

**NOMINATIONS OF ROBIN CARNAHAN,
JEN EASTERLY, AND JOHN C. INGLIS**

HEARING

BEFORE THE

**COMMITTEE ON
HOMELAND SECURITY AND
GOVERNMENTAL AFFAIRS
UNITED STATES SENATE
ONE HUNDRED SEVENTEENTH CONGRESS**

FIRST SESSION

NOMINATION OF ROBIN CARNAHAN TO BE ADMINISTRATOR,
GENERAL SERVICES ADMINISTRATION, JEN EASTERLY TO BE
DIRECTOR, CYBERSECURITY AND INFRASTRUCTURE SECURITY
AGENCY, U.S. DEPARTMENT OF HOMELAND SECURITY AND
JOHN C. (CHRIS) INGLIS TO BE NATIONAL CYBER DIRECTOR,
EXECUTIVE OFFICE OF THE PRESIDENT

JUNE 10, 2021

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

Printed for the use of the
Committee on Homeland Security and Governmental Affairs



U.S. GOVERNMENT PUBLISHING OFFICE

46–566 PDF

WASHINGTON : 2022

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

GARY C. PETERS, Michigan, *Chairman*

THOMAS R. CARPER, Delaware	ROB PORTMAN, Ohio
MAGGIE HASSAN, New Hampshire	RON JOHNSON, Wisconsin
KYRSTEN SINEMA, Arizona	RAND PAUL, Kentucky
JACKY ROSEN, Nevada	JAMES LANKFORD, Oklahoma
ALEX PADILLA, California	MITT ROMNEY, Utah
JON OSSOFF, Georgia	RICK SCOTT, Florida
	JOSH HAWLEY, Missouri

DAVID M. WEINBERG, *Staff Director*

ZACHARY I. SCHRAM, *Chief Counsel*

CHRISTOPHER J. MULKINS, *Director of Homeland Security*

CLAUDINE J. BRENNER, *Counsel*

PAMELA THIESSEN, *Minority Staff Director*

ANDREW DOCKHAM, *Minority Chief Counsel and Deputy Staff Director*

KIRSTEN D. MADISON, *Minority Director of Homeland Security*

AMANDA NEELY, *Minority Deputy Chief Counsel*

WILLIAM H.W. MCKENNA, *Minority Chief Investigator*

JEFFREY A. POST, *Minority Senior Professional Staff Member*

CARA G. MUMFORD, *Minority Professional Staff Member*

ANDREW J. TIMM, *Minority Professional Staff Member*

LAURA W. KILBRIDE, *Chief Clerk*

THOMAS J. SPINO, *Hearing Clerk*

CONTENTS

Opening statements:	Page
Senator Peters	1
Senator Portman	2
Senator Carper	18
Senator Lankford	21
Senator Padilla	24
Senator Hassan	27
Senator Hawley	29
Senator Ossoff	32
Senator Scott	35
Senator Sinema	40
Prepared statements:	
Senator Peters	45
Senator Portman	47

WITNESSES

THURSDAY, JUNE 10, 2021

Hon. Roy Blunt, a U.S. Senator from the State of Missouri	3
Hon. Mike Gallagher, a Representative in Congress from the State of Wisconsin	3
Hon. Angus S. King, Jr., a U.S. Senator from the State of Maine	5
Robin Carnahan to be Administrator, General Services Administration	
Testimony	7
Prepared statement	49
Biographical and professional information	52
Letter from U.S. Office of Government Ethics	72
Responses to pre-hearing questions	76
Responses to post-hearing questions	101
Jen Easterly to be Director, Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security	
Testimony	8
Prepared statement	108
Biographical and professional information	110
Letter from U.S. Office of Government Ethics	130
Responses to pre-hearing questions	136
Responses to post-hearing questions	169
Letters of support	172
John C. (Chris) Inglis to be National Cyber Director, Executive Office of the President	
Testimony	10
Prepared statement	189
Biographical and professional information	191
Letter from U.S. Office of Government Ethics	212
Responses to pre-hearing questions	219
Responses to post-hearing questions	250
Letters of support	261

APPENDIX

Mission Needs Chart	265
HSGAC Letters	266

NOMINATIONS OF ROBIN CARNAHAN, JEN EASTERLY, AND CHRIS INGLIS

THURSDAY, JUNE 10, 2021

U.S. SENATE,
COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Committee met, pursuant to notice, at 10:16 a.m., via Webex and in room SD-342, Dirksen Senate Office Building, Hon. Gary C. Peters, Chairman of the Committee, presiding.

Present: Senators Peters, Carper, Hassan, Sinema, Rosen, Padilla, Ossoff, Portman, Lankford, Scott, and Hawley.

OPENING STATEMENT OF CHAIRMAN PETERS¹

Chairman PETERS. The Committee will come to order.

Today we are considering three nominations: Robin Carnahan, who is joining us remotely, to be Administrator of the General Services Administration (GSA); Jen Easterly, to be Director of the Cybersecurity and Infrastructure Security Agency (CISA), within the Department of Homeland Security (DHS); and Chris Inglis, to be the first-ever National Cyber Director (NCD). Welcome to each of you, and welcome to your family members who are joining us here today.

Congratulations on your nominations, and thank you for your previous service and for your willingness to take on these important new roles.

The agencies or offices you have been nominated to lead, each play a critical role in strengthening our national security and ensuring the Federal Government is operating both effectively and efficiently.

The General Services Administration provides a wide range of support to Federal agencies, including managing Federal property and the Federal fleet and offering cost savings, acquisition programs, and technology services. In short, GSA helps ensure agencies can deliver for the taxpayer and for the American people.

Ms. Carnahan, if confirmed, you will lead GSA at a pivotal moment. The Coronavirus Disease 2019 (COVID-19) pandemic changed how workplaces operate across the government and across the Nation. The Biden administration is charting a course to make Federal buildings, vehicles, and operations more energy efficient, and agencies must do more to modernize and secure their information technology (IT) systems and their networks. I look forward to

¹ The prepared statement of Senator Peters appear in the Appendix on page 45.

hearing more about how you plan to lead GSA to tackle these and other challenges.

The next two nominations are both firsts for this Committee. Ms. Easterly, you are the first person nominated to lead CISA since it was created by this Committee in 2018 and charged with protecting and defending Federal networks and securing critical infrastructure. This Committee worked closely with Chris Krebs, who led the transformation from its predecessor agency, and CISA has made a lot of progress in a very short period of time. But we all know there is a whole lot more to do.

The recent SolarWinds hack and the Colonial Pipeline ransomware attack are only the latest reminders of what the Federal Government must do to secure its own networks and to work with and support our private sector, nonprofit, State, local, tribal, and territorial (SLTT) governments.

Mr. Inglis, you have been nominated to be the first-ever National Cyber Director, a position this Committee created last year to lead a new office within the Executive Office of the President (EOP) and coordinate national cybersecurity policy and strategy. The National Cyber Director will be central to ensuring a cohesive, whole-of-government approach to cybersecurity.

These are all vital roles, and I am pleased we have three highly qualified nominees here today who each bring a wealth of government and private sector experience. I look forward to hearing from each of you today.

With that, I will turn it over to Ranking Member Senator Portman.

OPENING STATEMENT OF SENATOR PORTMAN

Senator PORTMAN. Thank you, Chairman Peters, and I thank my colleagues for being here. Senator King, I just left you a few moments ago on a Zoom call. Senator Blunt, you and I have spent a lot of quality time together recently.

Senator BLUNT. That is our lives these days.

Senator PORTMAN. Yes. I have a very long, articulate and important statement to make that I am going to submit for the record¹ and instead just say welcome to Ms. Carnahan, Ms. Easterly, and Mr. Inglis. I have spoken to all of you. I have had the opportunity to get to know you a little bit. These are really important positions, and the leadership deserves careful consideration, which it will get at this hearing.

With that, Mr. Chairman, I will again submit my full statement for the record and look forward to hearing from my colleagues in the Senate.

Senator PETERS. Next we have some guests joining us today to introduce the nominees.

First, we are joined by our colleague Senator Blunt, who will be introducing Ms. Carnahan. Senator Blunt, thank you for being with us. Good to see you, and you are recognized for your introduction.

¹The prepared statement of Senator Portman appears in the Appendix on page 47.

**STATEMENT OF HONORABLE ROY BLUNT, A UNITED STATES
SENATOR FROM THE STATE OF MISSOURI**

Senator BLUNT. Thank you, Chairman Peters. As Senator Portman pointed out, the three of us, along with Senator Klobuchar, have spent a lot of time together over the last month. I am glad to be here on this topic as well as I was pleased to work on the other issues we have been working on.

Thanks for holding this hearing. I am glad to be able to speak to the Committee regarding the nomination of Robin Carnahan to be the Administrator of the General Services Administration. I am honored to welcome her to the Senate today even if it is only over video.

Robin Carnahan was born and raised in the great State of Missouri. Throughout her life, she and her family have served our State and our country in many roles and with distinction.

After graduating from William Jewell College in Liberty, Missouri, and the University of Virginia Law School, she practiced law in St. Louis and held positions with the National Democratic Institute and the Export-Import (EXIM) Bank of the United States. From 2005 to 2013, she served as the Secretary of State of Missouri. In this role, she utilized innovative technology to save money and improve government service for residents of Missouri, I probably should add here following the example of her great predecessor, my son, Matt Blunt, who held that job right before Robin did. It is a job I held as well, and the three of us have common appreciation for that particular place to serve Missourians. In 2016, she joined the Office of 18F at the General Services Administration. This office provides technology consultation to State and local governments.

I think the bottom line here, Mr. Chairman and Senator Portman, is that Robin Carnahan understands the GSA and she understands the importance of the GSA to the country. I have no doubt that, if confirmed, she would be a successful and an effective Administrator of the General Services Administration. I understand this to be a job of major significance in the daily operations and decisions of the government that fall within the purview of the General Services Administration. I look forward to supporting her confirmation. Of course, before I can do that, your Committee needs to recommend that that confirmation move forward, and I hope you do.

Chairman PETERS. Thank you, Senator Blunt.

Next we have a video from Representative Gallagher introducing Ms. Easterly.

**STATEMENT OF HONORABLE MIKE GALLAGHER, A REP-
RESENTATIVE IN CONGRESS FROM THE STATE OF WIS-
CONSIN**

Mr. GALLAGHER. Thank you, Senator Peters, Senator Portman, and distinguished Members of the Committee, for allowing me to introduce Jen Easterly for her nomination to be the Director of the Cybersecurity and Infrastructure Security Agency.

It is an honor to be here to introduce Jen. As the Co-Chair of the Cyberspace Solarium Commission (CSC) with my good friend Senator Angus King, I cannot overstate what a crucial role the Presi-

dent has nominated Jen to fill. Our bipartisan public-private commission assessed that CISA is the most important agency in the execution of Federal network security and the development of an effective public-private collaboration to protect our national critical infrastructure.

CISA is quite simply on the front lines of ensuring the Federal departments and agencies, the private sector, and the American people have the resources to detect, withstand, and respond to cyberattacks. Thanks in large part to the work of your Committee, we have made significant progress on strengthening the agency so that it can perform this crucial mission.

For example, we authorized CISA to perform threat hunting on Federal networks to more proactively identify cyber threats to Federal assets and systems and begin any necessary mitigation processes sooner. We also elevated the role of CISA Director so that the position is equivalent to that of the Transportation Security Administration (TSA) Administrator in order to emphasize the importance and stature of the agency and its leader. When we did that, when we amended the law to elevate the position of CISA Director, we stipulated that a qualified CISA Director would be someone who has extensive knowledge of cybersecurity, infrastructure security, and security risk management and has at least 5 years of experience fostering multistakeholder coordination and collaboration on these issues.

Jen Easterly's qualifications are well above and beyond those stipulated by the law. Her background is incredible. She is currently the head of Firm Resilience and the Fusion Resilience Center at Morgan Stanley. In this capacity, she is responsible for ensuring preparedness and response to business-disrupting operational incidents and risks. Jen joined Morgan Stanley in February 2017 to build and lead the firm's Cybersecurity Fusion Center, which is the operational cornerstone of its entire cyber defense strategy. Prior to joining the private sector, Jen served for three decades in the Federal Government. She was the Special Assistant to the President and Senior Director for Counterterrorism, where she led the development and coordination of U.S. counterterrorism and hostage policy. Prior to that, she was the Deputy for Counterterrorism at the National Security Agency (NSA), where she was responsible for leading operations to detect and disrupt terrorist attacks against the United States and our allies.

Jen is a two-time recipient of the Bronze Star. She retired from the U.S. Army after more than 20 years of service in intelligence and cyber operations. She was responsible for setting up the Army's first cyber battalion. She was also instrumental in the design and creation of U.S. Cyber Command (USCYBERCOM).

She is a distinguished graduate of the United States Military Academy (USMA) at West Point. She holds a Master's degree in philosophy, politics, and economics from the University of Oxford, where she studied as a Rhodes scholar. She is a real overachiever. I could go on. But Jen's accolades and accomplishments are so numerous that we might never actually get to the hearing itself. She was a critical member of our Red Team on the Solarium Commission, and I want to say what an honor it is to be at the same hearing where Senator King, my Co-Chair, will introduce our fellow

Commissioner Chris Inglis for his nomination as our country's first National Cyber Director.

Jen and Chris are great cybersecurity experts, to be sure, but more than that, they are also great Americans. They embody what it means to put politics aside and serve the Nation. They will be a great team that introduces the speed and agility into cybersecurity and critical infrastructure protection that I believe is needed to protect our country against the malicious cyber activity that we are seeing.

I look forward to this hearing and to the Committee's progress on putting Jen to work as quickly as possible as our next CISA Director. Thank you again, Senator Peters, Senator Portman, and the distinguished Members of this Committee, for your time and for your consideration of Jen's nomination.

Chairman PETERS. Now we are joined by the Co-Chair of the Solarium Commission. Senator King, great to have you before our Committee. Senator King will recognize Mr. Inglis. Senator King, you are recognized for your opening statement.

**OPENING STATEMENT OF HONORABLE ANGUS S. KING, JR., A
UNITED STATES SENATOR FROM THE STATE OF MAINE**

Senator KING. Mr. Chairman and Senator Portman and Members of the Committee, America is under attack. We are under attack today. This is one of the most serious conflicts, one of the most serious challenges that this country has faced in the post-World War II period.

The two positions that we are really talking about today are the equivalent of the Secretary of Defense and the head of the Joint Chiefs of Staff (JCS). These are people who will be charged with defending this country in what is an ongoing and serious conflict.

I am taking time out now from an Armed Services Committee hearing with the Secretary of Defense and the head of the Joint Chiefs, and cyber is one of the things that we will be talking about. It is a ubiquitous challenge not only to the government but especially to the private sector, and that is one of the really significant challenges in how we respond.

We have to reimagine conflict. We think of conflict in terms of armies and battleships and air forces, but we are really now talking about the front line of this conflict can take place in a server farm on Wall Street, in a pipeline company, or in an electric company, or in a water service utility anywhere in America.

Chris Inglis served with Mike Gallagher and me on the Solarium Commission, which was created by this Congress in 2019 to devise a national cyber policy. This was a unique Commission that had four Members of Congress, four members from the executive, and six members from the private sector, a totally nonpartisan process and a very intense process. In fact, next Monday will be our 43rd meeting of the Solarium.

Sitting next to me through most of those meetings was Chris Inglis, who I had never known before, but have gotten to know very well during this process. His credentials are impressive. In fact, when I first looked at it, I thought this guy has had two full careers; he must be 100 years old. He has 30 years of service in the Federal Government, particularly as Deputy Director of the Na-

tional Security Agency, but also 28 years in the United States Air Force (USAF), active duty and also in the Air Force Reserve, retiring as a general. He has degrees in computer science. He has immense knowledge and experience in this field.

Beyond that, however, and the reason I am so enthusiastic about his nomination, is his leadership qualities which I observed during the course of our deliberations as the Cyberspace Solarium Commission. He has a quiet but persuasive leadership style. All of us have been in meetings where there is one person when they begin to speak, you lean over and say, "Now, what are they going to say? Because this is going to be important." That is Chris Inglis.

This is an immensely important job because of the intersection between the private sector and the Federal Government and the complexity of the challenge throughout the Federal Government. The fundamental purpose of the National Cyber Director is to coordinate Federal cyber policy among all these different agencies that have a piece of it, but also to coordinate cooperation between the Federal Government and the private sector. He will be working with Jen Easterly and Anne Neuberger in the National Security Council (NSC), which I think represents three of the absolute perfect combination to lead this effort to defend our Nation.

I am very proud to be able to introduce Chris Inglis to the Committee. I honestly believe, based upon 3 years of extensive engagement in this issue with people across the country, he is the single best person to fill this role, and a particularly important role as the first leader of the Office of National Cyber Director in the Executive Office of the President.

Mr. Chairman, I cannot recommend Chris Inglis more highly, and I am delighted that he is willing to reenlist, if you will, in Federal service and service to the country.

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

Chairman PETERS. Thank you, Senator King, for the introduction. Thank you for your amazing leadership in terms of dealing with this incredible threat. You have been a real leader on cybersecurity issues. We appreciate all the work of the Commission and appreciate you being here today and your continued involvement on this issue. Thank you.

It is the practice of this Committee to swear in witnesses, so if each of our witnesses could stand and raise their right hands? Even on video, stand there and raise your right hands. Do you swear that the testimony you will give before this Committee will be the truth, the whole truth, and nothing but the truth, so help you, God?

Ms. CARNAHAN. I do.

Ms. EASTERLY. I do.

Mr. INGLIS. I do.

Chairman PETERS. Please be seated.

We will now hear from each of our nominees. Ms. Carnahan, you may proceed with your opening remarks.

**TESTIMONY OF ROBIN CARNAHAN,¹ NOMINEE TO BE
ADMINISTRATOR, GENERAL SERVICES ADMINISTRATION**

Ms. CARNAHAN. Good morning, Chairman Peters, Ranking Member Portman, and Members of the Committee. I appreciate the opportunity to be here today, and I am honored to be President Biden's nominee for Administrator of the General Services Administration. I am also grateful to Senator Blunt, my home-State Senator, for that kind introduction. We have known each other for more than 30 years and our families even longer. I value Senator Blunt's leadership, his passion for public service, and his commitment to the people of Missouri. Senator, thank you so much for your service.

Even though we are joining virtually today, I would like to acknowledge my family: my husband, Juan Carlos, for his unwavering love and encouragement; my mother, Jean, who has been a role model and hero all my life; and my brothers, Russ and Tom, and their wonderful families. They have been a tremendous source of love and strength.

Public service, as Senator Blunt said, runs in my family, much of that serving the people of Missouri. My grandfather and brother served in Congress. My father was Governor, and my mother was the first woman from Missouri in the U.S. Senate. But my mother's parents were also public servants, though they never ran for office. You see, mom was born in Washington, D.C. She grew up across the river in Anacostia. Her father was a farmer and plumber at St. Elizabeths Hospital, and her mother worked at the Navy Department during the war.

So growing up, the government did not seem like a faraway or abstract concept. For me, it was about the people who worked on behalf of their community and country, folks who went to work every day to improve the lives of children and families, to help businesses thrive and keep the country safe. I grew up believing that public service was a noble calling, worthy of our lives. I still do.

I have had the privilege of serving in elected office myself, as well as in appointed and staff positions in State and Federal Government. No matter what the role, I always understood my job was to deliver effective service for people and be a wise steward of taxpayer money.

I will never forget the first day on the job as Missouri Secretary of State. I was being introduced around the office, and I met more people who were manually opening mail and preparing checks to be deposited than we had in the entire IT department. That was the moment in 2005 that crystallized how I came to view the challenge ahead for government—to adapt modern technology tools to streamline operations and to serve people better.

So during my tenure, we invested time and money in modernizing our IT infrastructure in order to do better service for 400,000 businesses, 4 million voters, and millions of others who needed something from their government.

One lesson I learned was that digital infrastructure investments pay off, both in better service and lower costs to taxpayers. But I

¹The prepared statement of Ms. Carnahan appears in the Appendix on page 49.

also learned that without serious attention, these tech modernization projects can go wrong. The truth is there was nothing I did when I was in office that caused me to lose more sleep than the rollout of one of those new tech platforms.

So diving in to learn more about technology and procurement policy is what led me to GSA, where I served 4 years during the Obama and Trump administrations. I joined the digital consulting team 18F whose job was to help government partners more effectively buy and build modern software systems and train non-technical leaders on how to set their teams up for success.

Now, this past year has shown the importance and the fragility of our Nation's digital infrastructure. As the pandemic swept through the country, Congress responded fast with programs to meet the challenges. But yet too often the help was slow getting to the families and businesses that needed it most.

The bottom line is no program passed by this Congress can be effective without smart investments in an effective, secure digital infrastructure to deliver it. And GSA is uniquely positioned to support that mission across government.

Of course, I know GSA is about a lot more than technology, but I see similar opportunities to improve the way it delivers value to partners in real estate management and acquisition. If confirmed, I look forward to exploring creative, practical ways to right-size the Federal real estate portfolio to serve the changing needs of agencies and local communities.

In acquisitions, I look forward to working with stakeholders, including agency partners and companies, to streamline and simplify how they interact with GSA. I want to provide easy access and great value to those who buy through GSA and an easier on-ramp for businesses, especially small businesses, interested in selling through GSA.

