continue with—we will continue advising on the foreign intelligence threat to policymakers who want to employ those sanctions.

Senator WYDEN. Let me ask you one other question. What has been learned, again from a counterintelligence standpoint, since the OPM breach? You know, obviously, that affected an extraordinary number of Americans. I would hope that that would be seen as a wake-up call and there would be some substantive changes.

So what has been learned? What has changed since the OPM breach?

Mr. EVANINA. Thank you for that question, Senator Wyden.

I think that the biggest OPM reflection is that I think we learned as a country that nothing is off limits from foreign adversary attack here, specifically in our non-Title 50 organizations in our country and government as a whole. The intelligence community is no longer just the target and victim of adversaries; that as a country we need to be aware of our proprietary data, trade secrets and PII.

Senator WYDEN. Let me ask you one other question about encryption. Obviously counterintelligence risks are not limited just to classified systems. Extremely politically sensitive information is conveyed every day by government officials and members of Congress over unsecured phones. Should the intelligence community recommend that policymakers encrypt their unclassified phone conversations?

Mr. EVANINA. Yes, Senator.

Senator WYDEN. Okay. Thank you. I hope that you will think some more about this matter that has been raised by ZTE. I can understand why you might not want to comment about a specific company. But, I'm telling you, as a general proposition, this ought to be an enormous alarm bell from the standpoint of counterintelligence, cyber-security, and economics. So I hope you'll think more about that.

Thank you, Mr. Chairman.

Chairman BURR. Senator Rubio.

Senator RUBIO. Thank you, Mr. Evanina, for being here. Would you ever use a ZTE phone?

Mr. EVANINA. I would not, Senator.

Senator RUBIO. Would you recommend anyone in any sort of position that's sensitive, whether in commerce or in government or in contracting, use a ZTE phone?

Mr. EVANINA. No, I would not.

Senator RUBIO. So it's not an exaggeration to be—there's somehow the notion out there by some that this is a hysteria, not just unique to ZTE. But it is a fact, is it not, that China utilizes its telecommunication companies for purposes of espionage. Even if those companies' leadership may not be open to it, they don't really have a choice but to be cooperative.

Mr. EVANINA. Senator Rubio, we've been on the record in the intelligence community and law enforcement of that fact.

Senator RUBIO. There's an additional national security factor at play, and that is that Made in China 2025 is an endeavor by the Chinese government to dominate the top fields of the 21st century, many of them in telecommunications, aerospace, biomedicine, et cetera. If in fact they achieve that because they're more competitive, because they have better ideas, because they out-innovate us, that's one thing. But that's not how they're pursuing it. How they are pursuing it, is it not, is they are stealing intellectual property, reverse-engineering, the transfer of intellectual property?

There is a strategic aim on the part of the Chinese government to steal the commercial intellectual property of this country in order to advance themselves into a position of dominance in these key fields. Is that not something that is pretty clear?

Mr. EVANINA. That is correct, Senator.

Senator RUBIO. And that poses a national security threat, because our commercial capacity—just like our shipbuilding capacity is important to our military hardware and our aerospace is, our technological capacity in the private sector. If we lose the high ground and another nation is dominant because they cheated their way into that position, does that not pose a direct national security threat to the United States?

Mr. EVANINA. It does, Senator. And, as I mentioned, I believe our economic security is our national security.

Senator RUBIO. Now, I want to talk about a separate topic that has not, I don't believe, ever been discussed before, certainly not today. As you know, we live in an environment where false claims, even ones that are totally preposterous, can easily be spread on social media. And often the media, under tremendous pressure to deliver clicks on their website or ratings on their television station through outrage, are quick to jump on it.

I raise that because of the concept of something called "deep fakes." Are you familiar with that term?

Mr. EVANINA. I am not, sir.

Senator RUBIO. A deep fake is the ability to manipulate sound, images, or video to make it appear that a certain person did something that they didn't do. These videos in fact are increasingly realistic. The quality of these fakes is rapidly increasing due to artificial intelligence. Machine learning algorithms are paired with facial mapping software to make it easy and cheap to insert someone's face into a video and produce a very realistic-looking video of someone saying or doing something they never said or did.

This, by the way, technology is pretty widely available on the internet and people have used it already for all sorts of nefarious purposes at the individual level. I think you can only imagine what a nation-state could do with that technology, particularly to our politics.

If we could imagine for a moment, a foreign intelligence agency could use deep fakes to produce a fake video of an American politician using a racial epithet or taking a bribe or anything of that nature. They could use a fake video of a U.S. soldier massacring civilians overseas. They could use a fake video of a U.S. official admitting a secret plan to do some conspiracy theory of some kind. They could use a fake video of a prominent official discussing some sort of impending disaster that could sow panic. And imagine a compelling video like this produced on the eve of an election or a few days before major public policy decision with a culture that has already a kind of a built-in bias towards believing outrageous things, a media that is quick to promulgate it and spread it, and of course social media, where you can't stop its spread.

I believe that this is the next wave of attacks against America and Western democracies, is the ability to produce fake videos that can only be determined to be fake after extensive analytical analysis, and by then the election is over and millions of Americans have seen an image that they want to believe anyway because of their preconceived bias against that individual.

You've never heard of that term, but I ask you, is there any work being done anywhere in the U.S. government to begin to confront the threat that could be posed, or will be posed in my view, by the ability to produce realistic-looking fake video and audio that could be used to cause all sorts of chaos in our country?

Mr. EVANINA. Thank you, Senator Rubio, for that question. And the answer is yes. The entire intelligence community and Federal law enforcement is actively working to not only understand the complexities and capabilities of our adversaries, but what, from a

predictive analysis perspective, we may face going forward, particularly with the election this fall, as well as in 2020.

Chairman BURR. Senator Heinrich.

Senator HEINRICH. Mr. Evanina, welcome.

The DOD has recently banned sales of ZTE phones at military exchanges, as well as Huawei equipment. And last month, the Commerce Department banned China's smartphone maker, ZTE, from using U.S. technology after it illegally shipped U.S. goods to both Iran and to North Korea. This comes after numerous intelligence community warnings that ZTE poses a major cyber-security threat.

Yet, as we saw this week, President Trump announced that he is working with the Chinese president to give ZTE, quote, "a way to get back into business fast," end quote.

Do you assess that ZTE represents an economic or security threat to the United States?

Mr. EVANINA. Thank you for the question, Senator. I believe the intelligence community and law enforcement are clearly on the record, both in the public and in classified settings, with the threat from Chinese telecommunications companies.

Senator HEINRICH. Are you concerned from a counterintelligence perspective? Does it make sense to overrule the advice and judgment of the national security community and to offer ZTE a way to get back into business fast?

Mr. EVANINA. Thank you, Senator. I believe our role in the intelligence community and the counterintelligence community is to provide the relevant facts of the issue in the investigations to the policymakers for their decision-making processes.

Senator HEINRICH. How are you raising those facts with this White House?

Mr. EVANINA. We are garnering the support of the entire intelligence community and regulatory community. And, as a matter of fact, I think we've had meetings as recently as yesterday at the White House.

Senator HEINRICH. If China believes that we are willing to use national security matters as bargaining chips in trade negotiations, how do you think that will impact their behavior, moving forward?

Mr. EVANINA. Senator, thanks for the question. I'm not an expert on the Chinese diplomatic processes, but I can tell you that our national security is first and foremost in our perspective. And the whole-of-country approach posed by China clearly makes it difficult for us to bifurcate the issues.

Senator HEINRICH. So two months ago DHS and the FBI issued a rare public alert about a large-scale Russian cyber campaign targeting the U.S. power grid and other critical infrastructure with an intent to extract information and potentially lay a foundation for future offensive operations. This alert went further than past alerts, confirming Russia as the culprit and including indicators of compromise and a list of detection and prevention measures.

What's happened since March of this year, when the alert went out? And is this Russian cyber campaign ongoing?

Mr. EVANINA. Senator, thank you for that question. And I would agree that the pervasive threat from the cyber perspective by the Russian government continues today and will into the future.

The Federal Government, specifically the intelligence community, Federal law enforcement and DHS, have been working with the private sector every day.

As a matter of fact, NCSC, we brought in not only the Department of Energy, but major companies in the fuel, gas and oil perspective to give them a one-day read-in in a classified brief of the threat, so we could help them mitigate those issues back in their home facilities.

Senator HEINRICH. Did that include utilities as well?

Mr. EVANINA. It did.

Senator HEINRICH. Are you seeing a greater sense of urgency on the part of utility companies and other energy institutions to utilize this new information?

Mr. EVANINA. Yes.

Senator HEINRICH. Are we getting utility leadership through the clearance process fast enough?

Mr. EVANINA. I'm not sure about that, Senator. I'd have to get back to you with respect to the speed at which that's occurring.

Senator HEINRICH. Because that's another concern. And I know Senator Warner brought up the overall issue. I mean, one of the things that we have heard on the Energy and Natural Resources Committee is, that even former members of Congress who served on the relevant intelligence committee, can't get through that process.

And so, if we don't have partners who are read in on the other side, it makes it very difficult for those utilities and those other energy institutions to actually implement the changes that they need to implement.

Mr. EVANINA. Thank you, Senator. I believe, working closely with DHS—they are working diligently to provide an expeditious process to get individuals and companies cleared so they can receive this threat information on a real-time basis.

Senator HEINRICH. You've said that continuous evaluation is not the future, it's now, and that the government honestly has not done a good job. Industry is able to conduct continuous evaluation of their employees. Why has it been difficult for the government to do so? And what can we do about that?

Mr. EVANINA. Thank you, Senator, for the question. Continuous evaluation has been a constant bedrock in the intelligence community for years. What we've been asked to do at NCSC, through the auspices of the ODNI, from this committee is provide a robust continuous evaluation program for the rest of the Executive Branch, and we have done that. We are probably 80 percent complete, ahead of schedule, hope to be fully complete by the end of the year. We are expecting to have 20-plus agencies and 100,000 Federal employees outside the intelligence community enrolled into our continuous evaluation plan.

Senator HEINRICH. Thank you, Mr. Evanina.

Thank you, Mr. Chair.

Chairman BURR. Senator Lankford.

Senator LANKFORD. Mr. Chairman, thank you very much.

Thanks for being here and for going through this process. And by the way, thank you for your years of service leading up to this. It's exceptionally valuable for the country.

You make several very interesting statements in your opening statement and in your written statement that I want to be able to ask you to drill down a little bit deeper on. You made this statement: "A growing set of threat actors are now capable of using cyber operations to remotely access traditional intelligence targets, as well as a broader set of U.S. targets, including critical infrastructure and supply chain, often without attribution."

What are you recommending there? You're making a statement there, but you're also making a recommendation.

Mr. EVANINA. Thank you for that question, Senator Lankford. I believe that we as a Nation need to be more in a true public-private partnership with those out in our country who actually make things and build things—our utility companies, the energy, telecommunications and financial networks that are the bedrock of our Nation. The government needs to partner in a very, very close manner with them, so they can understand the threat and provide efforts to help mitigate that threat.

Senator LANKFORD. So what does that look like? In a public-private partnership, are you talking about government dictating how this would work in the private industry and the private industry does it? The private industry sets a set of standards from NIST or from wherever it may be?

Is this DHS? What entity do you think does that? And where does that happen most efficiently?

Mr. EVANINA. Thank you, Senator. I believe that it's a combination, starting with DHS. What we do at NCSC is provide that sliver of counterintelligence threat to not only the DHS and Department of Energy, but as well as all those companies, so they can understand the who and why and what's happening, and then help other Federal organizations and regulators provide mitigation to those. If I believe that those companies out there providing those services don't understand the threat and how it's manifested, they can't be in an effective position to prevent it.

Senator LANKFORD. What's the best way for them to get information about the threat? If I'm a pipeline company in Oklahoma, what's the best way for me to be able to determine what's the real threats that are coming at me?

Mr. EVANINA. Two ways, sir: through the Department of Energy, as well as the FERC, who is the regulator for that organization we work very closely with to provide threat information. And I believe that process is pretty effective.

Senator LANKFORD. Talk to me a little bit about hiring and retaining individuals for the team. You've got a lot of competition getting some of the best folks. We've got some incredible patriots that are there because of their love for their country and their respect for the rule of law. What are you seeing right now for hiring and retaining individuals and for the future?

Mr. EVANINA. Thank you, Senator. I'm pretty aware that the intelligence community continues to attract to the right type of amazing U.S. citizens for their jobs. I believe that our mission in the intelligence community will win the day. The challenge is getting them in the door, as we spoke of. But I believe the mission will keep them in for long periods of time.

The security clearance process has been—the undergoing of the business process re-engineering will help get us the individuals in the door quicker, more expeditious, not only in the government, but in the private sector, including industry as well.