As President Biden recently said in his speech to Congress, "We have to prove democracy still works. That our government still works—and can deliver for the people."

For me, helping our government, our democracy, effectively deliver for the people and taxpayers is why I am so excited about the opportunity to lead GSA.

Thanks for the chance to testify today. I am humbled, and I look forward to answering your questions.

Chairman PETERS. Thank you, Ms. Carnahan, for your opening remarks.

Ms. Easterly, you are now recognized for your opening remarks.

TESTIMONY OF JEN EASTERLY,¹ NOMINEE TO BE DIRECTOR, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, U.S. DEPARTMENT OF HOMELAND SECURITY

Ms. EASTERLY. Chairman Peters, Ranking Member Portman, distinguished Members of the Committee, I am honored to appear before you to discuss my nomination for Director of the Cybersecurity and Infrastructure Security Agency. I want to thank the President for nominating me, Secretary Mayorkas for his confidence in me, and Congressman Gallagher for his very kind introduction, and,

¹ The prepared statement of Ms. Easterly appears in the Appendix on page 108.

more importantly, for his and Senator King's absolutely superb leadership of the Cyberspace Solarium Commission.

I also want to thank my family and, in particular, my parents: my father, Noel Koch, a Vietnam veteran whose forebears fought in the Civil War to ensure that the Nation experienced "a new birth of freedom"; and my mother, Dr. June Koch, an English professor and the daughter of immigrants from Russia and Poland who came to America to enjoy that freedom. Both led lives of public service, instilling in me the importance of service and of actively participating in our great democratic project, to form, continuously, a more perfect union. Their example inspired me to commit 27 years of my life in service to the Nation, including more than two decades in the United States Army, leading soldiers in peacetime and in combat. It also motivates my return to public service after 4½ years in the private sector at one of our Nation's leading financial institutions.

Additionally, I want to thank my husband, Jas, for his love and support over the past 17 years, through multiple moves and four separate deployments. As a fellow U.S. Army combat veteran, I also want to thank him for his service to our country. I especially want to recognize our son Jet, the light and joy of our life, who aspires to one day be President.

Twenty years ago, the attacks of 9/11 fundamentally altered the course of my life, as it did for so many. As noted by Tom Kean, the Co-Chairman of the 9/11 Commission, "We were unprepared. We did not grasp the magnitude of a threat that had been gathering over a considerable period of time. This was a failure of policy, of management, of capability, and, above all, a failure of imagination." If the past year has taught us anything, it is the obligation we have as leaders to anticipate the unimaginable.

While the digital revolution of the past several decades enabled unprecedented growth and innovation, the increasing connectivity also introduced great peril: nation-states and non-state actors alike now leverage cyberspace with near impunity to threaten our security, our privacy, and our physical and digital infrastructure. Our adversaries combine hacking with malign influence operations to interfere in our democratic processes. They breach major corporations to steal capital and intellectual treasure, target industrial control systems to disrupt critical infrastructure, and incapacitate entities large and small with the scourge of ransomware. Even as we contend with the billions of daily intrusions against our networks by malicious actors, I believe that as a Nation we remain at great risk of a catastrophic cyber attack.

Congress established CISA in 2018 as the country's operational entity for managing and mitigating such risk, working closely with partners at the State, local, tribal, and territorial level, as well as with the private sector to ensure the security and resilience of our critical infrastructure.

Within the Federal cyber ecosystem, CISA is the "quarterback," charged with protecting and defending Federal civilian government networks; leading asset response for significant cyber incidents; and ensuring that timely and actionable information is shared across Federal, non-Federal, and industry partners.

In this context, I also thank the Committee for your leadership in establishing CISA, my good friend Chris Krebs for his absolutely superb work in standing up and leading the agency, and Acting Director Wales and the dedicated men and women of CISA for their tireless efforts defending our infrastructure against a myriad of significant and serious threats, and ensuring secure, interoperable emergency communications. If confirmed, it will be the greatest honor of my career to join their incredible team, to continue building the culture and the workforce of CISA, and to strengthen its capacity and capability to defend today and secure tomorrow.

The best quarterback, however, cannot win a game alone; cyber is and must always be a team sport. CISA fulfills its lead operational role for national cyber and infrastructure resilience in collaboration with other agencies at every level of government and with our industry and international partners. A critical element of this ecosystem is the National Cyber Director, who will ensure a coherent and unified Federal effort as the President's principal cyber adviser. If we are both confirmed, I look forward to working, once again, with Mr. Inglis. I also look forward to a productive and transparent partnership with this Committee.

I thank the Committee for considering my nomination and look forward to your questions.

Chairman PETERS. Thank you, Ms. Easterly, for your opening remarks.

Mr. Inglis, you are now recognized for your opening remarks.

TESTIMONY OF JOHN C. (CHRIS) INGLIS,¹ NOMINEE TO BE NATIONAL CYBER DIRECTOR, EXECUTIVE OFFICE OF THE PRESIDENT

Mr. INGLIS. Thank you, sir. Chairman Peters, Ranking Member Portman, and distinguished Senators, I am honored to appear before you. I thank this Committee for its support in the creation of this new role and your strategic leadership on cybersecurity. I thank the President for nominating me and Senator King for his generous introduction. I also want to thank both Senator King and Congressman Gallagher for their work leading the Cyberspace Solarium Commission's efforts to improve our Nation's ability to fully realize its aspirations in and through the critical realm of cyberspace.

I also want to recognize my family. I thank my parents, Robert and Kathleen Inglis, who gave their children the priceless gift of a home where service to others, respect, and accountability was expected and freely given as the foundation of life. I want to thank my wonderful wife, Anna, who is with me here today, and our children, Luciana, Paul, and George, for their love and support, which has inspired and sustained me through all of my adult life.

I am humbled by the privilege and the opportunity to reenter public service. While the position of National Cyber Director may be new, I am mindful that the team that I would join, should I be confirmed, is one that is already on the field, impressively diverse, and broadly engaged. It is a team that includes public servants at Federal, State and local levels, and private sector professionals

¹ The prepared statement of Mr. Inglis appears in the Appendix on page 189.

whose collective efforts build, operate, innovate, and defend the digital infrastructure upon which the delivery of critical services increasingly depends. I am particularly pleased to testify alongside Jen Easterly, the prospective Director of CISA, and Robin Carnahan, the prospective Administrator of GSA. Should we be confirmed, our collaboration will be an important element of any Federal cyber strategy going forward.

If confirmed, I expect that I should and will be held accountable to add context, leverage, and strength to the distributed work of that full cyber team. To that end, the enabling legislation for the National Cyber Director has clearly laid out its core responsibilities. These include forging a coherent and unified Federal effort; developing and overseeing the implementation of the National Cyber Strategy; ensuring the coordination of appropriate Federal budgets, policies, and plans; fostering mutually beneficial public-private collaboration; and, more importantly than all of those, demonstrable improvements in the resilience, the robustness, and the defense of the cyber ecosystem.

As the legislation acknowledges, these duties require robust engagement with both the private sector, which is on the front lines of this effort, and with the Congress, to whom the National Cyber Director owes regular updates on cyber risk and the status of U.S. cybersecurity efforts. Additionally, the National Cyber Director occupies a highly visible position within the U.S. Government—one that should be expected to offer a clear, unified voice in public communications and advocacy.

Supporting lines of effort must necessarily address the fact that cyberspace is not built and operated as a single, centralized organization and that it is comprised of far more than technology. Essential collaboration and integration will heavily depend on how roles and responsibilities are defined and executed, while the success of a national strategy will depend as much on the skills of our people as on the technologies that they employ.

Given those realities, we must ensure that our technology is built and deployed with security foremost in mind; that the supply chains that support them are free from security risk; that our people are cyber literate; and that roles, responsibilities, and attendant accountability are sufficiently well defined that we remove the fissures and seams in cyber defenses that offer adversaries opportunities to find and exploit weakness.

As this Committee and recent witnesses before you have so frequently discussed, SolarWinds, Hafnium, Colonial Pipeline, JBS, and other incidents all signal the urgent need to secure our national critical infrastructure. The pace of events and our adversaries deny us the luxury of biding our time before we seize back the initiative that has too long been ceded to criminals and rogue nations who determine the time and manner of their transgressions.

If confirmed, I will work closely with the Congress, the Executive Branch, the private sector, and State and local entities to stand up, harness, and realize the expected benefits of the Office of the National Cyber Director (ONCD).

I thank the Committee for considering my nomination, and I look forward to your questions.

Chairman PETERS. Thank you, Mr. Inglis, for your opening comments.

There are three questions that this Committee asks of every nominee, and I will ask each of you to respond briefly with a yes or no to these questions.

First, is there anything you are aware of in your background that might present a conflict of interest with the duties of the office to which you have been nominated? We will start with Ms. Carnahan and then go to Ms. Easterly and then Mr. Inglis. Ms. Carnahan?

Ms. CARNAHAN. No, sir.

Ms. EASTERLY. No, sir.

Mr. INGLIS. No, sir.

Chairman PETERS. Second, do you know of anything, personal or otherwise, that would in any way prevent you from fully and honorably discharging the responsibilities of the office to which you have been nominated?

Ms. CARNAHAN. No, Senator.

Ms. EASTERLY. No, sir.

Mr. INGLIS. No, sir.

Chairman PETERS. Last, do you agree without reservation to comply with any request or summons to appear and testify before any duly constituted committee of Congress if you are confirmed?

Ms. CARNAHAN. Yes, sir.

Ms. EASTERLY. Yes, sir.

Mr. INGLIS. Yes, sir.

Chairman PETERS. Great. Thank you.

Mr. Inglis, if confirmed, you will be in a very challenging position of being the first National Cyber Director. Your authorities have never been utilized, your role has never been performed, and many other leaders in government have cyber and security responsibilities as well.

So my question to you, sir, is: If confirmed, how would you see your role as being unique and different from that of the Director of CISA?

Mr. INGLIS. Senator Peters, thank you for the question, and thank you again for the work that this Committee did to invest the National Cyber Director with the authorities and the accountability that we are discussing here today. I think that if you stand back and read the very detailed language of the National Cyber Director authorization, what it really is pushing for is to create coherence, unity of effort, unity of purpose across what are already impressive, deep, and sharp capabilities within the Federal enterprise and a partnership with the private sector where most of cyber gets built, operated, innovated, and defended.

I think that the primary purpose of the National Cyber Director must be to add value, coherence, leverage, connection to all of those other pieces and to identify, when necessary, when something is missing and to ensure that the national strategy and that our implementation of that strategy ultimately creates a coherent effort. I think that the premise for us within the United States and like-minded nations must increasingly be that if you are an adversary in this space, you have to beat all of us to beat one of us. The National Cyber Director needs to make that true.

Chairman PETERS. Thank you.

Ms. Easterly, a similar question for you. CISA is the lead cybersecurity agency for operational Federal cybersecurity and supporting critical infrastructure. So my question to you is: If confirmed, where would you see the boundary between your work and that of the National Cyber Director?

Ms. EASTERLY. Thank you very much for the question, Mr. Chairman. As we know, CISA is the operational entity charged with managing and mitigating risk to digital and physical infrastructure working closely with partners at the State, local, tribal, and territorial level, and then, of course, with the private sector to be able to ensure the resilience and the security of our critical national infrastructure. I see CISA's role within the Federal cyber ecosystem as the quarterback, if you will, responsible for protecting and defending Federal civilian government networks in close partnership with the Office of Management and Budget (OMB), which, is responsible overall for Federal cybersecurity, also leading asset response for significant cyber incidents, and then, finally, for ensuring that timely and actionable information is shared across Federal and non-Federal and private sector partners. Within that ecosystem, I see the National Cyber Director as a critical partner, essentially the coach of the team responsible for overseeing the implementation of cyber strategy and policy and really bringing that sense of coherence and unity of effort to the Federal cyber ecosystem. If confirmed, I would look forward to working closely and collaboratively with Mr. Inglis.

Chairman PETERS. This next question will be to both of you as well. Ransomware attacks are nothing new, but they have been increasing in their impact, particularly the recent attacks that we have seen of our critical infrastructure. We had the Chief Executive Officer (CEO) of Colonial Pipeline in this room a short while ago. If confirmed, you each will play a significant role in helping us address this ever growing threat.

Ms. Easterly, my question for you is: How do you view the role of CISA in fighting back against these ransomware attacks?

Ms. EASTERLY. It is a very important question, Mr. Chairman. Thanks for asking it. Ransomware is clearly a scourge, clearly a national security threat, 2,400 incidents last year alone, \$350 million in cryptocurrency. This requires an all-hands-on-deck effort that leverages the talents and capabilities across the interagency, from law enforcement to the intelligence community (IC) to diplomacy to Treasury.

Very importantly, CISA's role in this ecosystem is to prevent people from having to make the really difficult decision about whether they end up paying the ransom or not. CISA's role is to provide the technical assistance, the threat information, the guidance, the educational resources to ensure that entities across the Federal Government, the non-Federal Government, and, of course, the private sector are prepared to defend themselves in this very complex cyber threat environment.

Chairman PETERS. Mr. Inglis, what role should the National Cyber Director play?

Mr. INGLIS. Thank you for the question. I would complement Ms. Easterly's answer by saying that the National Cyber Director needs to be an advocate and a connector for those various capabilities

represented in places like CISA, but also the Department of Justice (DOJ), Department of Treasury, within the private sector that can systematically attack the system that today is the scourge known as “ransomware.” When you think about how that system works, there are weaknesses in our technology and oftentimes in the knowledge of the people who are on the front lines. There are sanctuaries that give safe harbor to the transgressors. There are other transgressors who must be dealt with. We must bring them to justice. There are financial systems, there are a great many things that we need to knock the legs out from under, and that will require a team effort. The National Cyber Director has to ensure that there is, in fact, a strategy that connects all those pieces and that that is being implemented in a concurrent, unified way, such that we might take this down using all instruments of power.

Chairman PETERS. I am currently working on legislation that would help illuminate this threat and get more information on ransomware attacks into the government so that we can both warn potential victims and also work to dismantle these criminal networks that are engaged in these activities. My question to both of you: Would you commit, if confirmed, to working with me on this important legislation so that we can enhance our ability to fight against this threat? Ms. Easterly?

Ms. EASTERLY. Absolutely, Mr. Chairman. I would look forward to that if confirmed.

Mr. INGLIS. If confirmed, absolutely, sir.

Chairman PETERS. Great. Thank you.

Ms. Easterly, the threat of foreign disinformation is real and has had particular impacts on our elections and on our ability to combat COVID-19. CISA has recently stood up a mis-, dis-, and malinformation team to help address this threat. If confirmed, what role would you see CISA playing to help us address this issue?

Ms. EASTERLY. Thanks very much for the question. It is a very important one, Mr. Chairman. First I would say I absolutely agree with you about misinformation and disinformation. It is a particular worry of mine. You need to have the best information, the facts, to be able to make the best decision, and so I think that is absolutely critical. I am aware of CISA’s work stood up during the 2020 elections in particular known as “Rumor Control” to deal with some of the misinformation and disinformation efforts and then the MDM team that now sits under the National Risk Management Center.

If I am confirmed, I would take a very hard look at that effort to see what CISA’s role can be and should be in misinformation/disinformation, and I would also want to make sure that CISA is continued to be seen as a nonpartisan and apolitical agency in all of the actions that it took.

Chairman PETERS. Absolutely, and I appreciate your focus on this.

I am also currently working on legislation to codify CISA and DHS’ authorities in this area, so my question to you is: If confirmed, do you commit to working with me on this bill to ensure that the Department has the proper authorities and limits to combat this threat?

Ms. EASTERLY. Absolutely, Mr. Chairman.

Chairman PETERS. Thank you.

Ranking Member Portman, you are recognized for your questions.

Senator PORTMAN. Thank you, Mr. Chairman. I look forward to working with you on that legislation, and we will talk about accountability in a moment and the importance of having clear lines of accountability in what is an increasingly concerning issue, which is not ransomware but cyber attacks generally.

With regard to our oversight role here, in order to do it properly, we need to have information. One of the congressional complaints sometimes is about responsiveness. This is particularly true, unfortunately, in this area, and so I want to ask you some questions about that.

Ms. Carnahan, I will start with you on the video. I will ask you, do you agree to promptly provide the Committee with documents and information that we request?

Ms. CARNAHAN. Certainly, Senator.

Senator PORTMAN. Thank you.

Ms. Easterly, yes or no would suffice.

Ms. EASTERLY. Absolutely, sir.

Senator PORTMAN. Mr. Inglis?

Mr. INGLIS. Yes, sir.

Senator PORTMAN. Let me give you an example of this. Ms. Easterly, the authorization for CISA's flagship cybersecurity program, the EINSTEIN program, as you know, is expiring. It expires next year, so we have been working on a reauthorization bill. I hope to work with Chairman Peters and all Members of this Committee on that. It has to be reauthorized. And yet we are having a really hard time getting information.

On April 5th, Chairman Peters and I sent to CISA a letter requesting information about EINSTEIN to inform our legislative efforts. Until earlier this week, the only response we received were documents previously provided to Congress, so nothing new, and a lot of the documents we received this week were heavily redacted. Let me give you an example of that. We will put it up here behind me.

This is the document where everything apparently describing the mission needs of EINSTEIN is redacted. Not terribly useful and not helpful in order for us to give you the key tool that you would need, should you be confirmed, to be sure that DHS is effective at combating cybersecurity.

So my question for you would be, understanding you were not involved in this decision, but should you be confirmed, would you agree that the Chair and Ranking Member of an authorize committee should be allowed to review the mission needs of a program before attempting to reauthorize it?

Ms. EASTERLY. Thanks for that question, Ranking Member Portman. I would say that I absolutely believe in the strong oversight role that this Committee has, and if confirmed, I would 100 percent commit to doing everything I possibly can to make sure that you get all of the information that you need to perform those important oversight roles.

Senator PORTMAN. Thank you. We will hold you to that.

Mr. Inglis, we also sent a letter to the Federal Chief Information Security Officer (CISO), as opposed to CISA—this is OMB—on April 5th, which asked about the accountability for Federal cybersecurity, an issue, as you know from our conversation, I have a lot of interest in. All we have received to date is a list of public websites. That is it. Does that seem like a timely and sufficient response to you?

Mr. INGLIS. Senator, I similarly, if confirmed, commit to providing the Committee with all of the resources and insight required for them to do their duty. We know that the Senate is a principal source of authorization and resources necessary. Without insight into that specific kind of request, not knowing what the question is, I am unable to comment on that, but only to say that it does not sound correct and that, if confirmed, I will work to accommodate—

Senator PORTMAN. Thank you. I ask unanimous consent (UC), Mr. Chairman, that we submit for the record the letters¹ we have sent and the redacted page behind me.

Just personally, I need to know from all three of you, you are going to be more responsive. We are trying to work with you and do our work.

Ms. Carnahan, GSA has a lot of responsibilities. One, of course, is with regard to procurement. If confirmed, how would you increase Federal agency usage of GSA schedules and government-wide acquisition contracts for procurement?

Ms. CARNAHAN. Yes, thanks for that question, Senator. I am very interested in making GSA's services more user friendly. I know and I have talked to businesses that have tried to get on GSA's schedules. They have told me about how difficult that process is. I am interested in learning more about how we can streamline that. It creates more competition, and it creates good jobs in our country if we can get more people able to sell through the government and GSA schedules. Likewise, we need to make it easier for agencies to be able to buy through GSA schedules and make sure we are getting them the best price and the best value.

I am very interested in this topic, Senator, and look forward to working with you more on—

Senator PORTMAN. Good. I appreciate that. I think you are absolutely right; improving the user experience is key, and your commitment to it is appreciated.

During COVID-19, as you know, the government had waived certain requirements in order to move more quickly to acquire goods and services to respond to the pandemic. My question is for you: Why shouldn't we continue to waive these requirements for the urgent and critical non-pandemic contracts?

Ms. CARNAHAN. Thanks for that question. I will tell you, Senator, I am not familiar with all of the waiver requirements and waiver rules that were put in during the pandemic. But I think it is worth figure out how we can streamline and speed up the process. I think it is cumbersome now. I think it can be better. We know what good marketplaces look like. There are security and other kinds of impli-

¹ The letters submitted by Senator Portman appears in the Appendix on page 266.

cations that we have to think about all the time, but I am very committed to trying to make this work better.

Senator PORTMAN. We would appreciate working with you on that, particularly given the opportunity we have post-COVID. We have had this experience during COVID that worked pretty well and would help in terms of that responsiveness.

On accountability, again, this is an issue that I think is a deep concern of not just mine but a lot of Members of this Committee. In the Federal Government, we have CISA and Jen Easterly is up for the CISA confirmation. We have CISO at OMB. We haven't had the National Cyber Director. Mr. Inglis is the nominee for that job. We also have the Deputy National Security Adviser for Cyber. All have not just roles in cybersecurity but coordinating roles in cybersecurity.

I am concerned about the overlap. I am concerned about the duplication leading to a lack of accountability. I noticed in the conversation earlier, Mr. Inglis, you talked about the job is one of encouraging coherence, unity of purpose, partnership with the private sector. CISA talked about partnership with the private sector. You talked ensuring a national strategy. You talked about this being sort of like a coach, Ms. Easterly, the role that Mr. Inglis would play, if confirmed, and that you were the quarterback. What is CISO? Is CISO the running back? What is the Deputy National Security Adviser? Is that a defensive player, a linebacker?

I mean, really, all joking aside, I think we have a real opportunity here with real experts coming into these jobs to be able to be sure we are not duplicating efforts and, frankly, without accountability, no one is in charge. So ultimate accountability, if everyone is in charge, no one is in charge. So can you speak to that briefly, Ms. Easterly?

Ms. EASTERLY. Yes, Ranking Member Portman. Thank you very much for that question because I do think it is incredibly important.

As I said in my opening statement, cyber is and has to be a team sport, but I 100 percent agree with you that accountability is critical. I come before you as the nominee for Director of CISA. If I am confirmed, I would expect you and Secretary Mayorkas and the Committee to hold me accountable for the very specific operational mission that CISA has to manage and mitigate risk to our digital and physical critical infrastructure and resilience, working with all of our partners. So that is what I would expect to be held accounts for.

Senator PORTMAN. OK. In the wake of the Colonial Pipeline hack, we have a lot to talk about. They did not even manage to work with you guys. They reached out to the Federal Bureau of Investigation (FBI). The FBI reached out to your prospective new agency. I mean, if that is your responsibility at CISA, should you be confirmed, it does not seem to be working very well. We have lots to talk about, and I know, Mr. Inglis, you and I talked about having a whiteboard exercise where we can actually see all these different roles. That does not include all the roles at the agencies where there is also accountability. We look forward to working with you on that, but I would like a commitment from you all today that you will help us to ensure that we have the right people in the

right place and that we are not overlapping responsibilities so that we can more effectively provide both the defense and the offense on cybersecurity.

Thank you.

Ms. EASTERLY. I commit to that.

Senator PORTMAN. Thank you.

Mr. INGLIS. I do as well, Senator.

Senator PORTMAN. Thank you.

Thank you, Mr. Chairman.

Chairman PETERS. Thank you, Senator Portman.

The Chair recognizes Senator Carper for your questions.

OPENING STATEMENT OF SENATOR CARPER

Senator CARPER. Thanks, Mr. Chairman. Can you hear me?

Chairman PETERS. I can hear you just fine.

Senator CARPER. I just want to say a special welcome to each of our witnesses, and especially to Robin Carnahan, with whose father I served as a Governor together. We were Governors together. We actually ran for the U.S. Senate together. He was killed in a fatal plane crash, very sadly, during the course of that campaign. Her mother went on to become a Senator from Missouri for a period of time, and so I have had the pleasure of serving with Robin's Dad as Governor and with her mom as a U.S. Senator, and we are thrilled that you have been nominated for this position. I look forward to being able to support your nomination.

Robin Carnahan and I discussed, colleagues, the intersection between GSA and the Government Accountability Office (GAO), and how GAO puts out at the beginning of every 2 years, at the beginning of a new Congress, the High-Risk List, high-risk ways of wasting money, and gives us a whole laundry list of things that we can do to save taxpayers' money and draw on bipartisan support for doing so. The High-Risk List includes things like real property management, IT acquisition management, just to name a couple of things on the GAO High-Risk List.

Ms. Carnahan, would you please take a moment to discuss your plans for working with the Comptroller General, who is now Gene Dodaro—I call him “Comptroller General for Life”—to address these and other high-risk areas where GSA can make meaningful progress? Please go ahead.

Ms. CARNAHAN. Yes, thank you, Senator, for those kind words about my father and mother and also for that question. I have lots of respect for the GAO and the oversight role that they play in all of these things. I think more eyes on these projects and thoughts about how they can be improved make sense.

I know with respect to some of the high-risk topics that you mentioned, GSA has made some progress by following some of the GAO recommendations and getting the leasing segment off the GAO High-Risk List. But there are more that are left. My interest would be sitting down with the GAO to talk about how we can implement some of these recommendations and, frankly, understanding what the blockers have been to getting that done sooner.

Senator CARPER. Let me just interrupt and say I think that is a great idea. When I was privileged to chair this Committee, Senator Tom Coburn I think was the Ranking Member, there was a

woman named Jane Holl Lute, who was the Deputy Secretary of Homeland Security, and that was at a time when Homeland Security led the hit parade in things, we were wasting money, badly managed, bad morale, and Jane Holl Lute, the Deputy Secretary for Janet Napolitano, who was the Secretary, she would go meet with Gene Dodaro and the team at GAO literally every month and say, "How do we get off your High-Risk List?" They would just literally go through the list. It was sort of a personal approach, but a very deliberate approach. And you know what? They got off the High-Risk List before the end of this administration. It actually worked.

I like to say find out what works and do more of that, so I would urge you to—if you do not know Gene Dodaro already, get to know him. He and his team do great work. I think you will find him a good partner.

Ms. CARNAHAN. Thank you, Senator.

Senator CARPER. For Colonel Easterly, I am a Navy guy. Navy salutes Army, and they are proud of your history and your service, two Bronze Stars, as I recall. Not many people I know can claim that. But as I was going through your written statement, I came across something where you referred to Tom Kean. I am a former Governor of Delaware; he is a former Governor of New Jersey. I have huge respect for him, and he was the Co-Chair, of the 9/11 Commission. But I think you mentioned in reference to the 9/11 Commission a quote from him. Former Governor Tom Kean said, "We did not grasp the magnitude of a threat that had been gathering over a considerable period of time. This was a failure of policy, of management, of capability, and, above all, a failure of imagination." That is his quote, the Co-Chair of the 9/11 Commission, Republican from New Jersey.

In light of that quote, Ms. Easterly, I want to ensure our country is adequately addressing the magnitude and the severity of the increased cyber and ransomware attacks we are grappling with today. I would ask you, Ms. Easterly, how would you propose to work to improve our Nation's cyber posture in the role of CISA Director to ensure we have strong policy management and capabilities to address the increased cyber threats we are facing?

Ms. EASTERLY. Thanks very much for that question, Senator, and thank you for your service to the Nation, particularly your time in the Navy.

If confirmed, I would focus initially on three major things to ensure that CISA has the capacity and capability to execute its very complicated mission. First, I would ensure that CISA has the right resources to execute that mission, and that is people, its authorities, and its budget. Most importantly, I would say people. I think the quality of the workforce is incredibly important to be able to effectively execute the mission.

Second, I would ensure that CISA has the operational and technical visibility that it needs to be able to effectively defend Federal Government networks. We know if you cannot see it, you cannot defend it. So that is absolutely critical.

Third, I think it is absolutely fundamental for CISA to have the right partnerships to make it successful. We know that CISA is really an agency of partnerships, and its success is highly depend-

ent on the quality of those partnerships, whether that is State and local, tribal, territorial, whether that is partnerships within DHS, across the Federal Government, or the very important partnerships that CISA has with the private sector. So incredibly important to focus on resources, on visibility, and on those partnerships if I am confirmed, Senator.

Senator CARPER. Good. Thanks for that response.

Mr. Inglis, Ms. Easterly, same question for both of you, and that would be: How will each of you work to select, recruit, and retain a talented cyber workforce? How do you believe your past working experiences will serve you well in your new roles, if confirmed? Mr. Inglis, would you go first? Then Ms. Easterly. Just be fairly brief, if you would, Mr. Inglis.

Mr. INGLIS. Senator, thank you for the question. I think, first, in order to recruit to a workforce, you need to inspire them to come to a mission. You need to be very clear about what the purpose is and how they can make a difference to that. That culture is absolutely essential.

You need to then make sure that that workforce is not simply fit for purpose, but that broadly across that workforce it is sufficiently diverse that you will have the benefit of all the perspectives that are necessary.

Finally, you need to give them a viable career path. You need to ensure that you have accounted for their aspirations to do something more than what perhaps might be the opportunity of the moment. And to the extent that they can have agility and longevity in that career and you give them that feedback and you give them those investments, they will come and they will stay, and they will exceed your expectations.

Senator CARPER. Mr. Chairman, could I have 30 seconds maybe for Jen Easterly to respond to the same question, please?

Chairman PETERS. Without objection, yes.

Ms. EASTERLY. Thanks, Senator. A very important question and a personal passion of mine. Three things.

One, culture, as Mr. Inglis mentioned. Leaders need to create a culture that prizes collaboration and innovation and inclusion and ownership and empowerment. A good culture is key to being able to attract the best talent.

Second, you have to look at this not as a one-off position but as part of a talent ecosystem from recruiting to onboarding to integration to training and certification to rewards and recognition and promotion as part of a whole ecosystem to allow you not just to attract the best talent but also to retain the best talent.

Finally, you need to be relentlessly creative in using various different approaches to tap into a diverse pipeline of cyber talent, whether that is through internships, through apprenticeships, through expanding the cyber corps program, through reserve programs, through rotational programs, and then creating corridors with the private sector to enable easier passage so that you can bring in more private sector people to help to strengthen the connective tissue between the private sector and the government.

Senator CARPER. Very thoughtful responses from both of you. Thank you so much.

Thank you, Mr. Chairman.

Chairman PETERS. Thank you, Senator Carper.

I am going to need to step away briefly. The Senate Armed Services Committee (SASC) has a hearing with the Secretary of Defense and others that I need to go to to ask a few questions. Senator Padilla, you will be taking the gavel and the Chair. As the Senator comes up here to take the gavel, Senator Lankford, you are recognized for your questions.

OPENING STATEMENT OF SENATOR LANKFORD

Senator LANKFORD. Chairman, thank you very much.

Thanks to all of you from going through the process on this. I want to first say about the workforce issue that you were just talking about with Senator Carper as well, Senator Sinema and I spent a lot of time working on this issue, on the hiring. We obviously have great complications in the process. We are still over 100 days in hiring in the Federal workforce. There are lots of issues with bringing interns on as interns and then moving them to actually hire. What is common in the workplace is uncommon still in the Federal workplace. All those issues, as you rise up and start to reach out to people, please stay engaged with us and with our Committee in the days ahead. It will be essential that we make sure that we are removing barriers from the process.

Senator Peters and I have even worked for a while on dealing with some of the specialists in NASA and trying to figure out how to get a pilot project there so they can continue to be able to tap into some of the scientists. You will run into barriers in trying to get some of these professionals. We make sure that we are clearing as many of those as possible. But that is going to require communication among our teams to be able to do that. We invite that kind of communication so we can make sure that we are clearing the path.

I do want to ask a question that involves all three of you, and it is a point of connection for all three of you. Ms. Carnahan, I want you to be able to answer this first. I am going to take you back 7 years ago. This Committee was working with GSA to identify a vendor that was on the GSA approved list named "Kaspersky." At the time the GSA had approved them as a software package and said this is approved software. Many agencies were using it. More and more evidence came out that Kaspersky was housing the information that they were harvesting from users in Russia and were filtering those, and it became a pretty rapid issue of how do we actually get Kaspersky out of our system.

This is an intersection of all three of you in this process to deal with a vendor on multiple agencies to be able to identify who is a qualified vendor, who is a hostile vendor that is out there like Kaspersky clearly was, and how do we actually make sure that that does not happen that they get into the system, because at the time we were then trying to figure out with GSA how they would unwind, how agencies would switch virus protection to a different one, and how we could actually pull that out and replace and what is a decent vendor in this.

All three of you would have to be engaged in that at some level to make sure we do not get vendors like that. I would like to ask

how we are going to deal with the integration to be able to deal with it? Ms. Carnahan, you are up first.

Ms. CARNAHAN. Thank you, Senator, for that question. I will tell you that I see GSA's role here as really twofold: one, staying very tightly and closely coordinating with CISA and the National Cyber Director as they set policy and identify these threats. The main thing we all need to understand is that threats are not static. They are going to be changing all the time. And GSA's role in all of this is to be the implementing partner. We are the ones who will be helping agencies get the secure tools that they need and the services that they need, and they have to be always evolving with the evolving threats.

So my interest is making sure that GSA is using the best practices for the private sector and changing with those threats not being static and automating as much as we can to be able to continue to monitor the threats. I look forward to working with you more on that, but that would be my general approach to this.

Senator LANKFORD. Ms. Carnahan, I would say one of the challenges we will face will be trying to be able to go through that process in a timely manner, because we do not want every one of our agencies to all just have 3-year-old software by the time we actually get through all the approval process as well. So it is going to be the coordination, I completely agree, but also a timely process as well.

Ms. Easterly.

Ms. EASTERLY. Yes, Senator, thanks for the question. Hugely important. Could not agree with you more on the need to have rigorous and accelerated processes in place to ensure the security of the supply chain from foreign nation-state threats.

Two things that CISA does in this space that I am aware of. First, it hosts an Information and Communications Technology (ICT) supply chain risk management effort between the public and the private sector to work on recommendations for ensuring the supply chain. I think more importantly, though, CISA is a member of the Federal Acquisition Security Council (FASC) that was, of course, created by this Committee in 2018. That is a hugely important capability that I think came out of the Kaspersky piece to enable dangerous products that could present security threats to be excluded or removed from software.

I agree with you that as that is done, it needs to be done in a way that keeps up with the pace of technology. If confirmed, I look forward to advancing both of those efforts along with the GSA Director as well as the National Cyber Director and other key stakeholders.

Senator LANKFORD. OK. Thank you.

Mr. Inglis.

Mr. INGLIS. Senator, if confirmed, the National Cyber Director, I believe, must be committed to advocating the techniques, the mechanisms you have already heard described I think thoughtfully and well from the prospective head of GSA and the prospective Director of CISA. Also, these issues transcend cyber. I think you have thoughtfully pointed out some of the cyber relevant issues and would argue in some cases against the use of this technology within either the Federal enterprise or the kind of U.S. larger cyber en-

terprise. But there are issues of economic fairness as to whether these are level playing fields that foreign competitors are playing on and whether we should stand in to perhaps adjudicate and render a perhaps level playing field for the benefit of U.S. industry.

There are issues of legal perils that might not be directly injected into these systems because of some back door but, rather, because a legal system in another country that has access to this information can access it under something that we do not find suitable for our probable cause standard. That then moves this to a higher level where the National Cyber Director would be expected to participate in the National Security Council to bring to bear all the instruments of power to understand how do we render a level playing field for these systems and remove them when they are not in the U.S. interest.

Senator LANKFORD. OK. Thank you.

Ms. Carnahan, quickly, I want to be able to bounce a very complicated question off of you, and I am sorry for the short time on it. We can talk at greater length at another time also, but that is the issue of real property and our moving out of COVID-19 time period where we will have the Federal workforce returning back to buildings, but we will also have a significant number of the Federal workforce that will start working remotely permanently. We found a lot of flexibility in a lot of offices, and they are going to find ways to be able to say we could hire more people in more places and we will need less footprint of actual space.

You are in the difficult position, if confirmed in this, to have to manage that transition of work space while agencies are trying to also figure out how many more people they are going to have remote. How are you planning for that, thinking through that?

Ms. CARNAHAN. Thanks for that question, Senator. It is a very big deal for the Federal Government, just as it is a big deal in the private sector. The pandemic changed the way all of us did business and really is going to, I am sure, cause agencies to be rethinking how they want longer term to implement remote work and what the options are. That is going to impact their physical space needs.

I think as you said it is a great opportunity to think about how to right-size the Federal footprint of real estate and do that at a time where we can be smart about understanding the marketplace and where it is going and what future needs are going to be. I look forward to this. I, like you, think this is a big opportunity to rethink what our Federal Government looks like, what the future is going to look like. I know that there are task forces that are underway right now with OPM and OMB and GSA to think about all of these issues, and I look forward to seeing what they come up with and talking to you and other Members of the Committee about this, because I think this really is a long-term issue that we are going to be dealing with in the government, and we need to get it right.

Senator LANKFORD. It is exceptionally important, but the real property management has been a problem for GSA for quite a while. This is a fixable problem, but it has definitely been a problem. Another one I will talk about and put in a question for the record is the relationship between GSA and Customs and Border

Protection (CBP) on those Ports of Entry (POE), because that has been a point of frustration for a long time because CBP is pretty frustrated how the ports of entry are managed. They will say, “We are not a courthouse. We are not an agency building the same way that we are a port of entry.” That is a relationship we have to be able to work out in the days ahead.

Thank you, Mr. Chairman.

OPENING STATEMENT OF SENATOR PADILLA

Senator PADILLA [presiding]. Thank you.

For Members watching, it is my opportunity to ask questions next, followed by Senator Scott. Thank you to the witnesses and folks before us today.

I want to start by talking about my experience for the prior 6 years before my appointment to this body in January. I think we all agree that our right to vote is indeed the foundation of our democracy. Prior to joining the Senate, I served as California’s Secretary of State and helped oversee the 2020 election, and not just in that cycle but in prior years I saw firsthand CISA’s commendable work, particularly through the Project 2020 Campaign. Election cybersecurity, like all cybersecurity in all sectors, is certainly a work in progress.

In 2020, we learned about specific vulnerabilities highlighted in the 2016 election and were able to take actions to defend against those. But from this last election cycle, we learned specifically how dangerous it can be for election security to become politicized.

My first question is for Ms. Easterly. How are you thinking about CISA’s election security work and the challenge of ensuring the agency’s work is viewed as apolitical?

Ms. EASTERLY. Thank you for that question, Senator, and thanks again for your incredible leadership during 2020. As we know, fair and free elections are critical to the fabric of democracy, really foundational, and the American people’s belief that their vote is going to be counted is largely reliant on the security and resilience of election infrastructure.

As we know, State and local officials administer those elections. CISA’s role is to be a strong partner in this space to ensure that election officials have the resources, the technical guidance, the threat information sharing, and the assessment support that they need to be able to ensure the security of those elections.

I have had conversations with folks at CISA that worked as a part of that effort in 2020, and I think it was a real bright spot, as you pointed out. I have also had an opportunity to speak with some of the executive board of the National Association of Secretaries of State and know how important it is that CISA is seen as a nonpartisan, apolitical agency because CISA needs to be seen as an enabler for all Secretaries of State and all officials, regardless of party.

I would make it a very early priority to start building those relationships off the back of the superb relationships that Chris Krebs developed as the Director and would make that a significant area of focus.

Senator PADILLA. Thank you.

Mr. Inglis, a similar question. Your position is a new one, and so how would you see the role of National Cyber Director when it comes to election security specifically?

Mr. INGLIS. Senator, thank you for the question and for the opportunity to follow Ms. Easterly in answering that question. I think she gave an excellent answer. I think first and foremost I would fully support all of what she said in terms of the nature of the Federal Government's relationship with the States and locales who actually conduct those elections.

The National Cyber Director needs to make sure that at any moment in time that we have a viable strategy to effect that support that we can render the support, the assistance that is necessary and appropriate to those who conduct these elections, who execute these elections. That needs to ensure that not simply CISA has the resources necessary to do their job, but that the FBI, the intelligence community, the other resources the Federal Government can bring to bear can detect threats to those election systems, both in the technology and perhaps in the constitution of that threat from perhaps foreign entities, and that all of that is provided so that we can render the social contract between the Federal Government, the States, and the locales on something that is intact and sustained.

Senator PADILLA. And that actually anticipates my next question. We know that in order to defend our networks, we need both a robust community of cybersecurity professionals in government as well as a shared sense of responsibility to practice good cyber hygiene. Research points to a gap between the cybersecurity capabilities we need in the United States and those we currently have. According to the 2020 ISC Cybersecurity Workforce study, the U.S. cybersecurity gap is still a staggering 359,000 employees. When the Federal Government does hire, we have a lot of work to do to be able to retain cyber talent.

I want to pose a question to all three of you, and the question is this: What has been your experience in recruiting talent? How do you plan to recruit and retain cybersecurity professionals? We will start with Ms. Easterly, then Mr. Inglis, and then Ms. Carnahan.

Ms. EASTERLY. Thank you, Senator. Very important question and a real passion of mine. As you point out, the cyber workforce is lacking in a significant number of personnel, both within the Federal Government as well as within society, writ large. The approach that I would take is very similar to what I have been doing over the past 4½ years, building a team virtually from scratch to help defend Morgan Stanley in this very complex cyber threat environment.

A couple key pieces that I think we need to recognize.

First, culture is foundationally important. You have to build a culture of excellence that prizes inclusion, innovation, collaboration, empowerment, and ownership so that people wake up in the morning and they love what they do and they enjoy their teammates and they like who they work for. That is how you attract the best talent and retain the best talent.

Second, you need a talent ecosystem that treats a job not as one-off but as part of a career development strategy, so you look at re-

cruiting all the way to training, certification, promotion, retention, all of those things together as part of the ecosystem.

Finally, creative approaches, all different approaches to be able to tap into highly diverse pipelines of talent.

I think those are the three tenets that I would leverage if I am confirmed.

Senator PADILLA. Thank you.

Mr. Inglis.

Mr. INGLIS. Sir, I would only add to Ms. Easterly's very thoughtful answer and I think comprehensive answer that we have found that the pipelines are not generating enough, either in the diversity or in the literal numbers. We need to actually work those pipelines. We need to start as early as possible, K through 12, in creating awareness on the part of those up-and-coming students about what the possibilities are to take on very viable careers. If we meet their needs with the qualities that Ms. Easterly described, then I think we will find a greater number kind of come into those systems.