Senator LANKFORD. You had a nice, long hesitation on the security process, which all of us have incredible frustrations with at this desk and those that are doing the hiring. What is the right length of time to be able to get through a security clearance? Because we will do a good security clearance, but right now it's a ridiculous amount of time. What's the right amount of time?

Mr. EVANINA. Well, Senator, it's a trick question, but I'll give you—I believe that Secret clearances and below, which are primarily Department of Defense, I think in the end state we should be able to clear 80 or 90 percent of those within 30 days.

Senator LANKFORD. How long will it take to get to that spot, you think?

Mr. EVANINA. Again, with my partners watching closely here, I would have to say within the next two years we're able to get to that as an official policy and implementation. It's a little bit more complicated at the Top Secret level, as you're aware.

Senator LANKFORD. Sure.

Mr. EVANINA. We're working on those metrics, as well.

Senator LANKFORD. Yes, but most people are not going through the Top Secret level starting out through the clearance. I think a 30-day, 45-day even, is a reasonable amount of time to be able to go through a Secret clearance. What is the time right now per clearance?

Mr. EVANINA. It's closer to 100 days, sir.

Senator LANKFORD. Right. And for many people in excess of that, and that's a major issue for us.

You also make some interesting comments about the election security in your opening statement and in your written statement. Your concerns continue to rise about a Russian threat towards our election security. I know we're partnering with DHS. My question to you is not about the threat; it's about how we're responding to it. What's the current level of cooperation between you and DHS in preparing for those threats because DHS has the lead?

Mr. EVANINA. Thank you, sir.

And DHS has been a great partner, not only with the intelligence side, but NPPD, who has direct interface with the State and locals with respect to the election process, which—elections are local. We have been working really closely with them, bringing the entire intelligence community to service DHS and provide real, up-to-date threat information like we have never done before, so that DHS can manifest that information and provide mitigation strategies for all elections who are at the local level.

Senator LANKFORD. So cooperation and communication between DHS and you are consistent right now?

Mr. EVANINA. That's correct.

Senator LANKFORD. Okay, thank you.

I yield back.

Chairman BURR. Senator King.

Senator KING. Thank you, Mr. Chairman.

Mr. Evanina, welcome. Delighted to have you here today and appreciate the service that you've provided.

First, I want to associate myself with Senator Rubio's comments and emphasize one point. He talked about the deep fake, the idea of being able to create an alternative reality. If you add to that the powers of social media, it's a perfect storm of disinformation, because you can create the false reality and then you can circulate it in a way that it's very hard to counteract, to find, to see.

If somebody puts a negative ad about you on television, you can put up your own ad to rebut it. In this case, you're chasing smoke. It's all over the place—e-mails, Twitter, Facebook. It's very difficult. So, I think this is a very serious challenge.

That brings me to your comment on question 16 of the prehearing questions. You said: "I remain concerned that we may still be underestimating Russian capabilities and plans to influence the 2018 midterm and future elections." That's a chilling statement. Could you elaborate on that a bit?

Mr. EVANINA. Thank you, Senator. I would say that I don't think anyone in my profession or the intelligence community will underestimate the potential of the Russian Federation, Vladimir Putin, or the intelligence service in their capabilities, but, more importantly, their intent. And I think, from what we saw in the last election cycle, their intent is there and their capabilities are clearly there.

To your first statement regarding the deep fake, I think that serves as an opportunity for us in the analytical community and the Federal Government to provide enhanced training and awareness of the deep fake; and maybe also an opportunity to partner with the private sector and social media companies to understand the capabilities of our adversaries on our own social media networks.

Senator KING. Well, the ultimate defense on that is for our public to understand when they're being conned, for them to realize where this is coming from. And I think sources are very important.

You mentioned about the capabilities of the Russians and their intent. Do you have any doubt about the accuracy of the January 2017 report of the intelligence community on the Russian activities in the 2016 election?

Mr. EVANINA. I do not.

Senator KING. Thank you.

I also want to emphasize a point that's been made several times before. The clearance backlog is an enormous problem. My frustration is, I can't find out a single point, the single point in the United States government that's in charge of solving this problem. And I know it's not you, but you're in a key position. And I believe that in order to solve it it's going to take—and I keep hearing "whole-of-government." Whenever I hear "whole-of-government," I think that means "none-of-government."

Somebody's got to be in charge, and I hope that you will urge the administration, the IC, DNI, to take charge of this issue so that it's not scattered all over the government, because we've got to solve it. We had testimony there are something like 950,000 security clearances in backlog, and we're losing good people. There's an op-

portunity cost there, and it's just unacceptable in terms of our ability to defend the country.

So, I hope you will take on, as part of your mission, pushing for an organizational response to this, where there's some central responsibility and accountability for this.

Mr. EVANINA. Thank you, Senator. The government looks to the Director of National Intelligence as the security executive agent for this process, and I believe, and the government believes through executive order, that he is accountable for the policies set forth, how we conduct investigations and adjudications. And by virtue of—as executor of that program, I believe that responsibility of leadership lies with me.

Senator KING. When I was in business, I always tried to formulate contracts and relationships so that you had one throat to choke.

[Laughter.]

And that was the way you can get things done.

On this question of cyber security and the attacks on our country, in my view and the view of many of us in this committee and in other committees, one of the fundamental problems with our response to this is that it's purely defensive; that we're simply trying to patch our way out of this problem; and that there is no deterrent, there is no cyber doctrine or cyber strategy that will deter our adversaries and make them think twice. We had testimony before Armed Services from the head of the NSA that nothing we have done would, quote, "change the calculus of our adversaries."

Do you believe that this is an area that we need to do more work in and develop a public deterrence strategy so that those who intend to attack us through cyber, just as they would through kinetic, believe that they will and will certainly pay a price?

Mr. EVANINA. I do, sir.

Senator KING. And could you expand on that a bit?

Mr. EVANINA. Well, I believe two aspects of that. Number one, I think our adversaries need to know that our deterrence policy is real and it will manifest itself in their home base so they understand it.

But I think more importantly, I think we owe it to the American people for them to understand that the government has policies and procedures in place to protect them, protect private industry, from these cyber threats that we face.

So I concur we need to be a little bit more effective and efficient with our deterrence policies.

Senator KING. I hope you will help us develop that strategy, because I think otherwise we're just going to continue to be chipped away at. Again, we're looked on as a kind of free lunch in this regard.

Thank you. I appreciate your testimony.

Mr. EVANINA. Thank you.

Chairman BURR. Thank you, Senator King.

Vice Chairman WARNER. I just want to echo what Senator King has said, that we need that articulated cyber doctrine. I was, again, disappointed that it appears the National Security Council is now trying to eliminate the cyber position in the White House, a direct report to the President. That does not send the right signal.

But thank you very much, Bill, for your testimony. I look forward to working with you.

Mr. EVANINA. Thank you, Senator.

Chairman BURR. I have to admit I was questioning whether Senator King was going to be quoted from this hearing about a cyber doctrine or "one throat to choke."

[Laughter.]

I have a feeling I know which way it's going to go.

Senator KING. I realized I was taking that risk as the words were leaving my——

[Laughter.]

Chairman BURR. I think we have exhausted questions, Director. Thank you, and I thank your family again for your willingness to serve.

Let me note for members, QFRs are required before the end of business today. It is my intent to move the Director out of committee next week, so that we can get this to the floor as quickly as we can.

With that, again, our thanks for your service.

This hearing is adjourned.

[Whereupon, at 10:18 a.m., the hearing was adjourned.]

Supplemental Material

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- BIOGRAPIDCAL INFORMATION

1. FULL NAME: William R. Evanina
   OTHER NAMES USED: Bill Evanina

2. DATE AND PLACE OF BIRTH:
   DATE OF BIRTH: 06/15/1967
   PLACE OF BIRTH: Peckville, PA
   CITIZENSHIP: US

3. MARITAL STATUS: Married

4. SPOUSE'S NAME: JulieAnne Evanina

5. SPOUSE'S MAIDEN NAME IF APPLICABLE: Sebold

6. NAMES AND AGES OF CHILDREN:

   NAME

   INFORMATION REDACTED

7. EDUCATION SINCE HIGH SCHOOL:

INSTITUTION	DATES ATTENDED	DEGREE RECEIVED	DATE OF DEGREE
Keystone College	1985-1987	Associates	May 1987
Wilkes University	1987-1989	Bachelor of Arts	May 1989
Acadia University	2000-2005	Master of Arts	May 2005

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
ODNI	Director, NCSC also retains FBI status	Bethesda, MD	06/14 – present

CIA	Chief, Counterespionage also retains FBI status	Langley, VA	08/13 – 06/14
FBI	Assistant Special Agent Counterterrorism and Counterintelligence	Washington DC	09/10 – 08/13
FBI	Special Assistant National Security Branch	Washington DC	02/10 – 09/10
FBI	Assistant Section Chief	Washington DC	03/09 – 02/10
FBI	Supervisory Special Agent	Trenton, NJ	07/06 - 02/09
FBI	Supervisory Special Agent	Newark, NJ	04/04 - 07/06
FBI	Special Agent	Newark, NJ	09/96 – 04/04
GSA	Project Manager	Philadelphia, PA	06/89 – 09/96

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

   See previous.

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 currently serve as the Director of the National Counterintelligence and Security Center (D/NCSC), and have been in this role since June 2014. In this unique role, I oversee and guide the Intelligence Community (IC), U.S. Government agencies, and departments in protecting our nation from hostile threat actors and their associated intelligence collection against the U.S., our personnel, data, and systems. In this role, I am granted access to some of the most sensitive intelligence collection and investigations, and have developed a solid bond of trust and partnership with counterintelligence and security leaders across the U.S and private sector. Additionally, I have successfully led our Five Eyes (FVEY) partners in areas of counterintelligence and security in my roles as the Chair of the Allied Security and Counterintelligence panel (ASC) as well as Chair of the NATO Committee on Counterintelligence. These two roles have allowed me to drive strategic efforts across the globe against our most active nation state aggressors.

    Prior to my current role as D/NCSC, I served as the Chief of Counterespionage at the Central Intelligence Agency (CIA). Prior to serving at the CIA, I served as the Assistant Special Agent in Charge of the FBI's Washington Field office, leading both counterterrorism and counterintelligence investigations and programs. I also served as the Assistant Section Chief of the FBI's Russian Programs within the Counterintelligence Division. Prior this role I served as the Senior Resident Agent in the FBI's Trenton Office and as the Supervisory Special Agent for the FBI's New Jersey Joint Terrorism Task Force

while assigned to the Newark FBI Office.

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).

2018	Pinnacle Award presented by the Institution of Critical Infrastructure Technology (ICIT)
2016	Security Magazine's Top 18 Influential Security Professionals
2007	FBI Director's Award for Investigative Excellence (Espionage investigation of convicted spy Leandro Aragoncillo)

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
Alexandria Little League	Coach/Manager	2015-2017
Mt. Vernon Recreational Center	None	2012-present
Cameron Station Community	None	2009-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?

See attachment. The attachment represents my best effort to identify all published writings and speeches during my tenure at the National Counterintelligence and Security Center (NCSC). At my previous position at the CIA, I had no public speaking engagements. Prior to working at the CIA, however, I did extensive public speaking as a senior manager at the FBI.

If asked, I would be happy to provide a copy of any of these published materials.

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 believe that our nation is faced with a vast array of and increasingly complex threats from nation state actors and others, threatening our democratic systems and values. I believe I have the necessary leadership skills to work closely with the Intelligence Community, the entire U.S. Government, and strategic members of the private sector to counter these efforts.

I believe I am qualified to serve as the Director of the National Counterintelligence and Security Center for numerous reasons. First, my investigative, operational, and leadership experiences in the FBI and CIA have allowed me to understand the divergent missions, authorities, and responsibilities of respective departments and agencies within the Intelligence Community. Second, I have successfully led and managed personnel from multiple agencies and departments over the past 18 plus years in a collaborative working environment under one roof with one united mission to defend our nation. I have successfully served as the Director of the National Counterintelligence and Security Center since 2014, leading the counterintelligence and security community and providing strategic guidance and policy to over 100 departments and agencies in the U.S. Government. Additionally, I have concurrently and successfully served as the primary counterintelligence advisor to the Director of National Intelligence. I also serve as the Chair of the FVEYS Allied Security and Counterintelligence Forum and the Chair of the NATO Counterintelligence Panel. In these roles I lead and facilitate intelligence sharing and best practices with our international partners.

Beyond my personal qualifications for this position, my biggest personal strengths lie in three specific areas. The first is my personal passion for protecting our nation and understanding all the intangibles required to do so as a senior governmental leader. Second, my love of and success in leading and motivating men and women from disparate agencies, departments, and cultures to achieve a common goal – defending our national security. Third, my ability as a senior leader to clearly identify key stake holders and partners and hold myself accountable to those partners and to oversight by Congress.

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.

    I am currently a federal employee.

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.

    If confirmed, I would continue to serve as an employee of the U.S. Government.

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 currently have no plans subsequent to completing 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 ANYWAY 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.

Spouse currently serves as Vice President of Digital Sales and Marketing at SiriusXM. There is no relation between her company and her position to the position for which I seek confirmation.

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

INFORMATION REDACTED

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 ACQESCENCE AND YOU HAD REASON TO BELIEVE THE GIFT WAS GIVEN BECAUSE OF YOUR OFFICIAL POSITION.)

As a senior government official, I received a variety of hats, mugs, photographs, and other non-reportable gifts and items. Any reportable gift was listed in my agency disclosure reports.

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

Please reference 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, however please reference OGE 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.)

INFORMATION REDACTED

INFORMATION REDACTED

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.

    Virginia

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. I have ensured my financial holdings meet U.S. Government ethics requirements and I do not believe my current holdings would present a conflict of interest. If confirmed, I will execute and abide by an ethics agreement with ODNI to avoid any conflicts of interest under the applicable statutes and regulations.

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?

2017, 2016, 2015. 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.

A. 2007: FBI internal administrative inquiry into nominee and numerous others pursuant to the accidental death of a Special Agent during an operation/arrest. Nominee was subsequently cleared with respect to any and all administrative inquiries.
B. Anthony McGill vs. FBI (2009): This was a class action suit filed against 14 FBI personnel and NJ Law Enforcement personnel pursuant to an arrest. Applicant and all other FBI personnel were represented by the Department of Justice due to fact that apprehension took place within the confines of their official duties. Suit was dismissed in federal court.
C. Judicial Watch vs. Office of the Director of National Intelligence: No 17-CV-508 D.C., 2017: Sued in official capacity in this FOIA suit, applicant and other defendants named in official capacity are being defended by DOJ, Federal Programs Branch. DOJ filed Notice to Dismiss in August 2017.

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 GILTY 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.

See Number 38 above.

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.

Not to my knowledge. However, as a long-time federal employee (29 years), agencies of which I have been employed or worked for have been the subject of routine inspector general audits, reviews, and inspections.

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.

Yes, multiple times as part of my employment (FBI Special Agent) and as required for my Top Secret Security Clearance.

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 COUNTERINTELLIGENCE AND SECURITY CENTER AND THE INTELLIGENCE COMMITTEES OF THE CONGRESS, RESPECTIVELY, IN THE OVERSIGHT PROCESS.

As the Director of NCSC, one of ODNI's major mission centers, I have testified before Congress and briefed Members and staff numerous times over the years. I place a high value on these interactions, and believe that supporting Congress in its essential oversight role is an integral part of my responsibilities. Under Section 502 of the National Security Act of 1947, the DNI, in consultation with the heads of other departments and agencies involved in intelligence activities, shall keep the intelligence committees fully and currently informed of intelligence activities. I believe congressional notification must be timely, accurate, and complete to be effective.

Furnishing information to the oversight committees is vital to Congress' role in considering legislation, determining the appropriate level of resources for NCSC, assessing the effectiveness of the Center, and gaining a better understanding of counterintelligence and security issues. If confirmed, I will remain committed to ensuring that the NCSC workforce understands the importance of congressional oversight, provides thorough and timely information to Congress, and is responsive to congressional queries.

49. EXPLAIN YOUR UNDERSTANDING OF THE RESPONSIBILITIES OF THE DIRECTOR OF THE NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER.

As directed in statute, the D/NCSC serves as the head of counterintelligence for the U.S. Government, including coordinating the development of resource and allocation plans, setting operational priorities, developing strategies including the National Threat Identification and Prioritization Assessment and the National Counterintelligence Strategy, and conducting outreach and vulnerability assessments. The D/NCSC also serves as the principal substantive adviser on all aspects of counterintelligence for the DNI and serves in support of the DNI's central role in the development and implementation of personnel security policy across the U.S. Government.

Just as important as these statutory roles, the D/NCSC is responsible for leading the men and women of the NCSC in their integration, coordination, and oversight roles and ensuring they have the tools, authorities, and resources necessary to execute their mission. If confirmed, I would continue to leverage all existing authorities to support NCSC's workforce and to accomplish NCSC's vital mission.

AFFIRMATION

I, **WILLIAM R. EVANINA,** DO SWEAR THAT THE ANSWERS I HAVE PROVIDED TO THIS QUESTIONNAIRE ARE ACCURATE AND COMPLETE.

3 OCT 18
(Date)

SIGNATURE OF WILLIAM EVANINA

SIGNATURE OF NOTARY

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.

SIGNATURE OF WILLIAM EVANINA

Signature

Date: 3.5.19

Attachment: Publications and Speaking Engagements

9 July 2014	BENS New York remarks
11 Sep 2014	BENS Chicago remarks
1 Oct 2014	Tunneling Summit remarks
22 Oct 2014	Federal News Radio interview
5 Nov 2014	Continuous Evaluation/Social Media radio inquiry
24 Nov 2014	WTOP radio interview
4 Dec 2014	National Press Club remarks
8 Dec 2014	Federal News Radio interview
11 Dec 2014	2014 Law Enforcement – Homeland Security Forum remarks
7 Jan 2015	FBI's 811 Conference remarks
14 Jan 2015	Washington Post interview
15 Jan 2015	DOS/SPC Off-site remarks
24-28 Jan 2015	NATO CI Panel (Brussels) chaired and made remarks
23 Feb 2015	Russia CI Conference (NGA) remarks
18 Mar 2015	China CI Conference (NGA) remarks
19 Mar 2015	2nd Annual Cyber Security Summit (McLean) remarks
24 Mar 2015	Supplier Management Council Meeting National Security Threat Brief
31 Mar 2015	National CI and Security Conference remarks
2 Apr 2015	6th Annual Cybersecurity Technology Summit (AFCEA) remarks
13 Apr 2015	International Technical Security Conference (Dip Sec HQs) remarks
15 Apr 2015	BENS Washington, D.C. remarks
27 Apr 2015	30th Annual Nat'l Security Forum (Chantilly) remarks

18 May 2015	NDI/AIA National Conference (Scottsdale, AZ) remarks
21 May 2015	ODNI Annual Conference/FBI "Center's" panel discussion
9 Jun 2015	Partner's Board luncheon (Partnership Engagement) remarks
17 Jun 2015	2015 DCIA Faculty Representative Conference-NIM Panel (National Security & Global Issues)
22 Jun 2015	National Student Leadership Conf. on Intelligence and Nat'l Sec remarks
15 Jul 2015	Iran CI Conference remarks
21 Jul 2015	NATO CI Panel
18 Aug 2015	BENS Dallas remarks
19 Aug 2015	BENS Houston remarks
24 Aug 2015	Los Angeles Times interview
16-17 Sep 2015	Opening/Closing Remarks National CI & Sec Conference
29 Sep 2015	ASIS Conference (Anaheim, CA)
22 Oct 2015	WTOP radio interview
29 Oct 2015	DON Enterprise Annual Event remarks
2 Nov 2015	Wilkes University interview
3 Nov 2015	National Fusion Center Association (Alexandria, VA) remarks
5-6 Nov 2015	NASA CI Conference (Houston, TX) remarks
12-13 Nov 2015	Wilkes University remarks
10 Dec 2015	2015 Law Enforcement – Homeland Security Forum remarks
17 Feb 2016	BENS Baltimore remarks
18 Mar 2016	IPF Canberra remarks
30 Mar 2016	2016 National CI and Security Conference remarks

5 Apr 2016	31st National Security Institutes IMPACT Conference remarks
7 Apr 2016	BENS New York City
26 Apr 2016	Travel Financial Services Sector Conference (Chicago) remarks
28 Apr 2016	INSA Symposium (Chantilly) remarks
4 May 2016	China CI Conference remarks
13 May 2016	Op-Ed, "Security Clearances in the age of social media," The Hill
16-17 May 2016	NDIA/AIA Conference (Scottsdale, AZ) remarks
9-10 Jun 2016	NATO CI Panel (Sofia, Bulgaria) remarks
15 Jun 2016	2016 Cybersecurity Summit (Tysons) remarks
16 Jun 2016	2016 IC-Global Force Protection Summit remarks
20 Jun 2016	2016 Russia CI Conference remarks
15 Aug 2016	NGA Insider Threat Day remarks
7 Sep 2016	INSA/AFCEA Intelligence Summit (Panel)
15-16 Sep 2016	IPF (Ottawa) remarks
29 Sep 2016	JHUAPL CI Day (Laurel, MD) remarks
30 Sep 2016	JCITA (Quantico) remarks
4 Oct 2016	2016 Security Leadership Conference (Bethesda, MD) remarks
5-6 Oct 2016	2016 Fall National CI and Security Conference remarks
25 Oct 2016	NS2 Solutions 5th Annual SAP NS2 Summit (Falls Church) remarks
28 Oct 2016	Associated Press interview
15 Nov 2016	Fall NDIA/AIA Security Conference (San Antonio) remarks
30 Nov 2016	Delaware InfraGard (Newark, DE) remarks
14 Dec 2016	2016 Law Enforcement – Homeland Security Forum remarks

11 Jan 2017	Fed News Radio interview
11 Jan 2017	Kent School—Managing Collaborative Analysis (Reston) remarks
24 Jan 2017	HASC Hearing (CI Threat overview)
31 Jan 2017	SSCI Member briefing (CI overview)
2 Feb 2017	Harvard Club remarks
9 Feb 2017	Chaired NATO CI Panel (Brussels)
14 Feb 2017	Council on Foreign Relations (New York City) remarks
23 Feb 2017	ICIT Briefing on Insider Threat (National Press Club) remarks
28 Feb 2017	BENS (Atlanta, GA) remarks
16 Mar 2017	NRC Regulatory Information Conference (Bethesda) remarks
22 Mar 2017	MIT Lincoln Laboratory remarks
23 Mar 2017	SSCI hearing
4 Apr 2017	Insider Threat Summit remarks
10 Apr 2017	INSA CI Conference (Arlington, VA) remarks
20 Apr 2017	2017 DSAC Annual Conference (Boeing) remarks
25 Apr 2017	ASIS International CSO Center remarks
28 Apr 2017	IPF remarks
22-23 May 2017	2017 Joint Annual NDIA/AIA Industrial Conference (Scottsdale) remarks
1 Jun 2017	2017 National CI and Security Conference remarks
6 Jun 2017	SSCI Hearing
7 Jun 2017	FBI Washington Field Office remarks
14 Jun 2017	Domestic Security Executive Academy remarks
12 Jul 2017	SSCI staff briefing

12 Jul 2017	Cipher magazine interview
19-20 Jul 2017	Chair NATO CI Panel (Romania)
28 Jul 2017	Reuters interview
7 Aug 2017	Fox News interview
8 Aug 2017	Interagency OPSEC Support Staff Symposium (IOSS) remarks
15 Aug 2017	BENS (San Antonio, TX) remarks
16 Aug 2017	BENS (Austin, TX) remarks
30 Aug 2017	Op-Ed, "Holding a security clearance: A privilege as well as a responsibility," Federal Times
6 Sep 2017	AFCEA-INSA Summit panel
7 Sep 2017	Cuba CI Conference remarks
11 Sep 2017	NPR radio interview
13 Sep 2017	ISWG remarks
15 Sep 2017	NGA Federal Partners off-site remarks
25 Sep 2017	Annual Seminar and Exhibits (Dallas) remarks
26 Sep 2017	ASIS/InfraGard (Dallas) remarks
28 Sep 2017	Bloomberg TV interview
29 Sep 2017	National AFIO Symposium remarks
10 Oct 2017	2nd Annual Insider Threat Symposium remarks
11 Oct 2017	HOGAR Hearing (Security Clearance Investigations)
23 Oct 2017	Weinberger media interview
24 Oct 2017	SAP NS2 remarks
25 Oct 2017	HPSCI/HOGR briefing
27 Oct 2017	Annual 2017 DoD CI/HUMINT Conference remarks

31 Oct 2017	Reuters interview
31 Oct 2017	Op-Ed, "Cybersecurity Threat: A Call to Action," Federal Times Radio
1 Nov 2017	(Hearing) HPSCI Members
9 Nov 2017	National Fusion Center Association remarks
13 Nov 2017	NDIA/AIA ISC Fall Conference (San Diego) remarks
28 Nov 2017	BENS Boston remarks
5 Dec 2017	ACI's National Summit remarks
11 Dec 2017	Annual Russia CI Conference remarks
12 Dec 2017	Domestic DNI Representative Conference (Houston) remarks
5 Jan 2018	Op-Ed, "How to Protect Critical Infrastructure from Insider Threats," Institute for Critical Infrastructure Technology

SELECT COMMITTEE ON INTELLIGENCE

UNITED STATES SENATE

Additional Questions for
Mr. William R. Evanina upon his nomination to be Director of the National Counterintelligence and Security Center

Responsibilities of the Director of the National Counterintelligence and Security Center

The Director of National Intelligence (DNI) established the National Counterintelligence and Security Center (NCSC) in 2014 to integrate the Intelligence Community's (IC's) counterintelligence and security missions. The NCSC was designed to serve as the primary organization to undertake counterintelligence and security responsibilities within the Office of the Director of National Intelligence (ODNI).