I think we also need to revisit what the fundamental qualifications are to take one of these jobs. Not all of them require a Bachelor of Science (BS) in computer science. Many of them simply need good, critical thinkers, people who have a good work ethic, and we need to open the doors for them to make their way into these jobs such that they can make an immediate and positive difference.

Finally, we need to have some flexibility such that if you are hired into a job in one place, you are a candidate to take in any number of other places, and you see yourself as part of a larger community, an ecosystem where you can flow back and forth and everyone benefits from the diversity of experience that we then accrue.

Senator PADILLA. Ms. Carnahan.

Ms. CARNAHAN. Yes, thank you for that question, Senator. I worked actually on a tech team inside the government, and it was fascinating to watch how they were able to recruit talent. I think that there are ways we can do this just by being smarter.

One is we need to streamline human resources (HR) practices to make it so we are actually defining jobs as they are defined in the private sector, not as how they are defined in government, so people know what roles might make sense for them.

No. 1, we need to make use of remote work. That is a thing that is attractive to lots of people in the technology industry, not to have to pick up and move to another city or to move to Washington in order to do the important work.

No. 2, if we promote this as tours of duty in government so that they can get good experience and serve their country, it turns out that folks in technology and cybersecurity are patriotic and want to figure out ways to serve their government as well. So we should give them that opportunity.

Finally, I think the way you recruit is you talk about the impact. We often hear in government that you cannot afford people, but it turns out people will do a lot to serve their country, and if they know it has an impact on people, they are willing to do that as well.

I think there are some very practical things that we can do to recruit talent, and we need to get on it right away.

Senator PADILLA. Thank you very much.

Senator Scott has yet to arrive, so we will turn to Senator Hassan followed by Senator Hawley.

OPENING STATEMENT OF SENATOR HASSAN

Senator HASSAN. Thank you so much, Senator Padilla. Good morning to all three of our nominees. Thank you. I thank your families for your willingness to serve. Thank you for your expertise and your patriotism.

I want to start with a question to you, Mr. Inglis. I would like to follow up on a discussion we had in our prior meeting. It is clear that we have to work together to strengthen public-private cybersecurity information sharing, especially in light of the recent SolarWinds, Microsoft Exchange, and Colonial Pipeline attacks.

In your view, what are the biggest barriers inhibiting effective cybersecurity information sharing in both directions between the private and public sector? If confirmed, are there changes to the current information sharing framework that you would recommend?

Mr. INGLIS. Senator, thank you for the question, and thank you especially for the conversation we had, which I found quite enriching to my own understanding of some of these challenges.

With respect to information sharing, I think that that is a very important dimension of public-private collaboration, but often that fails because that is all we do, is share information. We do not share perspectives. We do not share what perhaps might be a hunch or an insight on one side of an otherwise stovepiped organization to another and, therefore, not feeling we have common cause, not sharing insight as opposed to simply information. We find that we disappoint one another. What you give me or what I give you is not as useful because I lack the context.

I think, therefore, we need to create common cause. We need to lower the boundaries, share at the lowest possible level, not after we have a well-formed idea but to put people shoulder to shoulder on floor plates where they can co-discover and co-mitigate threats on the fly. To the extent that we do that and we provide mutual advantage, the government to the private sector and vice versa, I think you will find that those relationships will take off and that they will then be self-sustaining and they will grow.

Senator HASSAN. Thank you. I really look forward to working on that with you.

Ms. Easterly, FBI Director Chris Wray recently indicated that the Bureau would be escalating the fight against ransomware and stated that disrupting and preventing ransomware attacks is a shared responsibility all across government agencies. However, the Federal Government only successfully prosecutes a small fraction of cyber criminals each year.

If confirmed, how would CISA work with law enforcement agencies such as the FBI to increase costs and deterrence for cyber criminals?

Ms. EASTERLY. Thanks for that question, Senator. I think as we heard earlier this week from the CEO of Colonial in dealing with

that incident, they reached out to the FBI, and the FBI immediately brought in CISA. I know some people look at that and say, “Well, the company did not call CISA,” but I actually think it is a tribute to those very strong collaborative relationships within the Federal Government that the FBI immediately brought in CISA. I think those relationships have actually evolved over the past couple years, and if confirmed, I would look to strengthen them.

We understand that the FBI’s role is, of course, from an investigation and a pursuit perspective. CISA’s role is to ensure that all the key stakeholders at the State, local, Federal, non-Federal, private sector have the guidance and information and resources that they need to be able to prevent such attacks.

We know at the end of the day a lot of this comes down to the basics of cyber hygiene, passwords, multifactor authentication, and so these basics are absolutely critical to be able to get out the information that is needed so that folks know how to protect themselves.

Senator HASSAN. Thank you. It is also important to note that Colonial said that it had not actually planned for a ransomware attack. It had planned for some other things, but not that, so we have some work to do.

Ms. Carnahan, when we met a few weeks ago, you remarked this is, I think, a quote from our conversation “The future of service is digital.” But the COVID-19 pandemic revealed just how many Federal agencies are not equipped to offer digital services due to their use of expensive outdated technology and paper-based data systems.

For Granite Staters, this meant significant delays in delivery of stimulus checks and the inability to access emergency funding to support their small businesses.

How will you proactively assist agencies in achieving their IT modernization goals and in turn save taxpayer dollars by reducing their reliance on outdated legacy IT systems?

Ms. CARNAHAN. Yes, that is a great question, Senator, and I enjoyed our conversation. I have lots of thoughts about this. As you know, I come from a State government perspective as well, and I watched, just as all of us did, horrified, that so much of the quick policy work and appropriation that was done by Congress was not able to get to the people that needed it because of outdated or not-working technology systems; and, likewise, that cyber criminals were able to take advantage of that and steal money.

Bottom line, if we cannot implement government policy, if we cannot make the damn websites work, I think that is my bottom line. We have to get that right. I want to ensure that we both serve people well and do that in a way that is a smart investment of money. I will also add that many times people think, if we are going to upgrade technology systems, it is going to cost a fortune, and it is going to take forever. What we know is that you can incrementally improve these systems, and you can do it for less money. It really is about focusing on the value that we are giving to users and also doing that in a way that is smart for taxpayers. I am very interested in getting your thoughts on this and getting started.

Senator HASSAN. I thank you, and I think one of the reasons to do this, too, is to your point about making sure that people under-

stand that their government can work for them. They need to be able to get the same level of service from their government that they get from the private sector digitally. I look forward to working on this issue with you as well.

Ms. Easterly, I have been particularly concerned about cyber attacks against State and local governments and entities. In your view, should the Department of Homeland Security provide more resources to State and local governments to improve their cyber posture?

Ms. EASTERLY. As a private citizen, I do not have a good sense of the resources that are being provided right now, but I absolutely agree with you on the importance of partnering closely with State and local so that they do have the resources to protect themselves. I think the addition of a cybersecurity coordinator at the State level was an important enabler there, and if I am confirmed, I will make that a priority to develop, continue to develop those partnerships.

Senator HASSAN. Thank you. Would you support creating a stand-alone cybersecurity grant program for State and local governments?

Ms. EASTERLY. At this point in time, Senator, I do not know much about that, but it certainly seems to make sense. I think grants are a very important vehicle to allow State and local to have the resources that they need to defend themselves. If confirmed, I would love to be able to learn from you more about that and to work with you on it.

Senator HASSAN. Thank you. Mr. Chair, I will turn my time back, but I would look forward to a deeper conversation with both Ms. Easterly and Mr. Inglis, too, about the appropriateness of apprenticeship programs as a way to really build our cyber workforce, and I look forward to that conversation.

Thank you, Mr. Chair.

Senator PADILLA. Senator Hawley.

OPENING STATEMENT OF SENATOR HAWLEY

Senator HAWLEY. Thank you, Mr. Chairman. Thanks to all the witnesses for being here. Congratulations on your nominations.

Ms. Carnahan, if I could just start with you, I enjoyed your conversation, I guess it has now been a couple of weeks ago. Congratulations on your nomination. I want to follow up on this important issue—you and I talked about it—of Federal procurement, so important to what GSA does and the Federal Acquisition Service, which is an important part of GSA's work.

Give me a sense of what role you see for GSA in ensuring that we protect our procurement process from security risks. What I am thinking here specifically—and we talked a little bit about this—is the threat from Chinese-based telecommunications products in government networks. What is your view on how to protect our procurement process from those kind of risks?

Ms. CARNAHAN. Thank you, Senator. I share your urgency about this issue and understand that Congress has been very clear about the dangers from both telecommunications equipment and other things under the National Defense Authorization Act (NDAA). I think it is important that GSA get on with, as the chief buyer,

strengthening the supply chain to ensure that it is complying with Section 889. My understanding is that it has worked on that, but in the end, there is no excuse for not just getting it done.

I do not know what the blockers are currently to having this fully implemented and enforcing these rules, but if I am confirmed, I am going to be interested in, as quickly as possible, getting to bottom of that issue.

Senator HAWLEY. Great. Thanks very much. I look forward to working with you on that.

Switching topics, I have been a big advocate of reopening the Federal agency field offices to ensure that our fellow Missourians and other folks around the country can get the services that they rely on and that they need. GSA, of course, operates a huge property portfolio that include many of those field offices.

Give me a sense of what role you see for remote work going forward. You have mentioned this a time or two today in your testimony, but what role do you see for remote work? What kind of balance do you think we need to strike between in-person work so folks can come in and ask their questions, get the information they need, get answers, and then the remote work for Federal employees. Tell me how you would strike that balance and what your view is there.

Ms. CARNAHAN. Yes, it is a great question, and I think it is something that the government is trying to get a handle on as well as private businesses. I think the pandemic has changed the way a lot of people are thinking about this, and it is certainly changing the way how government is thinking about it.

I know that GSA is currently in the mix with a task force on both reopening, but also the future of work and what that is going to look like. I will look forward to learning more about what that task force comes up with. I am not privy to that right now, but my sense is a lot of these agencies are going to be rethinking how many people need to be onsite, how many people need to be in buildings, and it is all going to be based on the mission. I think that is going to be different from one agency to the next, and our job at GSA is going to be just responding to agencies' needs as their workplace needs change.

I know it is a big topic, and I will be spending a lot of time on it, and I look forward to getting started.

Senator HAWLEY. Very good. Thanks very much.

Ms. Easterly, let me turn to you, if I could. We had the CEO of Colonial Pipeline before the Committee earlier this week. I was troubled, to be honest with you, about his lack of transparency over how much Colonial has invested in cybersecurity and just the steps that they were taking proactively before the most recent crisis in cybersecurity.

Do you think that we have currently adequate accountability for private sector companies in place?

Ms. EASTERLY. It is a great question, Senator. Thank you. I do not have a sense across the board in terms of accountability. I currently work in the financial services sector, and I think there is strong accountability there because of our regulatory framework. But I do think accountability is incredibly important for cybersecurity standards across the board.

Senator HAWLEY. Do you think that the Federal Government needs to require more of companies that operate critical infrastructure? For example—and I asked the Colonial CEO about this—until last month, I think the TSA reviews were optional, were voluntary. Do you think we need to impose new cybersecurity standards for companies that, again, in Colonial's case really are almost public utilities, serve 100-million-plus Americans; 16,000 different service stations were fueled, or not, by Colonial Pipeline fuel. What is your view about the level of standards that we may need to require?

Ms. EASTERLY. I think that is a great and important issue. I do not have a sense across the board, but it seems to me that voluntary standards are probably not getting the job done and that there probably is some sort of role for making some of these standards mandatory, to include notification. I do think it is important that if there is a significant cyber incident, critical infrastructure companies have to notify the Federal Government, in particular CISA. We have to be able to warn other potential victims.

Senator HAWLEY. Yes. Mr. Inglis, you were nodding your head there. Do you want to add to this? I would be curious as to your view.

Mr. INGLIS. Yes, Senator, I would simply add I strongly agree with the premise of your question, which is that this is an important question and that at the end of the day we have to ensure that our critical services, our critical functions, that we have confidence that they will be delivered. There are generally three ways that the standards kind of can come about. One is enlightened self-interest. That is apparently not working. The second is market forces. That is apparently not working. The third is some imposition of standards or regulation on top of that. We begin to take some steps in that direction. It remains to be seen how we can achieve kind of the full flowering of the innovation that we still need in the private sector while imposing an expectation in the standards that go with that to ensure that those critical services can and will be delivered, even under duress.

I am a big fan on market forces as the primary way to essentially drive the economy, but we have to kind of examine that. If confirmed, I would be happy to work with this Committee. I certainly will within the Federal branch or the Executive Branch to consider the problem.

Senator HAWLEY. Very good. Let me just ask you, Mr. Inglis, here in the brief time remaining how you would assess the current organizational structure around cybersecurity governance within the Federal Government. There are lots of agencies, dozens that are involved in cybersecurity. Congress created CISA obviously in order to drive coordination. Is the current structure working, in your view? If not, what do we need to do differently?

Mr. INGLIS. Senator, thank you for the question. I think it is the question of the moment. I think that is in part why the National Cyber Director, by virtue of the work of this Committee, has been created, that we want coherence, we want unity of effort, unity of purpose. Without kind of detailed knowledge, having not been on the job—and, if confirmed it will be my first question—I cannot give you a detailed answer. I would simply observe the following:

that we have plenty of diversity, we have some deep and sharp strengths. We have strength in places like CISA, the FBI, the national agencies that do intelligence, and GSA. But it is not entirely clear that they are coherent, that we have achieved unity of purpose, that they are all operating according to a single strategy that would connect that diversity such that it becomes a strength.

I think that we can and should become greater than the sum of our parts. I am not sure that we are yet there.

Senator HAWLEY. Very good. Thank you very much for your testimony. Thanks to both of you and Ms. Carnahan.

Thank you, Mr. Chairman.

Chairman PETERS [presiding]. Thank you, Senator Hawley.

OPENING STATEMENT OF SENATOR OSSOFF

Senator Ossoff, you are recognized for your questions.

Senator OSSOFF. Thank you, Mr. Chairman. And congratulations to these nominees. Thank you for your attendance today.

We have rightfully spent a significant amount of time in this hearing discussing cybersecurity given recent events. I want to turn to that in a moment, but first, Mr. Inglis, given your long tenure at the National Security Agency (NSA), I would like to ask you, how do you view the role of National Cyber Director and what is your understanding from the White House about this role as it pertains to surveillance, as it pertains to decisions that you may have to make or weigh in one that balance privacy and national security needs domestically?

Mr. INGLIS. Senator, thank you for the question. I will just start by saying that in the context of surveillance, if by that you mean kind of surveillance by national agencies of various activities that we would want to know something about in order to defend networks of interest, we have authorities in place that restrict surveillance conducted by the government to very narrow lanes, and I think that is appropriate, and we should not take those walls down.

To the extent that that surveillance can be of a more general sort, which is can we combine the insights that the private sector might have, the network owners might have, the commercial providers who run analytics across these networks might have, with the knowledge the government has about, say, foreign threats, I think that is where we can make some progress and we can put those together. But we never, ever take down the barriers that have provided protection for privacy, for proprietary information, for classified information at the same time we pursue collective security.

Senator OSSOFF. Mr. Inglis, I appreciate that answer. I just want to drill down a little bit more on what I mean by surveillance here. Do you anticipate that in your capacity, should you be confirmed, as National Cyber Director that you will be involved in decisions regarding, for example, collection of phone records or meta data of U.S. persons or other data pertaining to U.S. persons under, for example, but not limited to, Foreign Intelligence Surveillance Act (FISA) or PATRIOT Act authorities?

Mr. INGLIS. Sir, as I understand the National Cyber Director's responsibilities, as the law lays it out, I would not expect to be in

those conversations. But I would be happy to answer questions based on my prior experience about those.

Senator OSSOFF. Thank you, Mr. Inglis. On that note, what is your personal view of the balance that the Federal Government has tried to strike between national security and privacy interests? If you could comment specifically on what has been referred to as the bulk collection of phone records and meta data under Section 215 of the USA PATRIOT Act.

Mr. INGLIS. Yes, sir, I think that is a very important question. I think we go back to the Preamble of the Constitution, which does not use the word “or” when it describes the aspirations of this Nation. We have to defend privacy at the same time we pursue collective security. We cannot choose between them. We then have to work harder to deliver both of them. Those are difficult policy issues each generation has to face. How do we reconcile the technology, the threats, to the aspirations that endure? So in my view, privacy needs to be on the table up front. It is not something we can deliver as an afterthought.

Senator OSSOFF. Do you believe that there has been overreach in the collection of data pertaining to U.S. persons since the enactment of Section 215 of the PATRIOT Act and other similar authorities?

Mr. INGLIS. Sir, if by that you mean the collection of telephone meta data that would have occurred in the early 2000s and say up through perhaps the middle-2000-teens, I think that looking back over our shoulder with hindsight as our experience that we have decided as a Nation that that program is no longer necessary and, therefore, no longer appropriate. My understanding of the program at the time—and I was responsible for implementing that program—was that it worked very hard to align the interests of privacy at the same time pursuing security, and there were any number of controls that were imposed on it in deference to privacy as opposed to the simple pursuit of security.

Senator OSSOFF. Thank you, Mr. Inglis.

Ms. Easterly, when we met prior to this hearing, you and I discussed our shared desire, I believe, to help promote a culture of privacy, attention to the protection of personally identifying information (PII), and cybersecurity more broadly through American society to increase our resilience and the responsibility we take as individuals to protect our data and data that could impact the privacy of our fellow citizens.

What role do you see for CISA in helping to build that broader culture of privacy and cybersecurity and good data hygiene? Will you commit to engaging with my office to determine how Congress can support such efforts?

Ms. EASTERLY. Thanks for that question, Senator. It is a very important one. CISA is an agency of partnerships with the Federal Government, non-Federal, and then with our private sector partners. I believe that CISA can play a very important role working with partners at every level to ensure that they have the information that they need to be able to strike that very important balance between privacy and security and, importantly, to deal with some of the malicious cyber attacks that we are seeing at every place in society to have that critical information that they need to ensure

that they have good practices of cyber hygiene that are well implemented.

I would really enjoy the opportunity, if confirmed, to be able to work closely with your office on how to make this a culture of national resilience because it has to be more than the Federal Government. It has to really be a societal level that, frankly, starts at the youngest of levels so that folks understand at the end of the day what it means to be a good digital citizen.

Senator OSSOFF. Thank you, Ms. Easterly.

Ms. Carnahan, my office has been inundated with requests for assistance from Georgians who, through no fault of their own, experienced job loss due to the COVID-19 pandemic and, despite meeting eligibility criteria to receive unemployment benefits from Georgia's Department of Labor (DOL), have experiences, long delays in the processing and payment of their approved claims, which has sent them and their families into financial distress in the midst of a pandemic. These payment delays involving Georgia's Department of Labor were detailed in a report released by the Georgia Budget and Policy Institute in February of this year, and according to that report, a reliance on outdated technology at Georgia's Department of Labor is one of the key factors contributing to these ongoing delays, which is leaving Georgians in hardship.

So will you please commit to working with my staff and using the authorities and expertise of the GSA to assist State and local governments in improving these processes, including specifically supporting improvement of Georgia's Department of Labor's unemployment claims processing system so that so many Georgians are not left without vital support in a crisis?

Ms. CARNAHAN. Thanks for bringing that issue up, Senator. This is something that has happened across the country. Georgia is not alone in this. I know it feels like it sometimes, but every State has had similar issues because these unemployment systems were, frankly, not invested in for so many years and then were overwhelmed. But that is no excuse, and now we have to think of this as an opportunity to rebuild better.

What we know is that these unemployment systems from one State to the next are very similar. They are more similar than they are different, and so the key here, Senator, I believe, is to help figure out how to think about shared services that do not have to be reinvented and rebuilt and paid for by taxpayers over and over again in every State and if there are things that we can do to help that collaboration.

I am very interested in this topic. I know GSA has the ability to have technical talent and some resources that can be supportive of both the Department of Labor and, to a lesser degree, States. I would like to be able to expand our ability to work with State and local governments because, frankly, Senator, from a citizen's perspective, they do not care which part of government serves them. They just want good service. From a taxpayer's point of view, if it is tax money from the Federal Government or State government, they want it well spent. I think it is GSA's responsibility to try to work on that.

Senator OSSOFF. Thank you, Ms. Carnahan.

Mr. Chairman, I yield.

Chairman PETERS. Thank you, Senator Ossoff.
 Senator Scott, you are recognized for your questions.

OPENING STATEMENT OF SENATOR SCOTT

Senator SCOTT. Thank you, Chairman Peters.

First off, for all three of you, thank you for your willingness to serve. You are not taking easy jobs, and, all these jobs are pretty significant. We have seen all these cyber attacks, and they can impact hospitals, businesses I used to be in, looking at the grid, looking at the Colonial Pipeline and all this stuff. I have friends of mine in business, and it has never become public, but they have been attacked and paid out unbelievable amounts in ransom.

One, do you think this is going to stop? Either of you, Ms. Easterly and Mr. Inglis, do you think there is any reason this is going to slow down?

Ms. EASTERLY. I agree with you in particular with ransomware, but cyber attacks more broadly, we are now at a place where nation-states and non-nation-state actors are leveraging cyberspace largely with impunity to threaten our privacy, our security, and our infrastructure. I think we really are at a moment that requires an all-hands-on-deck approach that leverages the talents and capabilities across the interagency. If I am confirmed at CISA, I will ensure that CISA does everything it can within its multitude partners to manage and mitigate risk. I think we do have an opportunity to bring the government together to work with our partners to make a difference in this space.