QUESTION 1: What is your understanding of the unique role of the NCSC within the IC?

NCSC's unique role in the Intelligence Community (IC) arises from its unique mission set across the U.S. Government and with our allied partners. NCSC's current mission statement, as reflected in the *2018-2022 National Counterintelligence and Security Center Strategic Plan*, is to lead and support the U.S. Government's counterintelligence (CI) and security activities critical to protecting our nation; provide counterintelligence outreach to U.S. private sector entities at risk of foreign intelligence penetration; and issue public warnings regarding intelligence threats to the U.S. Within the IC, the Director of NCSC serves as the National Intelligence Manager for Counterintelligence (NIM-CI) and the Director of National Intelligence's (DNI's) principal substantive advisor on all aspects of CI.

Additionally, as the DNI's staff support element, NCSC executes 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 13587, NCSC also serves as the co-director—along with the Federal Bureau of Investigation—of the National Insider Threat Task Force on behalf of the DNI to strengthen insider threat programs across the U.S. Government (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 is the head of national counterintelligence for the U.S. Government. In this role, the Director of NCSC is responsible for producing strategic planning assessments, developing and implementing national counterintelligence strategies, overseeing and coordinating counterintelligence analysis, developing priorities for counterintelligence investigations and functions, conducting vulnerability studies, and performing counterintelligence outreach activities. The Director of NCSC also coordinates the development of CI budgets and resource allocation plans. NCSC is responsible for the production of the *National Threat Identification and Prioritization Assessment* as well as the *National Counterintelligence Strategy*.

Additionally, under Section 119B of the National Security Act, the Director of National Intelligence designated NCSC as a National Intelligence Center to align CI and security functions. In support of its role as a National Intelligence Center, the Director of the NCSC is responsible for leading and supporting the integration of the U.S. Government's CI and security activities, providing outreach to Federal and private sector entities, and issuing public warnings regarding intelligence threats to the U.S.

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

Yes, I have discussed these issues with DNI Dan Coats. He has high expectations of me as a leader, and high expectations of NCSC as a mission center. He expects continued mission and programmatic leadership in the CI and Security community, not only within the IC, but throughout the rest of the Executive Branch. Non-IC departments are a critical part of our national security fabric, yet they are particularly vulnerable to nation state HUMINT and cyber activities. Of great concern are the protection of our critical infrastructure and mitigation of supply chain threats which impact the U.S. Government, the private sector, research and development, and academia. Additionally, Director Coats expects a larger role for NCSC in private sector outreach to deliver threat information and warning about nation state activities. He is also expecting NCSC to take a leadership role in driving security clearance modernization across the U.S. Government, in partnership with the Office of Personnel Management and the Office of Management and Budget.

QUESTION 4: You are a long-time FBI employee. How do you ensure that each of the 17 intelligence agencies is represented at NCSC and is bought into the mission? Why does it make sense for the head of NCSC to be an FBI careerist?

As the Director of NCSC, it is critically important to me that the Center's workforce represents the community and has the requisite skills and experience. NCSC currently has a government workforce comprised of approximately half cadre ODNI officers, and half detailees from other agencies. Those agencies currently include the military services, the "Big Six" IC agencies, as well as some other key agencies in the CI and security community, such as the Departments of Energy and State. We also have detailees from non-IC agencies with significant CI and security experience. The mix of cadre and detailees is a function of the need for continuity and expertise over time (cadre), and the desire to avoid an entrenched bureaucracy (detailees). These rotational detailees refresh the workforce and infuse up-to-date operational knowledge and experience from across the IC, while gaining a better appreciation for the unique role of NCSC which they bring back to their home organizations. NCSC also must maintain a stable cadre population for continuity over time and oversight of various business and infrastructure capabilities. The current NCSC leadership team is a reflection of this balance: My deputy and I are detailees, while the #3 and #4 are ODNI cadre officers.

While I am a 21-year FBI veteran, much of my experience has been in national security programs where I have consistently partnered with other IC elements to accomplish the mission. Additionally, I served as the Chief of the CIA's Counterespionage Group, leading over 200 highly dedicated men and women. I firmly believe the Director of NCSC must have two fundamental characteristics: first is the demonstrated experience and ability to lead highly motivated senior personnel from multiple agencies with disparate missions and cultures, and second is significant experience in the counterintelligence arena. Hence, although an FBI national security executive typically meets these characteristics, I do not believe it is imperative that future directors of NCSC be from the FBI.

NCSC Mission

The NCSC's 2016-2020 Strategic Plan provides that the NCSC's mission is to "lead and support the counterintelligence and security activities of the U.S. Government, the U.S. Intelligence Community, and U.S. private sector entities at risk of intelligence collection, penetration or attack by foreign and other adversaries."

QUESTION 5: Are the findings of NCSC's annual mission review reports concerning the implementation of the National Counterintelligence Strategy of the United States (National CI Strategy) socialized with NCSC mission partners?
Yes. NCSC shares its analysis of mission partner responses to the Mission Review Questionnaire and community-wide findings in feedback letters to the IC elements. I personally sign the letters and my staff coordinates drafts of these letters with appropriate CI and Security elements before they are finalized. The findings are then shared in executive sessions between the NCSC Director and Deputy Director and CI and Security leadership from the IC elements. We include a holistic approach to this process, addressing issues such as CI, security, cyber, insider threat, supply chain, operations, collection, and analysis.

QUESTION 6: Does NCSC monitor the mission partner community for subsequent action taken in response to identified implementation shortfalls?
Yes. The comprehensive IC Mission Review process ensures that previously identified shortfalls are addressed in subsequent assessment activities. When Mission Reviews are conducted, NCSC reviews the prior year's findings and assessments and revisits them as necessary. We assess the status of previously identified issues, emerging concerns, and any gaps. We then monitor actions taken to resolve areas of concern and work with the individual agencies throughout the year to monitor progress. In the next cycle, we provide tailored Mission Review questionnaires to each IC element, requesting updates to agency-specific actions cited in earlier feedback letters. Our ultimate goal is to both ensure significant progress in previous year shortfalls, and at the same time, assist in driving mission enhancement by each agency.

QUESTION 7: NCSC and Defense Security Service (DSS) have closely related missions. How do you and DSS work together to secure the larger IC/DoD enterprise?

DSS strengthens national security at home and abroad through its security oversight of 13,000 cleared defense contractor facilities and their robust education operations. Given NCSC's private sector outreach responsibilities and focus on protection of critical technologies and our supply chain, there is a natural and healthy overlap. Recognizing this, in May of 2016, NCSC assigned a senior officer to DSS to perform liaison duties between DSS, NCSC, ODNI, and select departments and agencies within the Executive Branch. Since that time, several key liaison initiatives have enhanced analytic integration, operational support, and threat and warning.

Counterintelligence analysts from DSS provide threat information collected directly from private industry that highlights foreign intelligence attempts to target national security information at defense contractor facilities, which then informs national level assessments. Joint products highlighting the threat and recommending mitigation measures are now more widely available through the use of DSS's robust dissemination network. DSS's Center for the Development of Security Excellence is partnering with the National Insider Threat Task Force (NITTF) to make online insider threat training widely available across the USG and private sector. DSS and NCSC are also in coordination concerning security clearance modernization efforts to ensure that we maintain a trusted workforce. I communicate on an almost daily basis with the Director of DSS, who is a part of every leadership effort NCSC drives across the USG and private sector.

QUESTION 8: Based on your experience at NCSC, what is your assessment of the NCSC's current strengths and weaknesses as to NCSC's stated mission?

NCSC has transformed significantly since standing up as a national center in December 2014. NCSC's current strengths are clearly embodied in the diverse group of highly qualified women and men from numerous agencies who work together every day to accomplish the mission. Additionally, NCSC's ability to successfully lead IC- and government-wide collaboration and partnerships to deliver high level products to policymakers has never been stronger.

Due to NCSC's successes over the past few years, and the ever-increasing complexity of nation state threats, insider threats, and security clearance issues, NCSC is continuously asked to take on new challenges. Successfully addressing these challenges without a corresponding increase in resources is difficult. For example, increased staffing of technically skilled professionals is essential for meeting long-term mission requirements. In addition, we will have to better leverage technology and Artificial Intelligence in our increasingly data-rich world. NCSC has developed into a CI and Security leader among our "Five Eyes" and NATO partners. I currently serve as the Chair of CI and Security in both entities, which requires a significant amount of resources as well. Additionally, it is difficult to lead CI and Security across the U.S. Government when there are insufficient directed resources for departments and agencies to follow NCSC guidelines.

QUESTION 9: What do you believe are the greatest challenges facing the NCSC?

I believe there are a few challenges which directly impact the enduring success of NCSC. First, it is hard to conduct effective and sustained outreach to Federal Partners, research labs, and the private sector. Although NCSC is building capacity for such outreach, the demand is immediate, technical, and comprehensive. Another significant obstacle is the inability to secure funding across the non-NIP funded departments and agencies, specifically for insider threat, Continuous Evaluation, supply chain risk management, and fundamental CI and Security assistance and training.

QUESTION 10: Is direct public sector outreach and threat warning contemplated in the current NCSC Strategic Plan? If not, why not?

Yes, direct public sector outreach and threat warning is in our current 2018-2022 *Strategic Plan*, and in our NCSC Mission Statement. NCSC closely coordinates with other IC agencies that also provide threat warning and have intelligence dissemination authorities. Our main mission partners in this arena are FBI and DHS. NCSC also works directly with Executive Branch agencies to ensure we share best practices in countering foreign and insider threats. We use our website and social media presence to raise awareness as well. Additionally, I have just hired a senior executive to serve as our director of communications and guide the execution of our strategic communications plan.

QUESTION 11: Would the objectives of the National CI Strategy be advanced by NCSC exercising a more direct role in communicating counterintelligence threats to the public?

Yes, the objectives of the National CI Strategy are advanced through a direct role in communicating foreign intelligence threats to the public, which is a key part of NCSC's statutory mission. In today's environment, it is more important than ever to communicate consistently with the American people, industry, and academia regarding foreign intelligence threats to our national and economic security. We are also aware that what we say in public to the American people is also heard by our adversaries, so it is a challenge to issue credible threat information without revealing too much. That said, a comprehensive and enduring narrative on foreign threats is important for transparency, to the extent we can adequately articulate the threats. Partnerships are critical in forming a consistent and sustained public narrative. In addition to FBI and DHS, the private sector has a role in attributing nation-state or criminal cyber actors publicly.

QUESTION 12: 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 for NCSC is stated in our *Strategic Plan*: To be our nation's premier source for counterintelligence and security expertise, and a trusted mission partner in protecting America

against foreign and other adversarial threats. To fulfill our vision, NCSC is currently focusing on the specific goals and underlying objectives and initiatives outlined in the *Strategic Plan*. However, as an adaptive organization, we review those priorities annually to ensure they reflect the current threat environment. I anticipate that our organization will continue evolving, and in five years, will be an even stronger voice for CI and security issues.

Following the stand-up of the Center in December 2014, we have truly achieved integration between the CI and security disciplines, and will continue to drive that model across the USG and our allied partners as a best practice. We will have domestic NCSC representatives around the country with strong links to state, local, tribal, and private sector partners. At the Federal level, NCSC will have formal, strong ties to mission partners who appreciate NCSC's unique role. NCSC will have the resources and budgetary authority to provide critically needed funding to non-IC partners at risk from foreign and other adversarial intelligence threats or the authorities to ensure that separately appropriated funds are properly aligned.

We currently spend a lot of time raising awareness of threats. I envision that in five years, we will be well past that stage, and able to provide focused, sustained leadership in key areas such as: protecting our economic security by mitigating theft of intellectual property and critical technologies; countering foreign influence operations by coordinating the activities conducted by our mission partners; hardening our critical infrastructure; harnessing and mitigating both the promise and risk posed by cutting edge technology available to both the U.S. and our adversaries; and putting personnel security and insider threat programs in place to ensure a trusted workforce.

QUESTION 13: What specific benchmarks should be used to assess the NCSC's performance?

NCSC uses many benchmarks to assess progress against the goals outlined in our *Strategic Plan*. One specific example is the impact of the guidance we promulgate. For instance, a Collection Emphasis Message we disseminated directly led to the FBI publishing 90 Intelligence Information Reports. Another benchmark is the specific actions we take to heighten awareness of, and to counter, threats to our supply chain and critical infrastructure, such as our recent briefing to State officials in preparation for the 2018 midterm elections. We track the growing number of fora where NCSC is either leading or heavily engaged, many of which are international. For example, I chair the NATO CI Panel and the Allied CI and Security Forum with our "Five Eyes" partners. NCSC's Center for Security Evaluation is a leading voice to build secure embassies and consulates overseas, and NCSC conducts countless private sector engagements through trade association groups to raise awareness and share best practices. We gauge the effectiveness of our governance by assessing the quality and quantity of engagement of the various boards we chair – the National CI Policy Board, the IC Security Directors' Board, and the CI Strategy Board.

To measure the health and welfare of NCSC internally, we can point to the successful recruitment of highly qualified CI and security officers to serve at 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 enhances expertise across the Center and allows for professional growth.

Counterintelligence Threats

QUESTION 14: What in your view are the most critical counterintelligence threats that are currently confronting the United States?

The U.S. 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 both gain sensitive U.S. information and thwart U.S. collection and operations. The three most critical CI threats cut across these threat actors: influence operations, critical infrastructure, and supply chain. 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. Advanced technology previously available mainly to leading nation-states is now increasingly available to a wide range of nation-state and non-state actors as well. For example, a growing set of threat actors are now capable of using cyber operations to remotely access traditional intelligence targets, as well as a broader set of U.S. targets including critical infrastructure and supply chains, often without attribution. Insider threats, sometimes with the encouragement of external actors, are a pernicious intelligence threat to our national security.

QUESTION 15: What would be your top priorities for the NCSC, in terms of the counterintelligence threats facing the United States?

Our top priorities include countering a range of persistent threats from intelligence actors spanning a spectrum of traditional spying, targeting of our critical infrastructure, economic espionage, cyber operations, and supply chain threats. Russia and China present global, well-resourced and technically sophisticated threats to all of these targets. However, regional and non-state actor intelligence operations are marked by increasing technical sophistication as well. Cyber operations are part of a new global "gray space" between peace and military conflict where international norms are in flux, and the protocols for countering and responding to these actions are still being established. Similarly, adversaries leverage supply chains as a threat vector to reach information technology systems and other processes or systems the supply chains support. Moreover, the U.S. government faces the difficult task of identifying insider threats before they inflict serious damage, as evinced in recent years. Another top priority is the strengthening of security safeguards for non-IC Federal Partners to enable them to effectively protect their personnel, systems, and data from hostile actors and cyber threats. Additionally, the "influence" paradigm, which cut across the greater U.S. Government, academia, media, and research and development, manifests itself in many forms and can cause insidious harm to our nation.

QUESTION 16: In your opinion, what counterintelligence threats, if any, have been overlooked or underestimated?

Technology and the capabilities of foreign intelligence threat actors have evolved so rapidly that we have underestimated certain threats. I will focus on two key examples. Until fairly recently, the efforts by China to use its intelligence services to advance its national development by undermining the economic security of the U.S. did not receive adequate attention. The U.S. has been slow in responding, in particular, to China's systematic theft of U.S. technology across broad swaths of the U.S. economy, which represents a critical national security threat.

Similarly, as a nation we underestimated Russia's intent to interfere in U.S. democratic processes and institutions. I assess that the Russian intelligence services will continue their efforts to disseminate false information via Russian state-controlled media and covert online personas to encourage anti-U.S. political views, create wedges that reduce trust and confidence in democratic processes, weaken U.S. partnerships with European allies, undermine Western sanctions, and counter efforts to bring Ukraine and other former Soviet republics into European institutions. I remain concerned that we may still be underestimating Russian capabilities and plans to influence the 2018 midterm and future elections. Furthermore, the Russians are not the only threat actor with the capability and intent for malign influence, yet that is where the focus has been. In my opinion, we also need to look at China and other adversaries' efforts to take a page from Russia's playbook.

QUESTION 17: Some agencies are very good at developing and training a cadre of counterintelligence experts; others seem to treat this discipline as an afterthought. Tell us how you have worked to develop a workforce of counterintelligence professionals at NCSC.

a. How have you encouraged each agency to do the same in-house?

Workforce development is a top priority for me at NCSC. Given the evolving nature of the intelligence threat, it is important that our workforce remains current so they have the expertise to lead the CI community. One effective strategy has been to bring in a healthy mix of detailees with recent experience working CI issues at their home agencies. To enhance our experience in-house, we have cataloged available training on CI issues, as well as key mission management skill sets such as leadership and resource management. Each employee has an Individual Development Plan and is allocated money within our budget to pursue professional development courses. Supervisors are held accountable for supporting their employee's development. We tie every employee's performance plan to the NCSC *Strategic Plan*.

To further professionalize the workforce across the community, my office, in partnership with the IC Chief Human Capital Office, issued the CI Competency Subdirectory to provide a common taxonomy for describing the job-specific capabilities of CI professionalism in the IC. These competencies serve as the basis for IC-wide and/or agency-specific qualifications, training,

career development, performance, promotion, and other standards applicable to CI professionals. This year NCSC led the IC-wide effort to develop training standards based on these competencies. In addition to training CI professionals, I advocate for cross-training other disciplines – such as acquisition, procurement, information assurance, cyber, legal, civil liberties and privacy, Inspectors General, and human resources – in CI so they better understand the intersections between their work and that of the CI community.

b. In your opinion, is the NCSC adequately staffed to address your priorities identified above?

When resources are constrained, one of the first functions to be considered for reduction is training. As the Director of NCSC, it is my role to advocate for the resource levels the community needs to be effective. Within NCSC, we have a small staff dedicated to workforce training matters. In the community-wide CI Training Work group we lead, we stress the importance of continuing to support employee education and training, and my staff is actively engaged in the resource process to ensure that funding for CI training priorities is adequate to meet the requirement.

QUESTION 18: The IC once thought of counterintelligence as being all about spy-versus-spy. Now, the "spy" could be a student in a STEM program or an IP address that appears to originate within the United States. With these aspects in mind, how are you scoping and prioritizing the counterintelligence mission?

The recently produced *National Threat Identification and Prioritization Assessment* (NTIPA), signed by the President in January 2018, provides the foundational guidance for the USG and the IC to scope and prioritize the CI threat landscape. For example, in the NTIPA, we characterize the activities of threat actors who are targeting our sensitive technology and research and development information using students, scientists, and corporate employees in addition to traditional intelligence operatives. Using the NTIPA as a blueprint, NCSC has developed the *Unifying Intelligence Strategy for Counterintelligence* and *Strategic Counterintelligence Priorities* papers for the individual threat actors, and our *Counterintelligence Production Guidance*. We also regularly examine our collection and analytic gaps. We develop collection strategies to address these gaps which are disseminated to the IC via *Collection Emphasis Messages*, and we also issue *Analytic Emphasis Messages*.

QUESTION 19: What in your view is the appropriate role of the NCSC in conducting direct informational outreach to U.S. national labs, universities, and private sector start-ups vis-a-vis is their appeal as high-value targets for economic espionage?

NCSC has a statutory responsibility to provide CI outreach to U.S. private sector entities at risk of foreign intelligence penetration, in addition to leading and supporting the USG's CI and security activities. We execute this responsibility through a variety of means, including direct engagement with entities such as the U.S. National Labs, universities, and private sector. We have ongoing initiatives, such as the "Know the Risk, Raise Your Shield" awareness campaign

and the cyber training series—both of which are available on our unclassified website. We also published the *Insider Threat Guide: A Compendium of Best Practices to Accompany the National Insider Threat Minimum Standard* that has been widely disseminated. We continue to expand our outreach through CI and Security working groups and conferences across all sectors of U.S. society.

QUESTION 20: Please describe the counterintelligence threat resulting from the presence of thousands of foreign nationals from adversary countries at our National Labs.

The nature of the CI threat to our National Labs has changed over the past decades. A growing list of state actors is increasingly exploiting the culture of openness and collaboration within the United States to acquire information on research and development and new technologies to advance their military capabilities, modernize their economies, and weaken U.S. global influence. The U.S. Government's CI and security resources are challenged by the presence of foreign nationals in the labs. But we also gain expertise, insight and valuable skills by maintaining our commitment to a transparent and open innovation ecosystem. The CI community's understanding of what an "intelligence collector" looks like has evolved, and we now understand that foreign adversaries are taking advantage of the access we've provided to legitimate, talented foreign scientists and academics.

Direct and discoverable ties to foreign intelligence and security services are harder and harder to discover, or don't initially exist at all. That is compounded by the collectors often being experts in fields, meaning they can identify the key pieces of information that will help their home country. Providing threat awareness information to the National Labs will assist them in making more informed decisions about how to improve security and CI awareness. NCSC works closely with the Department of Energy, the Department of Defense, and academia to facilitate robust training and threat awareness to the National Labs since they are a critical piece of the national security ecosystem.

QUESTION 21: In particular, China has a documented history of attempting to steal secret information from our National Labs, yet the United States continues to provide access to thousands of their nationals. Why?

The research community at large is committed to open science and research and does not necessarily think in terms of dual use technologies. Accordingly, they might not be aware of the national security implications of some research initiatives. The work being done at our National Labs ranges from basic, non-sensitive research, to our most prized weapons secrets. China, like other foreign countries, has a very talented academic and science base. As China becomes more capable, some of our National Labs have made great strides in partnership with Chinese nationals, for example, on the protection of nuclear materials. The United States' national and economic security has benefitted from those partnerships. NCSC partners with Department of Energy's Counterintelligence office to help understand, identify, and mitigate threats from Chinese nationals attempting to exploit our system. In addition, many of the consortiums that run the National Labs are affiliated with U.S. educational institutions. In accordance with their

educational policies, the agreements between those entities and the U.S. Government stipulate that researchers will not be discriminated against based on the country of origin.

QUESTION 22: What actions would you plan to take to ensure that each of your identified priorities is satisfied?

As the director of a national center, I use the mechanisms that NCSC has available to address my identified priorities. One mechanism is the governance structures we have in place to promote collaboration and cooperation on critical strategic CI and security issues, such as the National Counterintelligence Policy Board, the IC Security Director's Board, the Security Executive Agent Advisory Committee, and the CI Strategy Board. In addition, NCSC regularly uses regional and functional communities of practice to identify, assess, and coordinate community-wide actions, and we issue guidance to collectors and analysts across the community to ensure high-priority CI and security issues and intelligence gaps are addressed in a timely manner. Another mechanism is my mandate to advise the DNI on IC programs and budgets that support national CI and security priorities, and recommend adjustments as necessary to meet priorities established by NCSC. Finally, I have found it useful to take full advantage of my position as the Director of NCSC to raise awareness, champion our concerns, and convene the right stakeholders to take action.

Congressional Oversight

QUESTION 23: 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 to '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 supp ort of the DNI, to keep the congressional intelligence committees fully and currently informed about matters relating to compliance with the Constitution and laws?

It is critical, to maintain the trust of the American people, that the IC fully comply with the Constitution and the laws of the United States.

In addition to the requirements to ensure national intelligence is provided to the Senate and House of Representatives and committees thereof under Section 102A, the DNI is also responsible under Section 502 of the Act to keep the congressional intelligence committees fully and currently informed of all U.S. intelligence activities. Such intelligence activities include "significant anticipated intelligence activities," and "significant intelligence failures."

The Director of NCSC, together with the DNI, likewise has an obligation to keep the

congressional intelligence committees abreast of all U.S. intelligence activities, and is responsible for fully complying with all IC directives related to the disclosure of information to Congress.

Furnishing information to the oversight committees is vital to Congress' role in considering legislation, determining the appropriate level of resources for NCSC, assessing the effectiveness of the Center, and gaining a better understanding of counterintelligence and security issues. If confirmed, I will remain committed to ensuring that the NCSC workforce understands the importance of congressional oversight, provides thorough and timely information to Congress, and is responsive to congressional queries.

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 National Intelligence Program (NIP) budget. The Director of NCSC is charged with providing such information as the DNI requests for determining the NIP budget. Additionally, under the Counterintelligence Enhancement Act of 2002, the Director of the NCSC, in coordination with the DNI, is responsible for coordinating the development of budgets and resource allocation plans for counterintelligence programs and activities, as well as ensuring that the budget and resource allocation plans address counterintelligence objectives and priorities.

Intelligence Community Counterintelligence Offices and Reforms

QUESTION 24: Please describe your authorities over the counterintelligence offices within the IC.

a. 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 foreign intelligence entities 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, I regularly work with the ODNI to assess whether adjustments to NCSC authorities to clarify its mission and functions are needed. I will notify Congress if NCSC identifies a need for changes to the Center's authorities.

b. How do you coordinate and deconflict with these other IC offices?