Mr. INGLIS. Senator, I would add to that. It will not stop of its own accord. It is not a fire raging across a prairie that, once it has consumed the fuel, it will simply stop and we can simply wait for that moment. We must stand in, and there is a range of activities that we must undertake. We must create resilience and robustness not simply in technology but in people. We must align actions to consequences. There should be benefits for behaving well and consequences of a negative sort for behaving badly. We should make this such that it is not simply a cyber-on-cyber problem. We should bring to bear all instruments of power in a hugely collaborative way across not just the private and public sector but nations, plural. Like-minded nations need to remove the sanctuary and bring to bear consequences on those who hold us at risk.

Senator SCOTT. Do you think it is doable? I mean, it sounds good—

Mr. INGLIS. I do think it must be doable. I do not think—so there is a really good discussion that takes place and this Committee has participated at length in it about whether deterrence is possible in cyberspace, whether we can—

Senator SCOTT. Right.

Mr. INGLIS [continuing]. Impact the decision calculus of adversaries in this space, and it often gets conflated with nuclear deterrence where kind of the job was to keep the nuclear weapon off the field. Thank goodness we have been successful in that.

Senator SCOTT. Right.

Mr. INGLIS. We are not going to be successful in that if that is the goal in cyber. What we need to do is to make these systems defensible. They will never be secure. We need to then defend

them. That is a human endeavor such that we can change the decision calculus of adversaries so we reduce it by 85, 90 percent. I am to understand that if we did two-factor authentication, something other than a password, if we did routine patching every Tuesday, if we built in segmentation fire breaks in our networks, 85 percent of the problem goes away. If we train our people, which are the vast majority of the weakness that adversaries take advantage of, maybe we can reduce that still further. Get it down to a reasonable kind of fire such that we can then manage that. It will never go away completely, but we can bring it down, we can bring it to heel significantly.

Senator SCOTT. Is there anything that Congress needs to do?

Mr. INGLIS. Sir, I would say Congress is doing it. Your investment in the authorities or the resources that we are having a discussion about today are an important part of that. The consultation between the Congress and the private sector that it serves and the Executive Branch that essentially derives its authorities and resources, that is important. That is vital. I would say that we need to continue that consultation. If confirmed, I know that the members at this table look forward to that continued consultation.

Senator SCOTT. Ms. Easterly.

Ms. EASTERLY. Yes, thanks for the question, Senator. I suspect there are probably things that Congress needs to do to help in this problem set. One of the things that I will look at very early on, if confirmed, is whether CISA itself has the right resources from a budgetary, a personnel, and an authorities perspective. I know that there is some discussion about FISMA reform to ensure that accountability is rightly structured. I know there is some discussion around whether there should be mandatory instant reporting. I think things like that are very important discussions to have, and if confirmed, I would look forward to working with this Committee on it.

Senator SCOTT. Who can take the leadership position to have the pulpit to get the private sector to do more? Because, I mean, Colonial Pipeline, a private company, but it impacted a lot of families, right? Who can do that? Whose responsibility is that, and who is going to do it, do you think?

Mr. INGLIS. Sir, I will start. I would say the private sector first is not a monolithic entity, and so you find great variance in terms of what influences the private sector.

Second, the private sector is influenced by quite a lot of activities, influences, or people. As I had indicated earlier, the private sector sometimes has enlightened self interest where they say that digital infrastructure is our business. It is not merely a commodity. And those tend to be leading the pack in terms of what they are doing to get ahead of this problem.

There are some that understand the market forces are going to drive them out of business if they do not prepare for this. Those market forces are beginning to have kind of a duly noted effect. But there are some that remain that do not think this problem affects them. It affects all of us, right? We are all in the boat. You do not need to be the target to be the victim. For them, when they are conducting critical activities upon which the Nation's interests depend, it may well be that we need to step in and we need to regu-

late or mandate in the same way we have done that for the aviation industry and for the automobile industry. I think it is going to be a combination of all those factors. The influence will come from many places. Ultimately, we have put people in place that ultimately are going to ensure that the system is working to that purpose. If confirmed, the National Cyber Director will have the responsibility to ensure to the President and to the Congress that the Federal cybersecurity strategy is the right one and then to oversee its implementation. We have had a rich discussion today here about what CISA's role would be, but there are so many other points of influence. We need to consider all of them and apply all of concurrently.

Ms. EASTERLY. The only thing I would add to Mr. Inglis' excellent answer, having spent the past 4½ years in the private sector at one of our critical infrastructure owners, is it is very important to have a coherence to the U.S. Government. I know sometimes when there is a threat stream or a vulnerability, there will be multiple outreach from different agencies, and I think it is incredibly important that the government is able to speak with one voice and that there is coordination across the board.

In particular, I think CISA as a trusted partner to the private sector can serve as a very effective front door. I think it then mandates that CISA is able to in near-real time share necessary information that comes in with the rest of the Federal Government to ensure that these problems can be addressed effectively. But those partnerships are incredibly important. I appreciate that from a firsthand view, and if confirmed, I would look to further cultivate that, working with colleagues across the Federal Government.

Senator SCOTT. I am almost out of time, but do you think it is appropriate to pay ransom? What do you all think?

Ms. EASTERLY. I am hesitant to start with that—

Mr. INGLIS. Sir, you have made—

Senator SCOTT. I do not know—I mean, I am not telling you because I know, but—

Mr. INGLIS [continuing]. Easy question, but as framed, no, it is not appropriate to pay ransom. Unfortunately, we get into a place where that is the only thing that is the remedy—

Senator SCOTT. Feasible, right?

Mr. INGLIS. Feasible to save lives or to bring back critical capabilities. It is a really important question, and I am not sure that I have the yes-no answer to it kind of out of context. We need to attack the problem as a system, make it such that we are a hard target, remove the sanctuary, the garrisons that give harbor to these transgressors, make it such that it is harder to move that money without some visibility, hold accountable companies not so much for paying the ransom, but for being in a position where they had to pay the ransom in the first place—right?—for the failure to prepare for that. That is where I think the point of accountability should be placed.

Ms. EASTERLY. It is an incredibly tough choice to make to pay the ransom. I think we heard that from the CEO of Colonial, Mr. Blount, and I have great sympathy for that. I think CISA's role is to prevent people from being in that position by ensuring that they have the technical guidance, the threat information, the best prac-

tices to protect themselves. If confirmed, that is what I would hope to do as the Director of CISA.

Senator SCOTT. Thanks.

Mr. INGLIS. Thank you, sir.

Senator SCOTT. Thank you, Madam Chair.

Senator ROSEN [Presiding.] I want to thank our nominees for your time today and for your work in the past and your work going forward. But I want to build a little bit on what my colleagues have already been discussing with you, and that is cyber workforce, because recent attacks like we have been talking about, SolarWinds, Colonial Pipeline, they are unprecedented, and we know attacks like these are going to continue.

Experts have been warning about this for years, and, of course, here we are. Policymakers at all levels in all branches of government must recruit and retain qualified IT workers and cybersecurity experts in every area across the spectrum to prevent—like you said, to prevent and respond to attacks.

To address the gap, I recently introduced bipartisan legislation establishing a Civilian Cybersecurity Reserve Corps. The Civilian Cybersecurity Reserve Corps would authorize civilian cybersecurity personnel to serve in temporary positions at the Department of Homeland Security or at the Department of Defense (DOD) to supplement existing agency cybersecurity personnel. This bill is based on a recommendation from the Cyberspace Solarium Commission.

I have a two-part question, the first part for you, Ms. Easterly, and the second part for you, Mr. Inglis. Ms. Easterly, if you are confirmed, will you ensure that DHS can mobilize the cybersecurity surge capacity at times of greatest need? And then for you, Mr. Inglis, how should the Federal Government support State and local governments in recruiting and retaining a strong cyber workforce?

Ms. EASTERLY. Thanks for that question, Senator. It is hugely important, and I really enjoyed our discussion on this. You know that workforce development and talent management is a particular passion of mine, and I did see your legislation. I think it speaks to the fact that we need to use all of the creative approaches to be able to attract and retain, importantly, talent into the U.S. Government, ensure that we are building a culture that people want to be a part of and that they feel like they have a career path. But reserve programs, apprenticeship programs, internship programs, and allowing for opportunities for people who want to come from the private sector to serve their country, I think that is where a reserve program could be incredibly effective. If confirmed, I would really look forward to working with you on this issue.

Senator ROSEN. Mr. Inglis.

Mr. INGLIS. Senator, thank you for the question, and thank you for the benefit of our conversation. I, too, enjoyed it greatly. My sense is that the greatest contribution we can make to making a difference in the cyber ecosystem is to address the human factors, the people piece of that.

You have asked whether or not the Federal Government has a role or what that role might look like in aiding and abetting States and locals with the creation of the cyber talent. I think there is a very strong role for the Federal Government. It should not encroach upon the initiatives and the sovereignty of the States and

locales, but it can help quite a great deal. It has the convening power such that we can have the venues where we can exchange best practices. It has the power to create ideas, initiatives to perhaps inspire people to think about talent development in a fundamentally different and new way.

It has the ability to curate and to share how do we create critical thinking skills, cyber literacy, at the earliest possible level. It has the ability to use the power of its purse to encourage the development of talent not simply in the old traditional ways of you have to be a computer scientist in order to enter into one of these jobs, but there is a role for everyone. It can perhaps help us redefine what it means to be a cyber-literate society.

I think there is an all-many-few kind of relationship here. There are a few that have the word “cyber” and “IT” in their names. We are critically short of those. There are many who need to know more about and do more about cyber than they might otherwise have learned from their professional schools. Every one of us needs to learn how to cross the cyber street in the same way we learned how to cross a physical street when we were young. The Federal Government, again, can be helpful in all of that, should not take over or perhaps kind of block out the initiative that the States and the locales I think are generating with great success.

Senator ROSEN. Thank you. I want to build on that because, obviously, we have had problems with our pipeline, but we have similar challenges with securing our electric grid. Last Congress I introduced the Cyber Sense Act, and, again, it is bipartisan legislation that would create a voluntary cyber sense program at the Department of Energy (DOE) to test the cybersecurity of products and technologies intended for use in our bulk power system. The bill would also direct the Energy Secretary to consider incentives perhaps to encourage the use of analysis and testing results when designing products and technologies.

Ms. Easterly, if confirmed, how do you envision CISA working with the Department of Energy to ensure the cybersecurity of our electric grid?

Ms. EASTERLY. Thanks for that question, Senator, and I did see that legislation, and I agree with you. One of the biggest threats is the threat to our energy grid. I am aware of the 100-day plan that we saw that brings together CISA and the Department of Energy to focus on efforts to help protect the energy grid, which I think is incredibly important. CISA, of course, works closely with the Department of Energy, who is the sector risk management agencies for the energy sector. If confirmed, I would look to continue to cultivate that relationship and collaborate closely with the leadership of the Department of Energy and with Cybersecurity, Energy Security, and Emergency Response (CESER) to do everything we can to continue to protect and help all of the critical infrastructure owners and operators protect the energy grid.

Senator ROSEN. Thank you. I want to move on a little bit and continue to talk to you about some of our vulnerabilities. Last year I introduced a bill with Senator Cassidy, the PROTECT Act, that is going to make permanent the Cybersecurity Education and Training Assistance Program (CETAP), as we call it. It is going to provide lots of resources—awareness, curricular resources, profes-

sional development—to elementary and secondary schools. The Clark County School District, the largest school district in my State, one of the largest in the country, had a large ransomware attack recently, and so I want to be sure that we keep CETAP funded.

So if confirmed to the position, do you have any insight into the administration's plans to support K through 12 schools or soft targets in the ransomware space?

Ms. EASTERLY. Thanks for the question, Senator. I have some awareness of the CETAP program and some of what CISA does to protect schools and other facilities that may be vulnerable around the country.

I absolutely agree with you that starting young is critical to building that national societal resilience, providing cyber awareness, knowledge of how to protect yourself, even at the youngest level, particularly now that kids are using all kinds of technology.

I also think it is important because that helps to create a pipeline for the workforce, the earlier piece that we were talking about. If, in fact, I am confirmed, I look forward to working with you on this issue and also working with partners at National Institute of Standards and Technology (NIST) and National Science Foundation (NSF) to ensure that there is the capability to be able to provide education to the K through 12 community.

Senator ROSEN. Thank you. I appreciate that.

And now, via Webex, I would like to recognize Senator Sinema.

OPENING STATEMENT OF SENATOR SINEMA

Senator SINEMA. Thank you, Chair Rosen. I appreciate the nominees joining us today, and I want to thank them for their willingness to serve our Nation in these critical positions.

Now more than ever, we see the importance of enhancing cybersecurity efforts and protecting critical infrastructure. We need only look to the most recent attacks of SolarWinds, the Microsoft Exchange Server, the Colonial Pipeline, and JBS Foods, which has a production facility in Arizona, to see how expansive cyber attacks have become and how damaging the results can be at the Federal, State, and local levels. The amount of time and resources needed to recover is daunting, and the number of attacks is only increasing.

The newly established role of the National Cyber Director and the office this person will lead is an important step to ensure cross-government coordination on cyber strategy and policy. The role of CISA Director has also never been more important to coordinate security and resilience efforts across the public and private sectors. These positions are a critical piece to ensuring that the United States can address the growing threat of cybersecurity attacks on our critical infrastructure.

My first question is for Mr. Inglis. Many of the recent attacks we have seen across the United States come down to a lack of standard cyber hygiene practices, for example, weak passwords or a lack of two-factor authentication at the user level. This is an education issue that I am extremely concerned about. There are a number of efforts across and outside the Federal Government to enhance cyber education efforts beginning in grades K through 12. But as

we talk to stakeholders, they are asking for a lead entity to coordinate efforts and create a strategic plan to organize around.

Do you believe that the National Cyber Director is that entity?

Mr. INGLIS. Senator, thank you for the question, and thank you for the benefit of our conversation, which I very much enjoyed, on these topics. I do believe the National Cyber Director has a role. The Cyber Director by law has a responsibility to inform and to ensure the adequacy of programs and policies intended to improve the cybersecurity posture of the United States. If cyber is a compilation of not simply the technology but of the people who live on the front lines of this as well as doctrine, what are the roles and responsibilities, the National Cyber Director by definition has to ensure that our strategy is the right strategy.

As Ms. Easterly has indicated, we have a number of entities within the Federal enterprise that are doing good work in curating and delivering cyber curricula, K through 12, sometimes in college. Whether that is the National Institute of Standards and Technology with their National Initiative for Cybersecurity Education (NICE) program, the National Science Foundation with their CyberCorps for Service, we need to make sure that those are coherent, that they are complementary, and that they cover the waterfront. I think the National Cyber Director would have a responsibility in that regard, and I would commit to working with this Committee and with you, if confirmed, on that role.

Senator SINEMA. Thank you.

Ms. Easterly, what role do you believe that CISA should play to enhance cyber education at the national, State, and local levels?

Ms. EASTERLY. Thanks for that question, Senator Sinema. Incredibly important. As I have said, CISA is an agency of partnerships, and among the critical partnerships are at the State and local level, and a lot of that is through our CISA's ten Regional Directors, ensuring that the State and local communities have the resources that they need, specifically the educational resources, the assistance, the information about cyber hygiene to be able to protect themselves I think is incredibly important. As I mentioned earlier, I am aware of CETAP; I am aware of other efforts being worked at NIST and NSF, as Mr. Inglis alluded to. If confirmed, I would look to better understand those efforts and really ensure that we can help with this issue of K through 12. It is a particular interest of mine because I think educating from the youngest is critical to ensuring that national resilience as well as creating that pipeline of talent that will need to enable our Federal cyber workforce and the larger workforce for the Nation.

Senator SINEMA. Ms. Easterly, last Congress I introduced legislation to establish a Cybersecurity Advisory Committee that would advise, consult with, and make recommendations to the Director of CISA on development, refinement, and implementation of policies, programs, planning, and training pertaining to the cybersecurity mission of the agency. The language was included and passed into law in the fiscal year (FY) 2021 NDAA. Now, recent cyber attacks have highlighted the importance of public-private partnerships and working with companies to protect against attacks on our infrastructure.

Do you agree that this Advisory Committee can play a critical role in supporting CISA's efforts to defend against threats, particularly those to critical infrastructure?

Ms. EASTERLY. Thanks for that question, Senator Sinema. I am aware of the Cybersecurity Advisory Committee. I think it is a terrific entity to help advise the CISA Director, particularly leveraging the private sector, but also I know that there are entities on there that are supposed to be from State and local. I think this can be a very powerful capability for the CISA Director to help further promote the public-private operational collaboration and to ensure that CISA can effectively coordinate and continue to cultivate those very important public-private partnerships.

I would very much welcome the opportunity to leverage the power of that Cybersecurity Advisory Committee if I am confirmed.

Senator SINEMA. Upon confirmation, I would like our staffs to stay connected on the progress of establishing this committee, so thank you.

Ms. Carnahan, as part of the 2018 National Defense Authorization Act, the GSA was directed to create three e-commerce marketplace pilot programs. In June 2020, GSA awarded proof of concepts to Amazon Business, Overstock Pro, and Fisher Scientific. I am hearing from businesses in Arizona that as of now only the Amazon model has been tested. If confirmed, will you work to ensure that the other models receive adequate testing before the conclusion of the 3-year pilot?

Ms. CARNAHAN. Thanks for bringing that up, Senator. This is not a topic I have been fully briefed on, but I certainly will do so and look forward to working with you and your team to make sure we get that done.

Senator SINEMA. When I talk to Arizona small business owners who depend on government contracts to keep their businesses open, they have two major concerns: first, that a move to a true e-commerce marketplace will obscure the origination of products and leave us vulnerable to the purchase of counterfeit products; and, second, specific to the Amazon marketplace, the platform provider is also a reseller on the platform, which could create a conflict of interest where their products are promoted instead of those of small businesses.

What steps would you take upon confirmation to ensure that the purchase of legitimate products and fairness exist in the system and to ensure that small retailers are treated equally in a system where the platform provider is also a reseller?

Ms. CARNAHAN. Yes, thanks for that. I will say that I have heard, too, from small businesses about their frustration in both getting on GSA's schedules and how hard it is to work through that. I am very focused on making sure that these marketplaces both serve well the agency partners and give them the best possible value and transparency about what they are buying, and also for the small businesses and companies in the United States that want to sell to the government. So these are important issues that you raise. They are things I will look forward to looking into once confirmed, if that happens, and working with your staff. I think these are worthy of very serious consideration, and I think it has long-term impacts for our country.

Senator SINEMA. Thank you, Madam Chair. I yield back my time.
Chairman PETERS [presiding]. Thank you, Senator Sinema.

I think we have gone through the list of Senators who have questions, but I will have one more questions for you, Ms. Carnahan, before we wrap up this hearing. As Chairman of this Committee, I am focused on making sure that we use our Federal fleet, which consists of well over 650,000 vehicles to manage those responsibly and efficiently, and also deal with the detrimental impacts of climate change that threaten irreversible damage to our climate, and sustainable fleet management is clearly critical for both the environment as well as from a fiscal perspective.

So my question to you is—President Biden has recently directed GSA to devise a clean and zero-emission vehicle procurement strategy for its portion of the fleet. So my question is: If confirmed, how would you work to expeditiously implement this plan while navigating supply chain and other implementation and adoption challenges?

Ms. CARNAHAN. Yes, thanks for that question. It is a really interesting one. This is a high priority for the Biden administration, and, interestingly to me, the marketplace is already moving and transitioning toward electric vehicles. I am sure you have seen that in your State, and we are seeing it across the country.

This creates all kinds of good opportunities for good-paying jobs in these sectors, and GSA has this important role to play. I think the key here is to make sure that there is a close consultation with the industry. There is a limitation now on some of the inventory of vehicles because the missions of some of the agencies have specific vehicle needs, and they are not always available in the marketplace right now. Signaling to the market what those needs are is going to be important so they can do their planning. Improved battery life is going to be an issue that everybody is going to want dealt with, and then with the government in particular, charging stations and more access to those charging stations is going to be important.

I think this is about closely coordinating with both industry, this Committee, and the administration on how to get this done, but it is a huge opportunity both to lower costs long term for these vehicles and the use of vehicles in the government, but also have all kinds of benefits for our environment. So this is an exciting opportunity that I really look forward to working with you on.

Chairman PETERS. Thank you, Ms. Carnahan. We look forward to working with you on it as well, because you are right, it is an important and exciting initiative.

In closing, I want to thank once again each of our nominees for being here today and congratulate each of you on your nomination for these very challenging positions. When I say that, very challenging positions, I also want to thank you for your willingness to take on these positions. They are incredibly important, incredibly time-consuming, so that means I definitely have to thank your families as well for their support and love and guidance in the years ahead, as all of you, you and your families, are going to be engaged in public service, and we certainly appreciate that.

The nominees have filed responses to biographical and financial questionnaires, answered prehearing questions submitted by the

Committee,¹ and had their financial statements reviewed by the Office of Government Ethics.² Without objection, this information will be made part of the hearing record with the exception of the financial data,³ which are on file and available for public inspection in the Committee offices.

The hearing record will remain open until 12 p.m. tomorrow, June 11th, for the submission of statements and questions for the record.