As the National Intelligence Manager for CI, we support national-level decision making by leading integrated analysis, collection, and CI initiatives to counter foreign intelligence threats. NCSC integrates CI across the IC through strategic prioritization, coordination, and deconfliction

of CI analysis, collection, and resources to address priority intelligence gaps and CI mission needs across the IC. The CI Strategy Board and various working groups and conferences serve as fora where the IC prioritizes, deconflicts, and aligns CI activities and initiatives to address priority threats and gaps. The National CI Policy Board and IC Security Director's Board are also key to helping coordinate and deconflict across the IC. These boards meet regularly and my interaction with the heads of the CI and security entities is persistent and steeped in trust and partnership.

QUESTION 25: NCSC is an organization with sweeping responsibilities but little by way of enforcement capability.

a. What tools does NCSC have to prompt IC agencies to move ahead with what may sometimes be challenging but necessary counterintelligence precautions?

Based on IC policy and directives and its statutory authorities, NCSC uses the following tools to lead and prompt the CI community:

- Strategy, Policy, Standards, and Guidance: Examples include the *National Threat Identification and Prioritization Assessment*; the *National CI Strategy*; national CI priorities for analysis, collection, and operations; Intelligence Community Directives and Standards; and NCSC contributions to legislation, Executive Orders, and Presidential Directives.
- Chairmanship of the National Counterintelligence Policy Board: NCSC convenes senior Executive Branch CI officials to drive decision making and ensure accountability on key CI issues.
- Mission Reviews: NCSC conducts annual Mission Reviews and other assessments to evaluate the IC's implementation of the *National CI Strategy*. For operational matters, this includes the annual *National Assessment of the Effectiveness of U.S. Offensive Counterintelligence Operations*, which evaluates the operational implementation of the strategy.
- Resource Advocacy: NCSC uses documents like the *National CI Strategy* and *Unifying Intelligence Strategy*, as well as *IC Major Issue Studies* and the *Consolidated Intelligence Guidance*, to communicate CI and security priorities to the IC. Using these priorities as a guide, NCSC advocates for IC element CI and security resource requests through the established budget process.

b. Are these tools sufficient to accomplish your mission?

While the NCSC can tout successes across our Center's mission areas, there are certainly challenges in enabling the IC to maximize CI capabilities towards efficient IC and whole-of-government CI support to national strategies and priorities. One specific issue is the inability for some non-NIP funded agencies outside the IC, who constitute our "soft underbelly," to properly resource their CI and security programs.

c. How might Congress and the DNI give the NCSC more authority to prompt action within the IC?

The United States faces daunting threats from foreign intelligence entities 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 counterintelligence activities across the United States Government, and greater outreach efforts to engage and disrupt FIE threats. The governance mechanisms in place now are effective and NCSC is viewed within the IC as a leader on CI and security matters.

QUESTION 26: What do you see as the most important outstanding priorities in the intelligence reform effort, as it relates to counterintelligence?

In the post-9/11 Commission Report era, one of the most important intelligence reform efforts has been increased intelligence information sharing. Within the CI discipline, which seeks to detect and deter a myriad of foreign intelligence activities against the U.S., that effort is equally as vital. By sensibly and responsibly reducing the restrictions placed on sharing sensitive data, the IC will improve its ability to collect against, analyze, and warn of important CI-related developments.

NCSC Analysis

QUESTION 27: What unique role does NCSC's strategic counterintelligence analysis play, as compared to the analysis produced by other IC components?

The Counterintelligence Enhancement Act of 2002 calls on the Director of NCSC, "in consultation with appropriate elements of the United States Government, to oversee and coordinate the production of strategic analyses of counterintelligence matters." Consistent with this authority, NCSC provides analytic production guidance to the CI analytic community that prioritizes foreign intelligence threats and identifies Key Intelligence Questions. These questions help focus limited CI analytic resources on the most important developments and trends relating to foreign intelligence entities. NCSC recently published the 2018-2019 *Counterintelligence Production Guidance* in collaboration with CI analytic elements throughout the Intelligence Community. In addition to analytic guidance, my office also produces CI risk assessments that integrate IC-coordinated threat information, vulnerability data, and mitigation strategies to assess specific CI risks to the U.S. Since many of these threats also impact our allied partners, we produce releasable versions of these products as well.

In 2014, as Director of NCSC, I advocated successfully for the establishment of the National Intelligence Officer for Counterintelligence (NIO/CI) at the National Intelligence Council. The creation of this position remedied the absence of IC-coordinated strategic CI analysis being provided to national policymakers in the Executive and Legislative branches. Since 2014, the NIO/CI in collaboration with NCSC and the CI analytic community has produced a vast range of

strategic CI analytic products that provide analytic insights on priority foreign intelligence threats. These products differ from analysis produced by other IC components in terms of analytic scope and policy impact. Also, they are estimative in nature, and are IC-coordinated representing the view of the entire CI analytic community.

QUESTION 28: What is the NCSC's role in coordinating and publishing the IC's counterintelligence assessments?

NCSC produces a range of unique risk and mission assessments for the CI community. These include the *National Threat Identification and Prioritization Assessment*, the *Foreign Economic Espionage in Cyberspace* report, and the *Counterintelligence Production Guidance*. In our role as CI mission manager, we also produce mission assessments that support collection and analytic emphasis messages to highlight high priority intelligence needs on select topics. NCSC contributes to and coordinates on CI assessments produced by other IC elements and the National Intelligence Council. The subject matter expertise that resides in NCSC's various directorates – to include supply chain risk management, technical CI threats, cyber, and the cadre of National CI Officers that support regional and functional National Intelligence Managers – serves as an important voice in the CI community's review and coordination processes.

State and Local Governments

QUESTION 29: What is the NCSC's role in producing and disseminating intelligence for state, local and tribal partners, including information as it relates to insider threats?

NCSC has a national-level role to support the flow of strategic CI and security threat assessments and mitigation strategies to state, local, and tribal partners. Foreign adversaries have demonstrated intent and capability to threaten U.S. interests at every level of our society, and state, local, and tribal partners are stakeholders and mission partners who play a vital role in identifying and mitigating CI and security threats. In the context of threats to U.S. critical infrastructure, for example, NCSC partnered with the Federal Energy Regulatory Commission, the Department of Energy, and the FBI to provide one-time access to classified information to state and local regulators to raise their threat awareness. We discussed threat actors and IC assessments as well as provided information on mitigating insider threats. In February 2018, NCSC worked with other elements of ODNI, DHS, and the FBI to provide one-time Secret level classified briefings to more than 100 Secretaries of State and state election officials from all 50 states. These threat briefings resulted in greater threat awareness on the part of the states, improved IC understanding of the needs of states, and served as the impetus to improve IC support to states to help defend against threats to the 2018 elections.

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

As a mission manager, NCSC is most often not the producer of finished intelligence products on threats, but rather provides strategic threat awareness information and collection and analytic guidance to Federal, state, and local partners. In contrast, the FBI and DHS are often best positioned to provide tactical threat information and warning to state, local, and tribal entities since they have well-established dissemination mechanisms.

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

Engagement among NCSC, FBI, and DHS is productive, collaborative, continuous, and broadens every day. As I have noted, NCSC is in the unique position, backed by statutory authority, to successfully integrate the IC and other Federal partners as well as state, local, and tribal partners to detect, understand, deter, disrupt, and defend against CI threats from foreign adversaries and insiders.

c. What priority have you assigned to this issue, and what priority do you plan to give this issue going forward?

Interacting with state, local, and tribal governments is one of NCSC's highest priorities. NCSC has detailees from the FBI and DHS to ensure we are providing the best service to the nation and leveraging authorities to best inform our state, local, and tribal partners. NCSC is deliberative in ensuring our products and publications can be shared with the broadest audience possible, including writing products at lower classifications based on the intended consumer. Furthermore, if we are able to establish Domestic NCSC Representatives, they will serve as an excellent conduit to enhance information sharing with our state, local, and tribal partners. We have requested that DHS send a detailee to NCSC to enhance our partnership in the critical infrastructure arena.

National Intelligence Manager for Counterintelligence

As the National Intelligence Manager for Counterintelligence (NIM-CI), the Director of the NCSC coordinates counterintelligence efforts to integrate collection and analytic priorities.

QUESTION 30: What is your vision of the Director of the NCSC in the role of mission manager?

As mission manager for the CI and Security community, my vision is for NCSC to lead innovative CI and security solutions, further integrate CI and security disciplines into IC business practices, and adequately resource such efforts. To do this, we will drive integrated CI activities to anticipate and advance our understanding of evolving FIE threats and U.S. security vulnerabilities. We will develop and implement 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 will 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 accomplishing these things, my goal is to create a more proactive CI and security posture in the U.S., employing all instruments of national power to prevent regional and emerging threat actors from gaining leverage over the U.S.

QUESTION 31: What is the Director of the NCSC's role in developing the National Intelligence Priorities Framework (NIPF) with regard to counterintelligence?

The Director of NCSC, through the NIPF Intelligence Topic Expert for Counterintelligence, who is an NCSC officer, guides the U.S. Government's efforts in the prioritization of collection and analysis on hostile FIEs intent on harming the United States. To collaboratively develop these priorities, NCSC, in September 2017, chaired the NIPF Focus Group on Counterintelligence. This group consisted of over 40 representatives from more than 30 agencies and departments, including CIA, DIA, FBI, NGA, NSA, and the State Department. Past NIPF changes in priority advocated by NCSC have positively shifted analysis and collection to ensure we remain focused on our highest priorities.

QUESTION 32: What is the Director of the NCSC's role in providing guidance on resource allocation with regard to particular counterintelligence capabilities and platforms?

I provide guidance on resource allocation regarding counterintelligence capabilities and platforms by developing strategic CI objectives within the *National Counterintelligence Strategy*. I also communicate CI and security priorities and guidance through the *Consolidated Intelligence Guidance*. In addition, I work within established budgetary processes to impact changes required to address CI and Security priorities in the National Intelligence Program and evaluate IC program resource allocations against *National Counterintelligence Strategy* objectives. A recent example is our successful advocacy for funding for the CITADEL program, which will position the community to collect information on CI threat actors to better mitigate threats posed to the USG.

QUESTION 33: What is the Director of the NCSC's role in providing guidance with regard to the allocation of resources among and within IC elements?

I provide guidance on the allocation of CI and security through the Intelligence, Planning Programming, Budgeting, and Evaluation process. I also advocate directly to the IC CFO and ODNI for resources across the CI and security mission space and evaluate whether IC programs are meeting their expected accomplishments. My resource allocation recommendations are informed by NCSC's annual Mission Reviews and through direct interaction with IC elements and DNI leadership.

QUESTION 34: Given resource constraints, how should the Director of the NCSC identify unnecessary or less critical programs and seek to reallocate funding?

I identify 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, I participate in the entire budget process and routinely make recommendations on strategic CI and security resource priorities, evaluate IC program requests, advocate for CI and security resources, and make recommendations on resource alignments.

While I do not have direct control over funds reallocation, I effectively communicate CI and security-related priorities through documents such as the *National Threat Identification and Prioritization Assessment*, the President's *National CI Strategy*, *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. Also, to actively shape the resource environment, NCSC routinely reviews and recommends CI and security-related resource requests as part of the budget process.

QUESTION 35: What are the most important counterintelligence gaps or shortfalls across the IC?

The IC and U.S. Government are facing important CI and security challenges today that affect our ability to perform critical mission objectives and effectively drive protection of our national security. To address these gaps, the IC must:

- Develop innovative solutions to discover, access, and exploit disparate and large data sets so the IC can use the information to enable warning and develop an agile CI and security posture.
- Advance its capabilities through the development of new, improved tradecraft, technical solutions, security clearance reform efforts, and enhanced information security. The IC must use the full spectrum of its capabilities and knowledge to deter and disrupt threats posed by foreign adversaries and insiders.
- Continue to develop and retain a highly skilled, technically proficient workforce with expertise, for example, in information technology, data science, and telecommunications, in order to develop offensive as well as defensive strategies.
- Develop an improved capacity to provide threat and warning to state, local, and tribal entities, as well as the private sector, so we are better able to connect CI and security threat information with vulnerability data to improve our understanding of and ability to mitigate risks to the U.S.

Insider Threats and Unauthorized Disclosures

QUESTION 36: What is the role of the NCSC in preventing and penalizing those who pose an insider threat to our classified intelligence information?

Executive Order 13587 established the National Insider Threat Task Force (NITTF) to assist in the development of an executive branch-wide national insider threat program. The Task Force is co-chaired by the DNI and the Attorney General, with day-to-day leadership from NCSC and the FBI. The NITTF developed the National Policy and Minimum Standards to set the basic elements necessary to establish insider threat programs, provide technical and programmatic assistance to approximately 100 departments and agencies, conduct training, disseminate best practices, and champion the push to professionalize the insider threat workforce.