This hearing is now adjourned.

[Whereupon, at 12:23 p.m., the Committee was adjourned.]

¹The information of Ms. Carnahan appears in the Appendix on page 52.

²The information of Ms. Easterly appears in the Appendix on page 110.

³The information of Mr. Inglis appears in the Appendix on page 191.

A P P E N D I X

**Chairman Peters Opening Statement As Prepared for Delivery
Full Committee Hearing: Nominations of Robin Carnahan to be Administrator, General
Services Administration; Jen Easterly to be Director, Cybersecurity and Infrastructure
Security Agency, DHS; and Chris Inglis to be National Cyber Director
June 10, 2021**

The Committee will come to order.

Today, we are considering three nominations:

Robin Carnahan, who is joining us remotely, to be Administrator of the General Services Administration, or "GSA", Jen Easterly, to be Director of the Cybersecurity and Infrastructure Security Agency, or "CISA", within the Department of Homeland Security, and Chris Inglis, to be the first-ever National Cyber Director.

Welcome to each of you and to your family members joining us today. Congratulations on your nominations, and thank you for your previous service and for your willingness to take on these important new roles.

The agencies or offices you have been nominated to lead each play a critical role in strengthening our national security and ensuring the federal government is operating effectively and efficiently.

The General Services Administration provides a wide range of support to federal agencies, including managing federal property and the federal fleet, and offering cost-saving acquisition programs and technology services. In short, GSA helps ensure agencies can deliver for the taxpayer and for the American people.

Ms. Carnahan, if confirmed, you will lead GSA at a pivotal moment.

The COVID-19 pandemic changed how workplaces operate across the government and the nation. The Biden Administration is charting a course to make federal buildings, vehicles, and operations more energy efficient. Agencies must do more to modernize and secure their IT systems and networks.

I look forward to hearing more about how you plan to lead GSA and tackle these and other challenges.

The next two nominations are both "firsts" for this Committee.

Ms. Easterly, you are the first person nominated to lead CISA since it was created by this Committee in 2018 and charged with protecting and defending federal networks and securing critical infrastructure. This Committee worked closely with CISA's first Director, Chris Krebs, who led the transformation from its predecessor agency. CISA has made a lot of progress in a very short period of time, but we all know there is a lot more to be done.

The recent SolarWinds hack and Colonial Pipeline ransomware attack are only the latest reminders that the federal government must do more to secure its own networks, and to work with and support our private sector, non-profit, and state, local, and tribal government partners.

Mr. Inglis, you have been nominated to be the first-ever National Cyber Director, a position this Committee created last year to lead a new office within the Executive Office of the President and coordinate national cybersecurity policy and strategy.

The National Cyber Director will be central to ensuring a cohesive whole-of-government approach to cybersecurity.

These are all vital roles and I am pleased that we have three highly-qualified nominees here today who each bring a wealth of government and private sector experience.

Opening Statement

Ranking Member Rob Portman

Homeland Security and Governmental Affairs Committee

*Nominations of:**Robin Carnahan to be Administrator, General Services Administration;**Jen Easterly to be Director, Cybersecurity and Infrastructure Security Agency, DHS; and**Chris Inglis to be National Cybersecurity Director*

June 10, 2021

Thank you, Chairman Peters.

Welcome, Ms. Carnahan, Ms. Easterly, and Mr. Inglis. Thank you for your willingness to serve. These are all very important positions that deserve this Committee's careful consideration.

Established more than 70 years ago, the U.S. General Services Administration plays a vital role in centralizing key support services across government. GSA provides office space, goods and services, technology modernization and acquisition assistance, purchase cards, and leased vehicles to virtually every federal agency. In 2020 alone, GSA managed more than 370 million rentable square feet of property and helped agencies acquire more than \$75 billion in goods and services. While work like this is rarely on the front page, it is vital to the business of government and the protection of taxpayer dollars. For example, one longstanding GSA offering, the City Pair Program, offers pre-negotiated airline rates for federal travelers to nearly 12,000 markets and despite lower levels of air travel due to the pandemic, it is still expected to save taxpayers \$1.2 billion in 2021 alone.

To lead this vital agency, President Biden has nominated former Missouri Secretary of State Robin Carnahan. In both her service with her home state of Missouri, and more recently in a term position with GSA, Secretary Carnahan has been an outspoken advocate of government technology modernization and improvement, which I hope would be a key priority for her if she is confirmed. I am pleased to have her here today and look forward to speaking with her about the position.

The other two nominees here today also are for key positions that must lead government modernization of our country's cybersecurity. Jen Easterly has been nominated to head the Cybersecurity and Infrastructure Security Agency at DHS and Chris Inglis has been nominated to be first ever National Cyber Director. Both Ms. Easterly and Mr. Inglis have years of impressive government service in positions protecting our national security.

As members of this Committee know all too well, cybersecurity failures are becoming all too common. It seems that America's data and information – both in the public and private sectors – has never been more at risk. As a result, DHS's Cybersecurity and Infrastructure Security Agency, or "CISA," has almost become a household name.

Earlier this week, the CEO of Colonial Pipeline testified before this Committee and we heard first-hand the troubling effects of a ransomware attack on a critical infrastructure company. In

that ransomware attack, cybercriminals in Russia shut down a major U.S. fuel pipeline for several days, leading to fuel shortages up and down the East Coast.

Colonial Pipeline is just one of many recent attacks on companies and public entities. Other recent victims include the world's largest meat processor, JBS; and a constituent outreach services platform used by the House of Representatives. It appears no one is safe from ransomware attacks.

These high-profile ransomware attacks come on the heels of major cyber campaigns against U.S. government agencies and private companies— SolarWinds, Microsoft Exchange, and Pulse Secure. The SolarWinds and Pulse Secure VPN attacks targeted federal agencies, yet it was private sector companies that discovered these intrusions. Despite all the increased funding appropriated for cybersecurity and the bipartisan legislation we've worked on here in this Committee, not one of these federal intrusions was discovered by the federal government.

As the SolarWinds attack unfolded, it became clear that the Department of Homeland Security—the agency tasked with securing other federal networks—was itself compromised. This included the very agency Ms. Easterly has been nominated to head, CISA. DHS should be an example for federal agencies, but it was hacked. It's clear that our federal cyber defenses are lacking.

The fact the federal government was hacked is not surprising. In June 2019, as the Chairman of the Permanent Subcommittee on Investigations, I released a report with Senator Carper detailing the extensive cybersecurity vulnerabilities of eight federal agencies. Many of these vulnerabilities had remained unresolved for a decade. Ms. Easterly, I am interested in hearing how you plan to ensure federal agencies are secure, and that the data we entrust them with is safe.

Also, Congress has just recently created the position Mr. Inglis has been nominated to fill. The National Cyber Director in the White House is tasked with coordinating implementation of national cyber policy and strategy.

I have long advocated for a single point of accountability for federal cybersecurity overseeing the federal government's role, both in ensuring our agencies are secure and in being a good partner with the private sector. I look forward to hearing how Mr. Inglis plans to strike that balance while standing up a brand new office.

I also hope to discuss the importance of transparency with Congress today. On April 5 of this year, Chairman Peters and I sent letters to CISA and the Federal Chief Information Security Officer requesting information about the federal response to SolarWinds and accountability for federal cybersecurity. To date, the Federal CISO has only provided us a list of web links. And until earlier this week, CISA had only provided us documents it had already provided to Congress previously. Many of the documents CISA provided this week also contain unexplained redactions.

I appreciate the three of you for being here today, and look forward to your testimony about how your qualifications prepare you for the positions for which you've been nominated.

**Hearing before the U.S. Senate Committee on Homeland Security and
Governmental Affairs
Ms. Robin Carnahan, Nominee to be Administrator, U.S. General Services
Administration
Thursday, June 10, 2021**

Good morning Chairman Peters and Ranking Member Portman, and Members of the Committee. I appreciate the opportunity to be here and am honored to be President Biden's nominee as Administrator of the General Services Administration. I'm also grateful to Senator Blunt, my home state Senator, for his kind introduction. We've known each other for more than 30 years and our families even longer. I value Senator Blunt's leadership, his passion for public service and commitment to the people of Missouri. Thank you, Senator, for your service.

Even though we're joining virtually today, I'd like to acknowledge my family. My husband Juan Carlos for his unwavering love and encouragement. My mother, Jean Carnahan, who's been a role model and hero all my life. And my brothers, Russ and Tom, and their wonderful families. They've all been a tremendous source of love and strength throughout my life.

Public service runs in my family; much of that serving the people of Missouri. My grandfather and brother served in Congress. My father was Governor of Missouri; and my mother was the first woman from Missouri in the US Senate. My mother's parents were also public servants, though they never ran for office. Mom was born in Washington, DC and grew up across the river in Anacostia. Her father worked as a farmer and plumber at St. Elizabeths Hospital; her mother at the Navy department during the war.

So growing up, the government didn't seem like a far away or abstract concept. For me, it was about the people who worked on behalf of their community and country. Folks who went to work every day to improve the lives of children and families, to help

businesses thrive and keep the country safe. I grew up believing public service to be a noble calling and worthy of our lives. And I still do.

I've had the privilege of serving in elected office, as well as in appointed and staff positions in state and federal government. No matter the role, I always understood my job was to deliver effective service for people and be a wise steward of taxpayers' money.

I'll never forget my first day on the job as Missouri Secretary of State. As I was introduced around the office, I met more people manually opening mail and preparing checks to be deposited than we had in the entire IT department. That moment in 2005 crystallised how I came to view the challenge ahead for government — to adapt modern technology tools to streamline operations and deliver better service to people.

So during my tenure, we invested time and money in modernizing our IT infrastructure in order to deliver better services to 400,000 businesses, four million voters, and millions of others who needed something from government.

One lesson I learned was that digital infrastructure investments pay off, both in better service and lower costs for both government and taxpayers. But I also learned that without serious attention tech modernization projects can go wrong. The truth is, nothing I did in office caused me to lose more sleep than the rollout of one of those new technology platforms.

Diving in to learn more about both technology and procurement policy led me to GSA, where I served for four years during the Obama and Trump administrations. I joined the digital consulting team 18F whose job is to help government partners more effectively buy and build modern software systems and train non-technical leaders on how to set their teams up for success.

This past year has shown the importance and fragility of our nation's digital infrastructure. As the pandemic swept through the country, Congress responded fast

with programs to meet the challenges, yet far too often that help was slow getting to families and businesses most in need.

The bottom line is, no program passed by this Congress can be fully effective without smart investments in an effective, secure digital infrastructure to deliver it. GSA is uniquely positioned to support that delivery mission across government.

Of course, GSA is about much more than technology. I see similar opportunities to improve the way GSA delivers value to partners in real estate management and acquisition. If confirmed, I look forward to exploring creative and practical ways to rightsize the federal real estate portfolio to serve the changing needs of agency partners and local communities.

In acquisitions, I look forward to working with stakeholders, including agency partners and companies, to streamline and simplify how they interact with GSA. I want to provide easy access and outstanding value to those buying through GSA and an easier on-ramp for businesses, especially small businesses, interested in selling through GSA.

As President Biden recently said in his speech to Congress "We have to prove democracy still works. That our government still works--and can deliver for the people."

For me, helping our government, our democracy, effectively deliver for the people and taxpayers is why I'm so excited about the opportunity to lead GSA.

Thank you for the opportunity to testify before you today. I am humbled and look forward to answering your questions.

REDACTED

HSGAC BIOGRAPHICAL QUESTIONS FOR EXECUTIVE NOMINEES

1. Basic Biographical Information

Please provide the following information.

<i>Position to Which You Have Been Nominated</i>	
Name of Position	Date of Nomination
Administrator, General Services Administration	April 6, 2021

<i>Current Legal Name</i>			
First Name	Middle Name	Last Name	Suffix
Robin	Colleen	Carnahan	

<i>Addresses</i>					
Residential Address (do not include street address)			Office Address (include street address)		
			Street: n/a		
City: St. Louis	State: MO	Zip: 63105	City:	State:	Zip:

<i>Other Names Used</i>						
First Name	Middle Name	Last Name	Suffix	Name Used From (Month/Year) (Check box if estimate)	Name Used To (Month/Year) (Check box if estimate)	
			Σ			

				m g		
n/a					Est <input type="checkbox"/>	Est <input type="checkbox"/>
					Est <input type="checkbox"/>	Est <input type="checkbox"/>

<i>Birth Year and Place</i>	
Year of Birth (Do not include month and day.)	Place of Birth
1961	Rolla, Missouri

<i>Marital Status</i>					
Check All That Describe Your Current Situation:					
Never Married	Married	Separated	Annulled	Divorced	Widowed
<input type="checkbox"/>	XX	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

<i>Spouse's Name (current spouse only)</i>			
<u>Spouse's First Name</u>	<u>Spouse's Middle Name</u>	<u>Spouse's Last Name</u>	<u>Spouse's Suffix</u>
Juan Carlos		Antolinez	

<i>Spouse's Other Names Used (current spouse only)</i>						
<u>First Name</u>	<u>Middle Name</u>	<u>Last Name</u>	<u>Suffix</u> Σ	<u>Check if Maiden Name</u>	<u>Name Used From</u> (Month/Year) (Check box if estimate)	<u>Name Used To</u> (Month/Year) (Check box if estimate)
n/a					Est <input type="checkbox"/>	Est <input type="checkbox"/>
					Est <input type="checkbox"/>	Est <input type="checkbox"/>

<i>Children's Names (if over 18)</i>			
First Name	Middle Name	Last Name	Suffix
n/a			

2. Education

List all post-secondary schools attended.

<u>Name of School</u>	<u>Type of School</u> (vocational/technical/trade school, college/university/military college, correspondence/distance/extension/online school)	<u>Date Began School</u> (month/year) (check box if estimate)	<u>Date Ended School</u> (month/year) (check box if estimate) (check "present" box if still in school)	<u>Degree</u>	<u>Date Awarded</u>
University of Virginia	Law School	8/83 Est X	Est Present 5/86	JD	5/1986
William Jewell College	Undergrad college	79 Est 8/	Est Present 12/82	BA	5/1983
University of Southampton	University	81 Est 9/	Est Present 5/82	none	none
		Est	Est Present		

3. Employment

(A) List all of your employment activities, including unemployment and self-employment. If the employment activity was military duty, list separate employment activity periods to show each change of military duty station. Do not list employment before your 18th birthday unless to provide a minimum of two years of employment history.

<u>Type of Employment</u> (Active Military Duty Station, National Guard/Reserve, USPHS Commissioned Corps, Other Federal employment, State Government (Non-Federal Employment), Self-employment, Unemployment, Federal Contractor, Non-Government Employment (excluding self-employment), Other)	<u>Name of Your Employer/Assigned Duty Station</u>	<u>Most Recent Position Title/Rank</u>	<u>Location</u> (City and State only)	<u>Date Employment Began</u> (month/year) (check box if estimate)	<u>Date Employment Ended</u> (month/year) (check box if estimate) (check "present" box if still employed)
Non-government	Georgetown University	Fellow	Washington DC	Est 3/2020	Est Present
unemployment				Est 2/2020	Est 3/2020
Federal government	U.S. General Services Administration	Innovation Specialist	Washington DC	Est 1/2016	Est 1/2020
Self	Confluents Ventures LLC	Principal	St. Louis, MO	Est 2/2014	Est 1/2016
Non-government	University of Chicago	Senior Fellow	Chicago	Est 9/2013	Est 12/2013
unemployment				Est 2/2013	Est 8/2013
State government	State of MO	Sec. of State	Jefferson City MO	Est 1/2005	Est 1/2013
Non-government	Global Ventures LLC	Principal	St. Louis, MO	Est 1/1997	Est 12/2004
Federal government	Ex-Im Bank of US	Special asst to the Chairman	Washington, DC	Est 6/1993	Est 7/1996
Non-government	Carnahan & Associates	Partner	Rolla, MO	Est 1/1991	Est 5/1993

Non-government	Nat'l Democratic Inst	Advisor	Washington, DC	Est 1/1990	Est 12/1990
Non-government	Thompson Mitchell	Associate	St. Louis, MO	Est 8/1986	Est 12/1989
Non-government	Brown Rudnick	Law clerk	Boston	Est summer '86	
State government	Missouri House of Reps	Research analyst	Jefferson City, MO	Est 1/1983	Est 7/1983

(B) List any advisory, consultative, honorary or other part-time service or positions with federal, state, or local governments, not listed elsewhere.

<u>Name of Government Entity</u>	<u>Name of Position</u>	<u>Date Service Began</u> (month/year) (check box if estimate)	<u>Date Service Ended</u> (month/year) (check box if estimate) (check "present" box if still serving)
n/a		Est <input type="checkbox"/>	Est <input type="checkbox"/> Present <input type="checkbox"/>
		Est <input type="checkbox"/>	Est <input type="checkbox"/> Present <input type="checkbox"/>
		Est <input type="checkbox"/>	Est <input type="checkbox"/> Present <input type="checkbox"/>

4. Potential Conflict of Interest

(A) Describe any business relationship, dealing or financial transaction which you have had during the last 10 years, whether for yourself, on behalf of a client, or acting as an agent, that could in any way constitute or result in a possible conflict of interest in the position to which you have been nominated.

In connection with the nomination process, I have consulted with the General Services Administration's Designated Agency Ethics Official, in consultation with the Office of Government Ethics, to identify potential conflicts of interest. Any potential conflicts of interest will be resolved in accordance with the terms of an ethics agreement that I have entered into with the agency's Designated Agency Ethics Official and have provided to the Committee. I am not aware of any other potential conflict of interest.

(B) Describe any activity during the past 10 years in which you have engaged for the purpose of directly or indirectly influencing the passage, defeat or modification of any

legislation or affecting the administration or execution of law or public policy, other than while in a federal government capacity.

N/A

5. Honors and Awards

List all scholarships, fellowships, honorary degrees, civilian service citations, military medals, academic or professional honors, honorary society memberships and any other special recognition for outstanding service or achievement.

- Rotary Foundation Scholarship 1981
- Aspen Institute Rodel Fellowship 2005
- William Jewell College Alumni Achievement Award 2009
- Jimmy Kirkpatrick Outstanding Public Service Award 2009
- University of Chicago
 - Senior Fellow, Harris School of Public Service 2013
 - Visiting Fellow, Institute of Politics 2013
- FedScoop 2017 TopWomen in Tech

6. Memberships

List all memberships that you have held in professional, social, business, fraternal, scholarly, civic, or charitable organizations in the last 10 years.

Unless relevant to your nomination, you do NOT need to include memberships in charitable organizations available to the public as a result of a tax deductible donation of \$1,000 or less, Parent-Teacher Associations or other organizations connected to schools attended by your children, athletic clubs or teams, automobile support organizations (such as AAA), discounts clubs (such as Groupon or Sam's Club), or affinity memberships/consumer clubs (such as frequent flyer memberships).

<u>Name of Organization</u>	<u>Dates of Your Membership</u> (You may approximate.)	<u>Position(s) Held</u>
Linux Foundation Public Health	2020-present	Advisor
National Council on Election Integrity/Issue One	2020-present	Member/advisory board
US Digital Response	2020-present	Volunteer
Aircraft Owners and Pilots Association (AOPA)	2020-present	Member

Missouri Historical Society	2018-present	Member
Missouri Botanical Garden	2018-present	Member
Democracy Fund	2015-2019	National Advisory Board member
LaunchCode Foundation	2011-present	Director
Chapter KU PEO	1995-present	Member
District of Columbia Bar Association	1987-present	Member
Missouri Bar Association	1986-present	Member

7. Political Activity

(A) Have you ever been a candidate for or been elected or appointed to a political office?

<u>Name of Office</u>	<u>Elected/Appointed/ Candidate Only</u>	<u>Year(s) Election Held or Appointment Made</u>	<u>Term of Service (if applicable)</u>
Missouri Secretary of State	Elected	2004, 2008	8 years
United States Senate	Candidate	2010	n/a

(B) List any offices held in or services rendered to a political party or election committee during the last ten years that you have not listed elsewhere.

<u>Name of Party/Election Committee</u>	<u>Office/Services Rendered</u>	<u>Responsibilities</u>	<u>Dates of Service</u>
---	---------------------------------	-------------------------	-----------------------------

n/a			

(C) Itemize all individual political contributions of \$200 or more that you have made in the past five years to any individual, campaign organization, political party, political action committee, or similar entity. Please list each individual contribution and not the total amount contributed to the person or entity during the year.

As a candidate for public office, I maintained a state candidate committee. After leaving office, the Robin Carnahan for Missouri candidate committee was terminated and remaining funds were transferred to Democracy 2.0, a Missouri political action committee. I have not made any individual political contributions of \$200 or more in the past five years.

<u>Name of Recipient</u>	<u>Amount</u>	<u>Year of Contribution</u>

8. Publications and Speeches

(A) List the titles, publishers and dates of books, articles, reports or other published materials that you have written, including articles published on the Internet. Please provide the Committee with copies of all listed publications. In lieu of hard copies, electronic copies can be provided via e-mail or other digital format.

<u>Title</u>	<u>Publisher</u>	<u>Date(s) of Publication</u>
See Attachment 1		

(B) List any formal speeches you have delivered during the last five years and provide the Committee with copies of those speeches relevant to the position for which you have been nominated. Include any testimony to Congress or any other legislative or administrative body. These items can be provided electronically via e-mail or other digital format.