The Task Force is working with DOD to extend the national program to the 13,000 facilities in the cleared defense contractor community. Finally, the NITTF is conducting independent assessments of department and agency insider threat programs to gauge their implementation of the Minimum Standards, and actively developing a model to advance programs beyond the minimum and make them more effective. The goal is not to catch malicious insiders after the compromise, but rather to proactively engage the workforce and build comprehensive and effective programs that preempt the compromise of classified information. If that fails, FBI and DOJ have the lead for investigating and imposing penalties for criminal action.

QUESTION 37: How does the NCSC work with the FBI's National Insider Threat Task Force (NITTF) to deter, detect, and mitigate insider threats?

The NITTF is co-chaired by the DNI and the Attorney General, with day-to-day leadership from NCSC and the FBI. Staffing currently comes from the NCSC, FBI, the Office of the Undersecretary of Defense for Intelligence, DIA, CIA, and the Transportation Security Administration. Agency representation is dynamic, and in the past, NSA, DOE, and others have provided their unique agency perspectives to the Task Force. The NITTF also leverages relationships with programs from the IC, DOD, and Federal Partners to champion issues of common concern and lead community working groups. Through these efforts, the NITTF works to train and assist Executive Branch departments and agencies to professionally handle insider threat matters, and, when appropriate, refers the matter to the FBI for further investigation in a manner that promotes a successful outcome.

QUESTION 38: In 2015, you were asked whether NCSC had identified OPM's security clearance database as a counterintelligence vulnerability. You responded that "[t]he statutory authorities of the National Counterintelligence Executive, which is part of NCSC, do not include either identifying information technology (IT) vulnerabilities to agencies or providing recommendations to

them on how to secure their IT systems." However, the NCSC Strategic Plan for 2016-2020 emphasizes the integration of counterintelligence with security, including the protection of networks. Please explain how you would implement that integration in terms of:

a. Assessing where government cybersecurity vulnerabilities create the greatest counterintelligence risks;

NCSC works with the IC and USG cyber community to provide the CI and security perspective on foreign adversarial cyber capabilities, intent, and attribution. We do not identify specific vulnerabilities or make targeted mitigation recommendations; rather we raise awareness of cybersecurity vulnerabilities and the impact of potential compromise or exploitation. One concrete example of this partnership is the IC Security Coordination Center, or SCC, which was a joint development effort between the IC CIO and NCSC. As part of the IC's approach to integrated risk reduction and a community-wide consolidated security risk posture, the ICC SCC operates one of the USG's seven Federal Cyber-Security Centers. It contains a fully integrated CI and Security Cell that works hand-in-hand with Information Assurance and Computer Network Defense professionals analyzing cyber security threat trends and network vulnerabilities, to include zero days, and produces warning and vulnerability mitigation reports called "Tippers" that are shared across the USG Cybersecurity Center network.

The Deputy Director for the IC SCC is a senior CI professional from NCSC whose function is to integrate into the Center such CI functions as supply chain risk management, cyber threat and vulnerability analysis, insider threat monitoring and analysis, and CI and related security liaison reach back. Plans are currently underway with the IC CIO to build greater combined capabilities in the areas of cyber security threat trends, vulnerability awareness, cyber "indications and warning," threat reporting and information sharing capabilities. Our National Counterintelligence Officer for Cyber works with the Cyber Threat Intelligence Integration Center (CTIIC) to infuse CI into CTIIC's analysis.

b. Recommending mitigation strategies; and

The IC SCC has collaborated across the USG to track known network vulnerabilities and mitigation status, such as (1) the "Heartbleed" zero day a couple of years ago and (2) more recently, the widely used web software "Apache Struts" zero day that was used to exploit Equifax and potentially could have impacted multiple USG departments and agencies. These are examples of how, through the IC SCC, we seek to help organizations understand known vulnerabilities and emerging threat trends so they can harden their network systems. We also believe that hardening the human operating system—your network users—through education and awareness is just as important.

To that end, NCSC developed a comprehensive cyber-CI awareness program called "Know the Risk, Raise Your Shield," which provides the USG, private sector, and the American public with cyber security awareness tips, cyber security hygiene tips, and educational videos on the basics and the interrelationship of counterintelligence, insider threat and supply chain risk

management.

c. Conducting damage assessments following any breaches.

NCSC, as directed by the DNI, leads and coordinates CI damage assessments to evaluate actual or potential damage to national security as a result of unauthorized disclosure of classified information. The CI concern is what our adversaries learn about our capabilities when sources and methods are publicly disclosed.

QUESTION 39: Intelligence Community Directive (ICD) 704 states: "Heads of IC Elements or designees may determine that it is in the national interest to authorize temporary access to SCI and other controlled access program information, subject to the following requirements - temporary access approvals shall be granted only during national emergencies, hostilities involving United States personnel, or in exceptional circumstances when official functions must be performed, pursuant to EO 12968. Temporary access approvals shall remain valid until the emergency(ies), hostilities, or exceptional circumstances have abated or the access is rescinded. In any case, temporary access shall not exceed one year." ICD 704 further states that "the DNI retains the authority in any case to make a determination granting or denying access to [SCI] information."

Are there any political appointees or other personnel in the Executive Office of the President who have been granted temporary access to SCI or other controlled access program information? If yes, please respond to the following:

ODNI does not routinely conduct individual access determinations, but instead establishes uniform standards and procedures for the grant of access to SCI and ensures the consistent implementation of those standards. Intelligence Community Directive 704 provides consistency in granting secure compartmented information access to the IC, but does not apply outside of the IC. Under Executive Order 12968, where official functions must be performed, temporary eligibility for access to classified information may be granted. While the DNI has oversight responsibilities of personnel security programs, agency heads are responsible for establishing and maintaining an effective program to ensure that access to classified information by personnel is clearly consistent with the interest of national security.

If yes, please respond to the following:

a. Has the DNI reviewed these cases?

See prior answer.

b. Has the DNI recommended in any of these cases that this access be denied?

See prior answer.

c. Which of the above requirements listed in ICD 704 have provided the basis for the temporary access?

See prior answer.

d. Has a temporary access been extended beyond a year?

See prior answer.

e. Who is responsible for managing these temporary accesses?

See prior answer.

QUESTION 40: What is your plan to ensure success in preventing and penalizing insider threats and unauthorized disclosures?

IC employees who misuse their access to intelligence information not only violate law and/or policy, they violate the public's trust and degrade the public's confidence in the integrity of the IC as a whole. Further, with today's technological capability for rapidly moving massive volumes of data from information systems, it is imperative that we have safeguards in place to detect such nefarious activity as close to near real time as possible.

An insider threat program is designed to focus on the central issue of human behavior: to proactively detect behavior of concern either in the physical or virtual world, place it in context, determine if a risk, threat, or vulnerability exists, and if it does, energize the appropriate agency elements to resolve the matter and mitigate the risk. Part of the solution is auditing and monitoring user activity programs in place across the IC. These are a critical piece because of the confidence we gain in knowing what is happening to information we share. Coupled with information from numerous parts of an organization—such as travel records, human resources, personnel security and data from Continuous Evaluation—these programs can develop a comprehensive view of anomalous activity and take proactive measures. Another key component is education of the workforce to instill a culture of awareness. When properly trained on insider threat indicators and reporting procedures, the workforce can become a force multiplier. NITTF assessments have shown that those departments and agencies with sound workforce and stakeholder engagement demonstrate the ability to identify not only threats to national security, but also threats to our people and mission resources. We plan to continue our ongoing public and USG awareness program about the damage caused by unauthorized disclosures that was initiated by the National Security Advisor last fall.

Acquisition and Supply Chain Risk Management

As you know, there have been recent incidents of supply chain intrusion in the U.S. government by contractors and vendors with foreign actor ties that went unnoticed - or, at least, not acted upon - by the IC.

QUESTION 41: What is the role of the NCSC in preventing and mitigating foreign state and nonstate actors from compromising the supply chains upon which the U.S. government relies for its products and services?

Impetus for securing our critical supply chains has grown in recent years given the mounting evidence that our adversaries are using our supply chain to cause us harm. This is a difficult challenge given the disparate players involved—CI, security, acquisition, procurement, information technology (IT), facilities and logistics, contracts, legal, civil liberties and privacy—with no real lead. NCSC's role has been foundational in this regard. We lead the IC in setting policy and standards to improve supply chain risk management (SCRM), creating a shared repository for SCRM-related assessments, raising awareness of supply chain risk across the USG and private sector, and advocating for the inclusion of supply chain risk into national-level decision-making processes and strategies. Specifically, in 2013, we established the first DNI policy addressing supply chain risk management.

Last year, I issued the policy standard, *Supply Chain Information Sharing*, which resolved a decade-long requirement to better share information to protect and defend our supply chains. NCSC participates in the Enduring Security Framework, a public-private partnership between the USG and key IT and Defense Industrial Base companies organized under DHS's authorities. NCSC partnered with the Federal Communications Commission to brief telecommunications representatives, and with the Federal Energy Regulatory Commission, to brief the energy sector on mitigating supply chain risk. NCSC successfully advocated for the inclusion of supply chain risk in the *National Security Strategy*, the *National CI Strategy*, and Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*.

QUESTION 42: What is your plan to increase the NCSC's success in preventing and mitigating foreign state and nonstate actors from compromising the supply chains upon which the U.S. government relies for its products and services? How do you measure and define "success" in this context?

NCSC's *Strategic Plan* delineates my approach to preventing and mitigating compromises to our critical supply chains. We plan to continue our whole-of-government approach by raising awareness about supply chain risk, fostering partnerships in the public and private sectors, and strengthening the exchange of threat and vulnerability assessments with mission partners. We share best practices and provide guidance on establishing and maturing SCRM programs, and advocate for the necessary resources.

I measure success by the foundational processes we establish and promulgate throughout the IC, by the continued recognition of this threat at the national level, and by the documented improvements made by individual IC elements. A recent example of a success is DHS's Binding Operational Directive requiring all federal agencies to identify the use or presence of Kaspersky Labs products and provide a plan of action to remove and discontinue present and future use. As stated in the DHS press release, "[t]he risk that the Russian government, whether acting on its own or in collaboration with Kaspersky, could capitalize on access provided by Kaspersky products to compromise federal information and information systems directly implicates U.S. national security."

QUESTION 43: Does NCSC conduct damage assessments relative to the licit and illicit acquisition of U.S. sensitive and advanced technology by foreign actors, to include nontraditional intelligence collectors?

Damage assessments are used to evaluate actual or potential damage to national security resulting in the unauthorized disclosure of compromise of classified national intelligence. NCSC oversees formal damage assessments and leads, when charged to do so by the DNI, or facilitates CI damage assessment teams when the unauthorized disclosure or compromise involves classified national intelligence affecting more than one IC element or USG department or agency. In the case of licit and illicit acquisition of U.S. sensitive and advanced technology at cleared defense contractors, DSS would have the lead.

QUESTION 44: 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?

Building CI threat awareness across government and our public and private sector partners must be permanent and enduring, and this is especially true regarding science and technology (S&T) partnerships. Put simply, we are going to have to make smarter, and sometimes difficult, decisions about who we partner with, and what the terms of those partnership are. This is in many ways a policy question, but the CI community's role is to highlight known vulnerabilities in our S&T infrastructure, and help identify and share best practices for security and CI awareness. We also need to be sure our partners know who to call when they identify a problem, and that we are responding to those needs effectively. Finally, we have many partners conducting outreach and briefings, and there is a leadership and coordination role for NCSC to play in making sure that those outreach materials and briefings are consistent and informative.

NCSC also has a role as a mission integrator. There are many excellent efforts already taking place from individual CI and security elements around the government, but we are up against actors that are incredibly organized and focused. Our response has to be organized and focused too, and NCSC has a role in identifying the wide variety of tools, authorities, and partners across government that should be connected to provide much more comprehensive protection for our most vital technologies and capabilities. Using our leadership of the NATO CI

Panel and the Allied Security and Counterintelligence Forum, we also need to exchange best practices with allied partners.

NCSC Personnel and Resources

QUESTION 45: Do you believe that the 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.

If confirmed, I will continuously evaluate NCSC's personnel and resource levels to ensure we are staffed to provide CI and security leadership and support to the U.S. Government, conduct CI outreach to appropriate U.S. private sector entities, and issue public warnings regarding intelligence threats to the U.S. We have recently established an NCSC Annual Planning Cycle which focuses our senior leadership team meetings on NCSC's goals, initiatives, resources, and staffing. We do this with robust input from our workforce.

We have to ensure our workforce is prepared to accomplish NCSC's growing mission requirements, especially in the areas of security clearance reform; leading, with the FBI, Executive Branch efforts to build insider threat programs; and developing national CI and Security policy to identify gaps, recommend priorities, and inform and shape resource decisions. I will utilize the ODNI planning and budgeting process to ensure NCSC has the technically trained and experienced personnel and resources to meet mission requirements. As those requirements continue to grow, I will reevaluate our staffing levels to minimize degradation to mission accomplishment.