<u>Title/Topic</u>	<u>Place/Audience</u>	<u>Date(s) of Speech</u>
See Attachment 1		

(C) List all speeches and testimony you have delivered in the past ten years, except for those the text of which you are providing to the Committee.

<u>Title</u>	<u>Place/Audience</u>	<u>Date(s) of Speech</u>
See Attachment 1		

--	--	--

9. Criminal History

Since (and including) your 18th birthday, has any of the following happened?

- Have you been issued a summons, citation, or ticket to appear in court in a criminal proceeding against you? (Exclude citations involving traffic infractions where the fine was less than \$300 and did not include alcohol or drugs.)
 - NO
- Have you been arrested by any police officer, sheriff, marshal or any other type of law enforcement official?
 - NO
- Have you been charged, convicted, or sentenced of a crime in any court?
 - NO
- Have you been or are you currently on probation or parole?
 - NO
- Are you currently on trial or awaiting a trial on criminal charges?
 - NO
- To your knowledge, have you ever been the subject or target of a federal, state or local criminal investigation?
 - NO

If the answer to any of the questions above is yes, please answer the questions below for each criminal event (citation, arrest, investigation, etc.). If the event was an investigation, where the question below asks for information about the offense, please offer information about the offense under investigation (if known).

A) Date of offense:

a. Is this an estimate (Yes/No):

B) Description of the specific nature of the offense:

C) Did the offense involve any of the following?

- 1) Domestic violence or a crime of violence (such as battery or assault) against your child, dependent, cohabitant, spouse, former spouse, or someone with whom you share a child in common: **Yes / No**
- 2) Firearms or explosives: **Yes / No**
- 3) Alcohol or drugs: **Yes / No**

D) Location where the offense occurred (city, county, state, zip code, country):

- E) Were you arrested, summoned, cited or did you receive a ticket to appear as a result of this offense by any police officer, sheriff, marshal or any other type of law enforcement official: **Yes / No**
- 1) Name of the law enforcement agency that arrested/cited/summoned you:
 - 2) Location of the law enforcement agency (city, county, state, zip code, country):
- F) As a result of this offense were you charged, convicted, currently awaiting trial, and/or ordered to appear in court in a criminal proceeding against you: **Yes / No**
- 1) If yes, provide the name of the court and the location of the court (city, county, state, zip code, country):
 - 2) If yes, provide all the charges brought against you for this offense, and the outcome of each charged offense (such as found guilty, found not-guilty, charge dropped or "nolle pros," etc). If you were found guilty of or pleaded guilty to a lesser offense, list separately both the original charge and the lesser offense:
 - 3) If no, provide explanation:
- G) Were you sentenced as a result of this offense: **Yes / No**
- H) Provide a description of the sentence:
- I) Were you sentenced to imprisonment for a term exceeding one year: **Yes / No**
- J) Were you incarcerated as a result of that sentence for not less than one year: **Yes / No**
- K) If the conviction resulted in imprisonment, provide the dates that you actually were incarcerated:
- L) If conviction resulted in probation or parole, provide the dates of probation or parole:
- M) Are you currently on trial, awaiting a trial, or awaiting sentencing on criminal charges for this offense: **Yes / No**
- N) Provide explanation:

10. Civil Litigation and Administrative or Legislative Proceedings

(A) Since (and including) your 18th birthday, have you been a party to any public record civil court action or administrative or legislative proceeding of any kind that resulted in (1) a finding of wrongdoing against you, or (2) a settlement agreement for you, or some other person or entity, to make a payment to settle allegations against you, or for s you to take, or refrain from taking, some action. Do NOT include small claims proceedings.

<u>Date Claim/Suit Was Filed or Legislative Proceedings Began</u>	<u>Court Name</u>	<u>Name(s) of Principal Parties Involved in Action/Proceeding</u>	<u>Nature of Action/Proceeding</u>	<u>Results of Action/Proceeding</u>
	Jackson County, MO	Carnahan v. Parker Hannifin Corp.	Wrongful death action	January 16, 2004 jury verdict for plaintiff.

From 2005 to 2013, I served as the Missouri Secretary of State. While serving in that role I was named in multiple lawsuits in my official capacity.

(B) In addition to those listed above, have you or any business of which you were an officer, director or owner ever been involved as a party of interest in any administrative agency proceeding or civil litigation? Please identify and provide details for any proceedings or civil litigation that involve actions taken or omitted by you, or alleged to have been taken or omitted by you, while serving in your official capacity.

<u>Date Claim/Suit Was Filed</u>	<u>Court Name</u>	<u>Name(s) of Principal Parties Involved in Action/Proceeding</u>	<u>Nature of Action/Proceeding</u>	<u>Results of Action/Proceeding</u>
N/A				

--	--	--	--	--

(C) For responses to the previous question, please identify and provide details for any proceedings or civil litigation that involve actions taken or omitted by you, or alleged to have been taken or omitted by you, while serving in your official capacity.

11. Breach of Professional Ethics

(A) Have you ever been disciplined 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? Exclude cases and proceedings already listed.

<u>Name of Agency/Association/Committee/Group</u>	<u>Date Citation/Disciplinary Action/Complaint Issued/Initiated</u>	<u>Describe Citation/Disciplinary Action/Complaint</u>	<u>Results of Disciplinary Action/Complaint</u>
N/A			

(B) Have you ever been fired from a job, quit a job after being told you would be fired, left a job by mutual agreement following charges or allegations of misconduct, left a job by mutual agreement following notice of unsatisfactory performance, or received a written warning, been officially reprimanded, suspended, or disciplined for misconduct in the workplace, such as violation of a security policy?

N/A

12. Tax Compliance

(This information will not be published in the record of the hearing on your nomination, but it will be retained in the Committee's files and will be available for public inspection.)

REDACTED

REDACTED

13. Lobbying

In the past ten years, have you registered as a lobbyist? If so, please indicate the state, federal, or local bodies with which you have registered (e.g., House, Senate, California Secretary of State).

N/A

14. Outside Positions

XX ☐ See OGE Form 278. (If, for your nomination, you have completed an OGE Form 278 Executive Branch Personnel Public Financial Disclosure Report, you may check the box here to complete this section and then proceed to the next section.)

For the preceding ten calendar years and the current calendar year, report any positions held, whether compensated or not. Positions include but are not limited to those of an officer, director, trustee, general partner, proprietor, representative, employee, or consultant of any corporation, firm, partnership, or other business enterprise or any non-profit organization or educational institution. Exclude positions with religious, social, fraternal, or political entities and those solely of an honorary nature.

<u>Name of Organization</u>	<u>Address of Organization</u>	<u>Type of Organization</u> (corporation, firm,	<u>Position Held</u>	<u>Position Held From</u> (month/year)	<u>Position Held To</u> (month/year)
---------------------------------	------------------------------------	--	----------------------	---	---

		partnership, other business enterprise, other non-profit organization, educational institution)			
PT Fund, Inc	Washington, DC	Pres. Transition	Volunteer	12/2020	1/2021
Georgetown University, Beeck Center	37th Street, NW, Washington DC 20007	university	Fellow	3/2020	present
US Digital Response	San Francisco, CA	non-profit	Volunteer	3/2020	present
National Council on Election Integrity/Issue One	Washington, DC	non-profit	Member/advisory board	2020	present
Union Labor Life Insurance Co	1625 Eye St. NW, Washington DC 20006	corporation	Director	5/2018	present
Center for Creative Arts (COCA)	6880 Washington Ave. St. Louis, MO	non-profit	Director	~2016	~2017
Democracy Fund	Washington, DC	non-profit	National Advisory Committee	2015	2019
LaunchCode Foundation	4811 Delmar St. Louis MO	non-profit	Director	1/2015	present
Confluents Ventures, LLC	St. Louis, MO 63105	LLC	Member	2/2014	present
Nat'l Democratic Institute for Int'l Affairs	455 Mass Ave. NW Washington DC	non-profit	Director	11/2011	present
Family Revocable Trust	St. Louis, MO	Trust	Trustee	1/2002	present
Carnahan Farms	PO Box 904, Rolla, MO	LLC	Member	9/2001	present
Debonair Associates	PO Box 904, Rolla, MO	LLC	Member	11/1999	present

15. Agreements or Arrangements

XX ☐ See OGE Form 278. (If, for your nomination, you have completed an OGE Form 278 Executive Branch Personnel Public Financial Disclosure Report, you may check the box here to complete this section and then proceed to the next section.)

As of the date of filing your OGE Form 278, report your agreements or arrangements for: (1) continuing participation in an employee benefit plan (e.g. pension, 401k, deferred compensation); (2) continuation of payment by a former employer (including severance payments); (3) leaves of absence; and (4) future employment.

Provide information regarding any agreements or arrangements you have concerning (1) future employment; (2) a leave of absence during your period of Government service; (3) continuation of payments by a former employer other than the United States Government; and (4) continuing participation in an employee welfare or benefit plan maintained by a former employer other than United States Government retirement benefits.

<u>Status and Terms of Any Agreement or Arrangement</u>	<u>Parties</u>	<u>Date</u> (month/year)

16. Additional Financial Data

All information requested under this heading must be provided for yourself, your spouse, and your dependents. (This information will not be published in the record of the hearing on your nomination, but it will be retained in the Committee's files and will be available for public inspection.)

REDACTED

REDACTED

SIGNATURE AND DATE

I hereby state that I have read the foregoing Statement on Biographical and Financial Information and that the information provided therein is, to the best of my knowledge, current, accurate, and complete.

Robin Carnahan

This 4/18/2024 Day of May, 20

REDACTED

UNITED STATES OFFICE OF
GOVERNMENT ETHICS

April 16, 2021

The Honorable Gary C. Peters
Chairman
Committee on Homeland Security
and Governmental Affairs
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

In accordance with the Ethics in Government Act of 1978, I enclose a copy of the financial disclosure report filed by Robin Carnahan, who has been nominated by President Biden for the position of Administrator, General Services Administration.

We have reviewed the report and have obtained advice from the agency concerning any possible conflict in light of its functions and the nominee's proposed duties. Also enclosed is an ethics agreement outlining the actions that the nominee will undertake to avoid conflicts of interest. Unless a date for compliance is indicated in the ethics agreement, the nominee must fully comply within three months of confirmation with any action specified in the ethics agreement.

Based thereon, we believe that this nominee is in compliance with applicable laws and regulations governing conflicts of interest.

Sincerely,

DAVID APOL

David J. Apol
General Counsel

Digitally signed by DAVID
APOL
Date: 2021.04.16 13:00:13
+0400

Enclosures REDACTED

April 5, 2021

Mr. Nitin Shah
Designated Agency Ethics Official
General Services Administration
Office of General Counsel
1800 F Street, NW
Washington, DC 20405

Dear Mr. Shah:

The purpose of this letter is to describe the steps that I will take to avoid any actual or apparent conflict of interest in the event that I am confirmed for the position of Administrator of General Services. It is my responsibility to understand and comply with commitments outlined in this agreement.

SECTION 1 – GENERAL COMMITMENTS

As required by the criminal conflicts of interest law at 18 U.S.C. § 208(a), I will not participate personally and substantially in any particular matter in which I know that I have a financial interest directly and predictably affected by the matter, or in which I know that a person whose interests are imputed to me has a financial interest directly and predictably affected by the particular matter, unless I first obtain a written waiver, pursuant to 18 U.S.C. § 208(b)(1), or qualify for a regulatory exemption, pursuant to 18 U.S.C. § 208(b)(2). I understand that the interests of the following persons are imputed to me:

- Any spouse or minor child of mine;
- Any general partner of a partnership in which I am a limited or general partner;
- Any organization in which I serve as an officer, director, trustee, general partner, or employee; and
- Any person or organization with which I am negotiating or have an arrangement concerning prospective employment.

In the event that an actual or potential conflict of interest arises during my appointment, I will consult with an agency ethics official and take the measures necessary to resolve the conflict, such as recusal from the particular matter or divestiture of an asset.

If I have a managed account or otherwise use the services of an investment professional during my appointment, I will ensure that the account manager or investment professional obtains my prior approval on a case-by-case basis for the purchase of any assets other than cash, cash equivalents, investment funds that qualify for the regulatory exemption for diversified mutual funds and unit investment trusts at 5 C.F.R. § 2640.201(a), obligations of the United States, or municipal bonds.

I will receive a live ethics briefing from a member of the ethics office after my confirmation but not later than 15 days after my appointment pursuant to the ethics program regulation at 5 C.F.R. § 2638.305. Within 90 days of my confirmation, I will submit my Certification of Ethics Agreement Compliance which documents my compliance with this ethics agreement.

I understand that as an appointee I will be required to sign the Ethics Pledge (Exec. Order No. 13989) and that I will be bound by it. Among other obligations, I will be required to recuse from particular matters involving specific parties involving my former employer or former clients for a period of two years after I am appointed, with the exception of states and local governments.

I will not modify this ethics agreement without your approval and the approval of the U.S. Office of Government Ethics pursuant to the ethics agreement requirements contained in the financial disclosure regulation at 5 C.F.R. § 2634.803(a)(4).

SECTION 2 – RESIGNATIONS

Upon confirmation, I will resign from my positions with the following entities:

- Georgetown University
- Union Labor Life Insurance Company
- LaunchCode Foundation
- National Democratic Institute for International Affairs
- U.S. Digital Response

I also previously resigned from my position with PT Fund, Inc. (Biden-Harris transition team). Pursuant to the impartiality regulation at 5 C.F.R. § 2635.502, for a period of one year after my resignation from each of these entities, I will not participate personally and substantially in any particular matter involving specific parties in which I know that entity is a party or represents a party, unless I am first authorized to participate, pursuant to at 5 C.F.R. § 2635.502(d).

SECTION 3 – CONFLUENS VENTURES, LLC

I formed a limited liability company doing business as Confluens Ventures LLC, to manage my consulting work. It is currently dormant. During my appointment to the position of Administrator, the firm will remain dormant and will not advertise. I will not perform any services for the firm, except that I will comply with any requirements involving legal filings, taxes and fees that are necessary to maintain the firm while it is in an inactive status. As Administrator, I will not participate personally and substantially in any particular matter that to my knowledge has a direct and predictable effect on the financial interests of Confluens Ventures LLC. In addition, pursuant to the impartiality regulation at 5 C.F.R. § 2635.502, I will not participate personally and substantially in any particular matter involving specific parties in which I know a former client of mine is a party or represents a party for a period of one year after I last provided service to that client, unless I am first authorized to participate, pursuant to 5 C.F.R. § 2635.502(d).

SECTION 4 – FAMILY FARM

My family and I own a family farm held by Carnahan Farms LLC. Under Missouri law, this LLC is organized in a way that all members are managers. I will continue to have a financial interest in this entity, but I will not provide services material to the production of income. Instead, I will receive only passive investment income from it. I will not participate personally and substantially in any particular matter that to my knowledge has a direct and predictable effect on the financial interests of Carnahan Farms LLC, unless I first obtain a written waiver pursuant to 18 U.S.C. § 208(b)(1).

SECTION 5 – FAMILY TRUST

I will retain my position as a trustee of the Family Revocable Trust. I will not receive any fees for the services that I provide as a trustee during my appointment to the position of Administrator. I will not participate personally and substantially in any particular matter that to my knowledge has a direct and predictable effect on the financial interests of the Family Revocable Trust, unless I first obtain a written waiver, pursuant to 18 U.S.C. § 208(b)(1), or qualify for a regulatory exemption, pursuant to 18 U.S.C. § 208(b)(2).

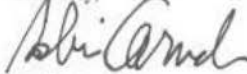
SECTION 6 – SPOUSE EMPLOYMENT

My spouse is the sole proprietor of his consulting firm, which does business as Falcon Aerial Analytics LLC, an aerial inspection and data analytics consulting company. I will not participate personally and substantially in any particular matter that to my knowledge has a direct and predictable effect on the financial interests of Falcon Aerial Analytics LLC, unless I first obtain a written waiver, pursuant to 18 U.S.C. § 208(b)(1). Pursuant to the impartiality regulation at 5 C.F.R. § 2635.502, I also will not participate personally and substantially in any particular matter involving specific parties in which I know a client of my spouse is a party or represents a party, unless I am first authorized to participate, pursuant to 5 C.F.R. § 2635.502(d).

SECTION 7 – PUBLIC POSTING

I have been advised that this ethics agreement and the Certification of Ethics Agreement Compliance will be posted publicly, consistent with the public information law at 5 U.S.C. § 552, on the website of the U.S. Office of Government Ethics with ethics agreements of other Presidential nominees who file public financial disclosure reports.

Sincerely,



Robin Carnahan

**U.S. Senate Committee on Homeland Security and Governmental Affairs
Pre-hearing Questionnaire
For the Nomination of Robin Carnahan to be
Administrator, General Services Administration**

I. Nomination Process and Conflicts of Interest

1. Did the President give you specific reasons why he nominated you to be the next Administrator of the General Services Administration, and if so, what were they?

No.
2. Were any conditions, expressed or implied, attached to your nomination? If so, please explain.

No.
3. Have you made any commitments with respect to the policies and principles you will attempt to implement as Administrator? If so, what are they, and to whom were the commitments made?

No.
4. Are you aware of any business relationship, dealing, or financial transaction that could result in a possible conflict of interest for you or the appearance of a conflict of interest? If so, please explain what procedures you will use to recuse yourself or otherwise address the conflict. And if you will recuse yourself, explain how you will ensure your responsibilities are not affected by your recusal.

No.
5. Please provide the name of any individual, law firm, consulting firm, lobbying firm, public relations firm, or other entity you have formally retained or contracted with regarding this nomination, including any amounts paid in fees or otherwise.

N/A. I have not formally retained or contracted with anyone regarding this nomination.

II. Background of the Nominee

6. Why do you want to serve as the Administrator of the General Services Administration (GSA)?

This is a unique moment to reimagine how government, at every level, can more effectively deliver services to the public and be better stewards of taxpayer money. GSA is uniquely

positioned to help agencies across government do that work, and by doing so, help restore public trust in government and in democracy. That's why I'd be honored to serve as GSA Administrator.

7. What specific background, experience, and attributes affirmatively qualify you to be Administrator?

Much of my career has focused on improving how government works for people and provides value to taxpayers. I've worked in both the public and private sectors, in both state and federal government, in the executive and legislative branches, and in elected, appointed, and staff positions. This breadth of experience, including a four year term leading a technology team at GSA, makes me well prepared to lead an agency that services all branches, agencies, and levels of government. In addition, my experience in leading government technology modernization efforts is especially relevant given the increased demand for better digital service delivery and cybersecurity across government.

8. Please describe:
a. Your leadership and management style.

A leader's job is to listen and learn from their team, customers and stakeholders; understand the operating environment; align the team around common goals; communicate a shared vision of success; and create incentives and metrics to measure progress. My management style is collaborative. I am highly focused on increasing value to customers and taxpayers; being data-driven, impact-oriented, and respectful of career public servants; and focused on investing in and empowering teams to succeed.

- b. Your experience managing personnel.

As Missouri Secretary of State I managed a staff of 250 full-time employees in seven operating divisions responsible for providing in person and on-line services to over 400,000 businesses, 4 million voters, 134,000 brokers and financial professionals, and hundreds of thousands of other customers.

- c. What is the largest number of people that have worked under your supervision?

250 people.

9. What would you consider your greatest successes as a leader?

Aligning and empowering teams to provide outstanding customer service and improve peoples' lives by delivering government services that are better, faster, and cheaper. That has taken many forms throughout my career, from streamlining regulations and cutting red tape and costs for agency customers, to improving efficiency and reducing budget during my tenure as Missouri Secretary of State, to launching the state and local practice at 18F, GSA's technology team, to help state and local government agencies improve the way they buy and build technology to deliver better digital services to the public.

10. What would you consider your greatest failure as a leader? What lessons did you take away from that experience?

One of my biggest disappointments as Secretary of State was leaving office before the completion of a major technology modernization project used by hundreds of thousands of businesses. That experience taught me the importance of ensuring that leadership at the highest levels understands and stays actively involved in technology modernization projects, from budgeting to procurement to implementation. Executive engagement is important to ensure delivery of the value promised on time and on budget. This was a pivotal experience in my career and led me to dive deeply into understanding technology and the role leaders, both in and out of government, must play to set those projects up for success.

11. Please give examples of times in your career when you disagreed with your superiors and advocated your position. Were you ever successful?

I grew up as the only girl in a family with three brothers, so I am no stranger to robust debate and disagreement. Fortunately, in the workplace I've had the opportunity to work with superiors who have been open-minded, solicited honest feedback and often used that to inform and make decisions. I learned the value that approach provides in improving employee morale and team performance and have strived to do the same during my career.

12. Do you seek out dissenting views and encourage constructive critical dialogue with subordinates? Please provide examples of times in your career when you have done so.

I am a strong believer in cross functional teams and the value of soliciting opinions and feedback from a wide variety of sources as a way to get the best information on which to base decisions. Throughout my career, I have understood the value of engaging with a wide variety of stakeholders, whether those be customers, legislatures, businesses, or constituents.

13. Please list and describe examples of when you made politically difficult choices that you thought were in the best interest of the country or your organization.