QUESTION 46: Does the NCSC currently employ contractors?

a. If so, what is the numerical ratio of contractors to government employees?

Yes, NCSC relies on the technical skills and talents of contractors to augment those of our government staff. Currently contractors comprise 43 percent of our workforce.

b. What are NCSC's plans for employing contractors in the future, and what is the basis for those plans?

Contract personnel are part of an integrated team of professionals who bring remarkable, often rare, expertise. They support U.S. Government personnel in performing mission and mission support activities. They are an excellent source of highly qualified experts, and often provide a level of technical depth not found in government. Additionally, contracting staff can help provide surge support to tackle emerging needs as we engage in the slower (but necessary) process of workforce transformation. The staffing mix NCSC currently employs provides the right balance between cadre, detailees, and contractors to ensure NCSC is optimally postured.

Professional Experience

QUESTION 47: Please describe specifically how your experiences have enabled you to serve as the Director of the NCSC, and how these experiences would enable you to serve effectively in the future.

In serving as the Director of NCSC for more than three years, I have been fortunate to lead amazing women and men from multiple missions and cultures to accomplish critical national security objectives. My leadership and motivation skills developed over three decades of government service enable me to effectively lead and manage a diverse workforce, leverage individual and collective skill sets, and facilitate a high performing workplace where talented government employees and contractors want to work. My 21 years of experience in the FBI has placed me in numerous high stress operations, with high stake outcomes, and precarious situations, which result in a portfolio of deep and broad experience to draw upon when significant national security events and serious personnel situations arise.

My substantial experience serving as the Chair for CI and Security for our integral "Five Eyes" and NATO partners has enabled me to drive an enhanced footprint and impact on our partners, and at the same time develop new and enduring relationships with CI and Security leaders from those countries which fosters trust and enhanced collaboration. In the same context, I have built extensive trust and partnership, not only with senior leaders of CI and Security within the IC and the Federal Partner entities, but also with chief executives, information officers, and security officers from key private industry sectors critical to national security missions.

Over the past three years, I have successfully engaged with senior level leadership and policymakers in the National Security Council and developed a keen insight into the critical interlocking of intelligence and policy development. Additionally, I have successfully conducted numerous briefings and provided extensive testimony to this and other congressional committees, individual Members, and congressional staff on a broad array of CI and security issues. With such experience, I have gained an enhanced appreciation of the critical role of oversight, and the constructive relationships required to effectively enhance the CI and security mission.

The above experiences and leadership qualifications provide me a solid platform, if confirmed, to lead NCSC to the next level as a national center. In today's complex and persistent threat environment, our national security is dependent, not only upon our capabilities, but also on strong and experienced leadership to lead our dedicated women and men. I believe, if confirmed, I can continue to enhance the NCSC vision of being the nation's premier source for counterintelligence and security expertise.

May 17, 2016

Questions for the Record, Senate Select Committee on Intelligence, Confirmation Hearing for the Director, National Counterintelligence and Security Center, Designate, William Evanina, May 15, 2018

Sen. Heinrich question (posed during testimony)

QUESTION 1: Are we getting Utility leadership through the clearance process fast enough? (Page-18 of testimony transcript)

(U//FOUO) The Department of Homeland Security (DHS) is working expeditiously to increase the speed and number of security clearances processed for the leadership of Utility and other critical infrastructure sectors. Per DHS, the clearance process through-put has significantly increased in CY2018, specifically to support the protection of the DHS infrastructure mission. We have also made use of the authority to grant one-time access to classified information to provide threat briefings to the Energy Sector in the absence of a final clearance.

Sen. Cornyn questions (email Tuesday 15May2018-1053)

China: Last July, then-CIA Director Pompeo suggested in an interview that China represents the greatest potential long-term threat to our national security, greater than Russia or Iran. I agree with him; in fact, I believe China presents a threat unlike anything the U.S. has ever faced – an extremely powerful economy protected by state-driven industrial policies that undermine the free market, married up with an aggressive military modernization and an apparent intent to dominate its own region and potentially beyond. And, of course, it is ruled by a Communist dictatorship that has a very different set of values than we do.

QUESTION 2: How serious of a long-term national security challenge to you consider China to be, and how would you rank it compared to the threats posted by Russia, Iran, North Korea, or terrorism?

(U//FOUO) China and Russia pose the most serious intelligence threats to our national security due to their growing capabilities and intent to harm US interests. The threat posed by China, in particular, to our long-term national security is formidable. China's theft of intellectual property -- ranging from stolen drought-resistant corn seed formulas to pharmaceuticals to jet engine technology -- is resulting in billions of dollars of economic loss for the United States and is eroding our military advantage in key areas. Another reason this threat is so serious is China's use of traditional and non-traditional collectors to acquire U.S. information, technology, and expertise from the U.S. Government, academic institutions, and the private sector -- which is very difficult to detect and counter.

QUESTION 3: Do you consider China to have a comprehensive strategy to facilitate the transfer of U.S. technology and knowledge from U.S. entities back to China?

(U//FOUO) China has multiple strategies that either elicit or facilitate the transfer of U.S. technology, intellectual property, research, and knowledge from U.S. and other Western nations. These strategies are contained in a number of comprehensive national development plans, including China's well-known Five Year plans, the National Medium and Long-Term Development Plan, and Made in China 2025. China is able to acquire and transfer critical U.S. technology through their intelligence services, foreign direct investment, joint ventures, the Chinese Talent plans, open-source science and technology acquisition programs, academic and scientific collaborations, non-traditional collectors, and front companies. Such technology transfer is also facilitated by China's laws and regulations, which allow access to sensitive or proprietary foreign company information. For example, the new China Cyber Security law requires Chinese information and communication technology companies to provide Chinese intelligence and security services access to information that transits Chinese networks

QUESTION 4: Would you explain what types of recruitment programs China utilizes, such as the so-called Thousand Talents program, and what national security concerns these might raise?

(U//FOUO) The Chinese Talent Program is a critical element of China's national strategy to strengthen its economy and national security, primarily by recruiting individuals to acquire foreign technology and knowledge. The Talent Program includes various recruitment plans, all of which are managed by the Central Committee of the Communist Party of China through its Organization Department. The United States has lost significant intellectual property because of the Talent Program, and appears to have indirectly facilitated and funded China's recent economic transformation by funding U.S.- based Talent Program recruits. The Chinese Government has transferred advanced technology and basic research from the United States and other Western nations by paying scientists, engineers, and other professionals to bring research and technology with them to China through programs run by China's Communist Party. These recruits have influenced the type of research undertaken in Western countries to help the Chinese Government attain key military and economic objectives. This has helped fuel China's unprecedented growth at the expense of U.S. and Western academic, business, and government interests.

QUESTION 5: Recognizing that you're an FBI agent and not an immigration expert, how well do you believe that our current visa policies on China are serving our national security interests?

(U//FOUO) China exploits seams in our policies and laws -- to include U.S. visa and immigration policies -- to send students, scientists, engineers, and business people to the United States to acquire sensitive R&D information and technological know-how in support of China's economic and military development goals. We work closely with U.S. policymakers to review U.S. counterespionage laws and other legal, policy, and regulatory frameworks that support the CI mission and inform them of CI risks inherent in the changing threat landscape.

QUESTION 6: How does China use so-called "non-traditional collectors" to gather commercial and technological intelligence from the U.S.?

(U//FOUO) Non-traditional collectors are individuals from the academic or business communities, who are able to collect data on behalf of their governments through their daily work activities. Through their placement and access in U.S. government institutions, colleges and universities, and technology companies, in particular, they are able to steal intellectual property, proprietary information, and other sensitive data to benefit China's military, state-owned enterprises, and other businesses.

CFIUS: Venture capital and joint venture investments are not currently reviewable by the Committee on Foreign Investment in the United States (CFIUS).

QUESTION 7. What role are these types of transactions playing in foreign acquisition of advanced and sensitive U.S. technologies, and how important is it that we plug these gaps?

(U//FOUO) The foreign investment landscape has changed significantly over the last several years, with non-controlling investments, including venture capital investments, and joint ventures becoming more prominent methods used for technology acquisition. Many cutting-edge technologies being developed for commercial uses also have the potential to be applied to military end-uses. For this reason, foreign investment in a start-up may raise just as serious concerns from a national security perspective as the acquisition of a defense or aerospace company. Preventing threat actors from exploiting gaps in our existing jurisdictional authorities to acquire these technologies is very important for protecting US national security.

Senator Harris questions (email Tuesday 15May2018-1854)

QUESTION 8: Do you think the Intelligence Community was well prepared to counter the threat of Russian influence operations on social media during the 2016 election?

(U//FOUO) No, in my view, the Intelligence Community did not adequately anticipate the intentions or scope of Russian influence operations aimed at the 2016 campaigns and elections.

(U//FOUO) The Intelligence Community has taken several steps to improve the information it provides to policymakers about Russian influence operations on social media, to include providing classified threat briefings to state election officials, exploring ways to improve information sharing between federal and state entities, and providing guidance to IC analysts and collectors on the key intelligence requirements on threats to our democratic processes.

QUESTION 9: Does NCSC have a written strategy for how the IC should coordinate to counter foreign influence operations on social media going forward? If yes, will you share it with the Committee? If no, why not?

(U//FOUO) Although NCSC does not have a written strategy on this specific issue, NCSC is playing a leading role in government-wide efforts to counter foreign influence operations, to include on social media. Countering foreign influence operations that use social media is a shared responsibility across FBI, DHS, CIA, State Department, together with NCSC and other elements of the Office of the DNI.

(U//FOUO) NCSC is actively informing ongoing interagency policy deliberations to develop a whole-of-government strategy to counter Russian influence. NCSC is also focusing the Russia counterintelligence community to publish assessments on Russian influence activities through its issuance of the Strategic CI Priorities for Russia, CI Analytic Production Guidance, and associated collection requirements and emphasis messages identifying the top intelligence priorities for countering foreign influence operations.

QUESTION 10: What is NCSC doing in preparation for the 2018 mid-term elections regarding the foreign influence threat over social media?

(U//FOUO) NCSC is actively working to anticipate and counter threats to the 2018 mid-term elections, including both foreign threats to electoral infrastructure and foreign influence operations aimed at the elections.

- (U//FOUO) In February 2018, NCSC co-sponsored with DHS and FBI a two-day classified threat briefing to state election officials from all fifty states. The session provided state election officials with access to a full-range of the IC's top cyber and counterintelligence experts to discuss threats and vulnerabilities associated with the 2018 elections. It also allowed DHS, FBI, and other IC elements to better understand the needs and perspectives of the states in countering threats to U.S. elections.
- (U//FOUO) On 26 April 2018, NCSC and the Cyber Threat Intelligence Integration Center (CTIIC) co-sponsored a day-long table top exercise (TTX) aimed at strengthening the U.S. Government's information sharing posture to counter foreign intelligence threats to U.S. elections. The day-long TTX was attended by more than 50 senior representatives from the National Security Council and offices in CIA, DHS, FBI, NSA, and ODNI with cyber, counterintelligence, regional, and intelligence reporting responsibilities. Participants identified the demands, constraints, and challenges of information sharing and knowledge management within and between agencies on a sensitive issue that spans multiple regional and functional areas. Based on this TTX, NCSC, CTIIC, and other ODNI components identified a set of actionable whole-of-government recommendations for improving our election security posture over the near-term and mid- to long-term horizons.
- (U//FOUO) NCSC has worked to expose Russian influence operations to domestic and foreign audiences. In the past year, the Director of NCSC has conducted numerous public appearances on media networks to talk about Russian influence operations and how they can undermine the integrity of our democratic processes.

- (U//FOUO) NCSC works with international partners to discuss Russian influence operations and to share best practices at countering them.

QUESTION 11: Does NCSC have a written strategy for how the IC should coordinate to counter foreign intelligence threats to U.S. elections? If yes, will you share it with the Committee? If no, why not?

(U//FOUO) Although we do not have a formal, written strategy for how the IC should coordinate to counter foreign intelligence threats to the elections, NCSC, together with CTIIC, is actively informing ongoing interagency policy deliberations to improve IC coordination processes.

QUESTION 12: Has NCSC conducted a written review of what the IC could have done better, from a counterintelligence perspective, regarding Russian Active Measures targeting the 2016 election, and what lessons could be learned? If yes, will you share it with the Committee? If no, why not?

(U//FOUO) NCSC has conducted wide-ranging, informal collaboration and outreach to understand the lessons of counterintelligence from and cyber support to the 2016 U.S. elections, using its Counterintelligence Critical Infrastructure Task Force. For example, the Task Force spearheaded a 26 April 2018 Table Top Exercise aimed at strengthening the U.S. Government's information sharing posture to counter foreign intelligence threats to U.S. elections. Co-sponsored by NCSC and CTIIC, this exercise drew on lessons learned from the 2016 elections to explore ways in which information flows to support the 2018 elections could be improved.

○