Politically difficult choices come with the job of being an elected official. Some of the most difficult for me occurred during the 2008 global financial crisis when I served as Missouri's State Securities Regulator. State regulators came under intense pressure from distressed financial institutions in their states to delay or limit enforcement of state securities laws. But wronged investors relied on my office to help them during a time of crisis. Striking the right balance was challenging and carried a political price.

14. Please describe how you build credibility and trust among staff as a leader.

In my experience, active listening, treating people with respect, clearly communicating expectations, and delivering on commitments are key elements to building trust among teams.

15. During your career, has your conduct as a government employee ever been subject to an investigation or audit by the Office of Special Counsel, Department of Justice, agency Equal Opportunity office or investigator, agency Inspector General, or any other similar federal, state, or local investigative entity? If so, please describe the nature of the allegations/conduct and the outcome(s) of the investigation(s) or audit(s).

No.

16. Please describe your responsibilities during your previous four years at the General Services Administration. What do you believe are your greatest accomplishments?

From January 2016-January 2020, I served on the GSA digital consulting team, 18F. In addition to advising federal agency partners, I started the state and local practice to advise state and local agencies administering federal programs (ie. child welfare, Medicaid, etc.) on modern practices for procuring services and overseeing technology modernization projects. During that time our team advised more than a dozen federal, state, and local agencies on ways to improve customer facing digital services and cut costs. Besides the value of training dozens of government partners in modern software and procurement practices, another valuable accomplishment was co-authoring a handbook, De-risking Custom Technology Projects: A handbook for state grantee budgeting and oversight, a guide for budget specialists, legislators, and other decision makers who fund or oversee state government technology projects.

17. On June 21, 2017, the GSA Office of Inspector General released a finding that former GSA Administrator Denise Turner Roth retaliated against a whistleblower for making protected disclosures related to “concerns of violations of law, gross mismanagement, a gross waste of funds, and abuse of authority” related to the then structure and management of Technology Transformation Services (TTS). Please describe any involvement you had in decisions related to the organizational structure of TTS in 2016 and whether you were involved, and to what extent, in GSA IG investigations into this issue.

While at 18F, I was not involved with decisions related to the organizational structure of TTS. As an 18F staff member, I believe I may have been interviewed regarding the IG investigation, but do not remember details nor have any notes and materials from that time.

III. Role of the GSA Administrator

18. Please describe your view of GSA's mission and what you would consider to be your role and responsibilities, if confirmed as Administrator.

GSA's mission is to "deliver value and savings in real estate, acquisition, technology, and other mission-support services across government."

As Administrator, my job will be to ensure:

- *GSA's career professionals are empowered and equipped with the tools and training they need to carry out the mission;*
- *alignment on a shared agenda, outcomes, success metrics, and clearly communicate those throughout the organization;*
- *feedback from agency customers, industry partners, Congress, and other stakeholders is consistently solicited and integrated into the services GSA provides, especially digital services;*
- *a culture of innovation and continuous improvement focused on delivering outstanding service to the public and the best value for taxpayers whether that be related to real estate, acquisition services or technology tools.*

19. What do you anticipate will be your greatest challenges as GSA Administrator, and what will be your top priorities? What do you hope to accomplish during your tenure?

The COVID-19 pandemic continues to dramatically impact lives across the globe and has forced changes in the way businesses and governments operate. Responding to those changes will continue to be an enormous challenge. GSA and its agency partners will be tasked with rethinking the future of work, including workplace needs such as physical space, building safety, and the hardware and software needed to securely work outside traditional government buildings. At the same time, public safety and expectations have shifted toward increased demand for more government services being made available on-line even as cybersecurity threats increase. Meeting those public expectations and security threats will continue to be a challenge.

If confirmed, besides working to address the challenges mentioned above, my priorities will include attracting and investing in the career professionals needed to carry out GSA's mission and empowering them with the tools and training needed to provide outstanding service; providing greater value and security to our agency and industry partners by reducing the complexity and cost of doing business with GSA and striving to be the most trusted source for acquisition solutions; right-sizing the portfolio of government owned and leased property to provide the best value to agency partners and US taxpayers; improving digital platforms to provide a better experience for users (both internal and public facing) and develop more offerings for high impact, secure government-wide shared-service platforms.

20. In your opinion, is GSA currently fulfilling its responsibility to provide the "best value in real estate, acquisition, and technology services" to the government? Please explain.

GSA has done an admirable job of staying focused on its core mission. As with any large organization, adapting to the speed of societal and technological change is a challenge. While GSA has been a leader among government agencies in adapting to these changes, I'm convinced that even more can be done to improve the value and service and efficiency of how GSA delivers on that mission.

21. As GSA Administrator, how will you work to promote efficient government operations?

Making government work better for people and taxpayers has been my life's calling and it would be an honor to continue that work at GSA. I'll work every day to inspire the team to stay focused on its public service mission while encouraging the adoption of best practices from the private sector, including data-driven and impact-focused decision making to improve service delivery and efficient operations.

IV. Policy Questions

Real Property Management

22. What do you view as the major challenges facing the federal real estate portfolio?

Deferred repair and maintenance and rightsizing the federal footprint are challenges facing the federal real estate portfolio. In order to adequately maintain its portfolio, GSA needs appropriate resources for repairs and alterations. Additionally, examining partner agencies' current and future space needs given the potential move toward a more remote federal workforce will be critical.

The GAO has acknowledged that GSA's limited access to all revenues deposited in the Federal Buildings Fund (FBF) is a key impediment to GSA's ability to more effectively manage federal real property assets. Restricting access to all funds deposited in the FBF adversely impacts GSA's real property management activities, including causing project delays, cost escalations, and increasing deterioration of facilities. If confirmed, I look forward to collaborating with the Public Buildings Service, Congress, and the Administration to figure out the best course of action to resolve these federal real estate challenges and ensure the needs of our federal buildings and partner agencies are met.

23. What role do you believe GSA should play in determining the size of the federal government's property portfolio?

Each agency has its own unique mission and established utilization and space standards. GSA's role is to procure space that supports customer missions and is cost effective for the customer and taxpayer. If confirmed, I'd like to work with GSA staff and customer agencies to examine mission requirements in light of telework opportunities to determine the most effective space utilization strategy moving forward.

24. Sixty percent of GSA's held leases were set to expire between 2019 and 2023. If confirmed, how will you approach leasing at this pivotal moment? What considerations will you prioritize? Do you believe the last Administration's focus on securing savings from larger leases first was the right approach?

If confirmed, I will work to continue to minimize the cost of leasing by focusing on technology to improve lease cycle time and to drive timely lease replacement. During this unique time, it will be important to work with federal agency partners to define their requirements for a post-pandemic workforce and negotiate savings for the government and taxpayers. Continuing improvements like lease cost avoidance by negotiating favorable rates; replacing leases on time, thereby avoiding costly lease extensions; and working with customers to reduce their footprint will be critical.

25. If confirmed, what concrete steps will you take as Administrator to reduce agency reliance on leases in cases where government ownership would be more cost-effective over the long term?

If confirmed, I look forward to working with Congress and agency partners to seek resources in order to consolidate leases into owned space. I will also work with staff to evaluate the portfolio of expiring leases to seek greater co-location of agencies into owned space; optimize of the federal footprint while minimizing the upfront capital needs of our customers in right-sizing their operations; and find opportunities for projects where agencies can move into owned space when it is financially beneficial.

26. The Government Accountability Office (GAO) has included federal real property management on its High Risk list each year since 2003. GSA is the primary agency responsible for improving this high-risk area. What steps will you take as Administrator to remove federal real property management from GAO's High Risk list?

I was pleased to learn that in March 2021, GAO removed the leasing segment of Managing Federal Real Property from its High Risk List. GAO's removal of costly leases from its High Risk List is a recognition of the great work that GSA has done to improve its federal real property management activities. However, more work remains to be done to remove other federal real property management activities from GAO's list. On GAO's 2021 High Risk List, excess and underutilized property, data reliability, and physical security remain areas of concern. I share an urgency about the need to address these concerns, and if confirmed, commit to building on the Public Buildings Service's efforts to date.

27. The Federal Property Management Reform Act and the Federal Assets Sale and Transfer Act (FASTA) both became law in 2016. Do you believe these laws have been successfully implemented? What additional steps do you think are necessary to improve the government's management of its property portfolio?

If confirmed, I look forward to assessing the implementation status of both laws over the past five years, in order to determine where successes or challenges may lie. I know that ultimately the goal is to improve the management of our federal property, and in a transparent and collaborative way. I recognize GSA's important role in leading the Federal Government in optimizing its real property portfolio through effective disposition and utilization strategies, and I welcome the opportunity to work with all of you in Congress to ensure that these laws are being implemented effectively.

28. The Public Buildings Reform Board (PBRB) is an independent Board established by FASTA to identify opportunities for the federal government to reduce its real property inventory. A January 2021 GAO report found that PBRB did not fully document how it evaluated properties and determined which to recommend for disposal. What steps will you take as Administrator to work with PBRB to increase transparency into this process?

Transparency and collaboration are essential components of successful transactional management, especially in the disposal of federal real property. If confirmed I will work with PBRB and/or any federal agency to continue this transparent, collaborative approach working with local stakeholders, regulators, and market participants.

29. In a January 26, 2021 memo, President Biden directed all agencies to engage “in regular, meaningful, and robust consultation with tribal officials in the development of federal policies that have tribal implications.” In April, Acting Office of Management and Budget (OMB) Director Shalanda Young informed GSA and Public Buildings Reform Board (PBRB) that plans to sell the Federal Archives and Records Center in Seattle, Washington were “counter to this administration’s tribal consultation policy.” What steps will you take as Administrator to ensure diverse community perspectives and civil rights concerns are factored into how and where federal facilities are both disposed of and built?

I value the importance of regularly engaging with community partners to understand their perspectives and factor those into the decision-making process. If confirmed, I commit to strengthening and improving these interactions and fostering meaningful, collaborative, ongoing consultation with tribal officials on GSA policies, programs, and projects that hold tribal implications.

30. GAO has reported extensively that GSA’s database of agencies’ inventories of real property assets, the Federal Real Property Profile (FRPP), is inaccurate and unreliable due to inconsistent reporting by agencies. What steps will you take to improve the accuracy of the FRPP so that it can be a useful tool to assist in disposing of excess, underutilized, or surplus real property?

If confirmed, I am committed to improving the database accuracy, completeness, and usefulness. I look forward to working with GSA staff on governmentwide standardization efforts and to work with federal agencies to improve the reliability of their real property data. Improving data quality and bringing further public transparency will further assist to identify underutilized, surplus, and excess properties for consolidation, collocation, and disposal opportunities.

31. What role do you believe GSA should play in helping increase energy efficiency at federal buildings in order to save taxpayer dollars on energy costs and address climate change?

GSA is well positioned to help address the Biden Administration’s priorities of combating the climate crisis by increasing energy efficiency and reducing costs in its federal buildings. GSA can serve as a leading example of how to do that effectively across its portfolio.

Globally, one-third of the world's energy is consumed by buildings, and most buildings are deeply inefficient. If confirmed, I plan to collaborate with relevant stakeholders, including this committee, as part of the whole-of-government approach to address the issue of climate change. I look forward to building on GSA's long-standing efforts to minimize environmental impacts.

32. In April 2021, GSA announced its commitment to 100 percent renewable electricity sources for the federal real estate portfolio by 2025. What challenges do you anticipate in the effort to provide renewable energy to a real estate footprint of 186 million square feet? How do you plan to overcome these challenges?

The President has challenged government agencies to work toward carbon pollution free energy for the federal government by 2035, and this will be a significant step toward that longer-term goal. While GSA has considerable experience in energy procurement, as GSA has the foundational responsibility for all utility procurement for the federal government, I'm sure there may be challenges along the way. I look forward to using power purchase agreements effectively and ensuring that they are well integrated into the grids that supply GSA buildings; and encouraging utility power suppliers to increase the percentages of clean energy delivered and specify increasing amounts of clean energy in utility agreements. To be effective, these approaches will take time and the ability to adapt to rapidly evolving technologies. But, done well, GSA's approach can be a model for other agencies, and ultimately benefit the public and taxpayers with cleaner energy and lower costs.

33. GSA maintains and operates a facility opened in 1934 known as the Central Heating Plant that provides heating and cooling to a number of federal buildings in the downtown Washington, DC area via a series of gas-fired turbines. In light of GSA's stated commitment to 100 percent renewable electricity sources by 2025, do you believe that the Plant must be decommissioned within that timeframe?

I would need time to assess the situation, first, and learn more about the Central Heating Plant, how it functions and the impact to the federal property portfolio in DC. What I do know is that an efficient and flexible model that supports many types of working arrangements and scenarios will be needed as GSA works to achieve this goal. I look forward to exploring opportunities and challenges for reducing greenhouse gas emissions, in alignment with national climate goals and action plans, through the use of renewable energy, energy efficiency, electrification and smart building technologies at federal buildings.

34. Given limits on Federal funds and the growth of telework, do you believe it is a better investment for GSA to focus on shrinking its portfolio into new higher performing buildings or renovating its existing portfolio?

The answer to that depends on a range of factors, and each project is evaluated on its own merits. Some of those major factors include the cost of renovation versus new construction. In addition to total project cost, GSA could consider a renovation option if the current

building has a return on investment. That said, new construction could be considered if the current location is not meeting agency mission and/or security needs. Given that specific facts and conditions for each project are the driving determinants for GSA action, it's important that projects be assessed on a case-by-case basis.

35. In an April 16, 2021 letter the PBRB informed OMB and GSA that GSA's recent decision to not adhere to the PBRB's disposal process recommendation for the properties it identified, and OMB approved, for sale, "will result in the Administration's failure to meet both the spirit and the letter of the law." Do you believe that GSA has the authority to not use the PBRB's recommended disposal process?

If confirmed, I look forward to engaging with stakeholders in the property disposal space to ensure that we are delivering excellent value to the American people. It is my understanding that under the Federal Asset Sales and Transfer Act (FASTA), it is GSA's responsibility to execute sales in a manner that will maximize taxpayer value. If confirmed, I will ensure that GSA continues to focus on harnessing the expertise and insights of relevant stakeholders as I carry out my responsibilities to ensure the Government's sales are fair, competitive, and transparent while maximizing proceeds for the taxpayer.

36. How do you believe GSA should approach the answer to whether to own or lease federal buildings?

It is my understanding that when GSA and client agencies begin discussing space needs, GSA first checks its inventory of Government-owned and Government-controlled leased space. It is also my understanding that, if no suitable space is available, a leasing action will be required. If confirmed, I will work to be responsive to the needs of client agencies and at the same time work to maximize taxpayer value. Effectively delivering GSA services in a taxpayer-focused way means meeting client agencies' needs based on their unique circumstances.

37. Due to chronic underfunding of GSA's repairs and alterations account, GSA's outstanding maintenance backlog is currently measured in billions of dollars, leading to a deterioration in the habitability of many of GSA's owned buildings. Given this backlog, where do you think the appropriate balance is between improving the quality of the buildings and improving their environmental characteristics?

I share the concern about the growing backlog of repairs and alterations needed to maintain federal facilities in a condition suitable to house one million federal employees. The deferred maintenance of GSA's owned inventory includes modernizing building systems. Replacing HVAC, plumbing, building envelope, and lighting systems with modern equivalents will not only improve the quality of the buildings, but also reduce energy consumption and operating costs.

38. In recent years, budgetary constraints and scoring rules have made large federal real estate projects increasingly difficult to initiate. One major example of this has been the \$3 billion FBI headquarters project, which failed once in 2017 due to a lack of Congressional

appropriations and a faulty procurement strategy, and again in 2018 due to partisan concerns. To avoid the need for large capital outlays, could the government use a ground lease-leaseback strategy, where the federal government would lease property to a developer who would then construct a building that the federal government would then pay rent on and at the conclusion of the rental period, the building would revert to federal ownership? Would you support such an approach for large real estate acquisitions?

I look forward to learning more about this approach. In the absence of sufficient appropriations to implement sorely needed new construction and modernization projects, ground lease lease-backs could prove a valuable tool to meet mission requirements in a manner more cost effective than through simply engaging in large scale leases for long-term federal requirements. If confirmed, I look forward to working with Congress to explore additional disposal strategies to reduce excess underutilized property.

Personal Property and Federal Fleet

39. The federal government's personal property inventory – which includes furniture, cars, laptops, machinery, and equipment – is valued at over \$1 trillion. Sound management of this portfolio is essential in preventing waste, fraud, and abuse. The Federal Personal Property Management Act of 2018 instituted a process to streamline the federal property review process. The legislation requires GSA to issue guidance that directs federal agencies to assess property more regularly, including the age and condition of the property and the extent to which the property is used and needed so that they can dispose of unneeded property more regularly. What steps will you take as Administrator to ensure agencies fully comply with the GSA guidance required under the Federal Personal Property Management Act and avoid retaining unneeded property?

GSA has long been a leader in helping agencies right-size their portfolio. GSA should continue to play a critical role in helping agencies identify, prepare, and divest unneeded property, and the effective reuse, donation, and sale of Federal Personal Property. If confirmed, I look forward to working with Congress to explore additional disposal strategies to reduce excess underutilized property.

40. On January 27, 2021, President Biden issued Executive Order 14008 directing the Administrator of GSA to work with the Director of OMB, the Chair of the Council on Environmental Quality, and relevant federal agency heads to develop a plan that includes a clean and zero-emission vehicle procurement strategy. What challenges do you expect to encounter in developing and implementing this strategy? If confirmed, how do you plan to address those challenges?

I look forward to the opportunity to lead an agency that will be at the forefront of deploying a zero-emission vehicle strategy. That said, I realize that this is an ambitious task that will come with challenges. Some of those challenges will be model availability and finding electric vehicles that meet the mission requirements of Federal agencies; acquiring funding that is required to purchase vehicles and put charging infrastructure in place; and creating a culture change amongst Federal employees who, like most Americans, are not familiar or

comfortable with driving electric vehicles. Addressing these challenges effectively will take time and significant coordination with agency and industry partners as well as Congress. If confirmed, I will join GSA staff in working with agency partners, CEO, and OMB on a government-wide strategy for greening the federal fleet; working with industry to clearly understand the marketplace and ensure its effectively leveraging the Government's buying power to negotiate the best possible deal for taxpayers; addressing issues/barriers through educational campaigns and developing customized agency electric vehicle adoption plans; and working closely with Congress on how to fund and build out the charging infrastructure that will be needed to make this transition.

COVID-19 and Disaster Response

41. GSA is a critical component of the nation's disaster response apparatus, assisting federal, state, and local governments to quickly purchase additional ambulance services, search and rescue services, medical supplies, food and water, and other emergency supplies.

- a. Please describe your understanding of GSA's role in responding to hurricanes and other disasters.

As I understand, GSA is a part of the National Response Framework (NRF), which provides foundational emergency management doctrine for how the country responds to all types of incidents. GSA's Federal Acquisition Service provides a wide array of products and services and is often relied upon to supplement FEMA's efforts for emergency supplies by state and local governments in preparation for, response to, or recovery from an emergency and is a great resource during times of crisis.

- b. What reforms, if any, would you suggest to improve GSA's capacity in this area?

If confirmed, I look forward to engaging with congressional and federal agency stakeholders on reviewing and, if necessary, improving existing emergency response protocols. It is important to build upon the program's previous successes and to strengthen existing interagency emergency support collaborations for disaster responses that afflict our communities across the nation.

42. The federal government's operating environment has changed rapidly within the last year as a result of the COVID-19 pandemic with a substantial portion of the federal workforce working remotely.

- a. If confirmed, how would you go about working with federal agencies to update telework and space-planning policies and guidance? Would you commit to assessing how the pandemic has changed the amount, type, and cost of space GSA and federal-tenant agencies need?

With the events of the past year, it seems likely that agencies will begin rethinking telework policies to allow for more flexibility. This, in turn, may impact their space needs (reductions, consolidation, or reconfiguration) going forward. As agencies determine how

to best meet mission needs in an ever-evolving work environment, many are still trying to determine what their workplace of the future will look like. If confirmed, I am committed to being flexible and helping our customer agencies adapt to any necessary changes.

- b. As Administrator, how would you address changing tenant space needs in existing spaces and incorporate these needs into current and future construction project requests?

If confirmed, I would leverage GSA's Center for Workplace Strategy expertise and services to engage with agency partners to further inform, define, and confirm their workspace needs as they look to the future. This information would help GSA refine the requirements and provide appropriate workplace solutions for agencies to meet their missions. Overall flexibility, adaptability, and sustainability will be key.

Procurement Policy

- 43. If confirmed, what will be your immediate and longer-term priorities related to federal contracting and procurement?

As Administrator, my priorities will be to leverage the Federal procurement spending to help fight the pandemic, and support the nation's efforts to reopen schools and the economy, as soon and safely as possible. For GSA, this includes working with agency partners to ensure they can secure critical supplies and provide safer workplaces.

I hope to help GSA achieve these policy objectives by focusing on improving the user experience of selling to the Federal government and the customer experience of buying through GSA. In doing so, careful attention must be paid to modernizing how GSA buys IT across the Federal government to support agencies' delivery of their missions and improving the value citizens receive from government services. By ensuring that improving the user experience and adding value are the foundational components of any IT modernization, GSA can have an outsize impact on improving outcomes for the public good and saving money for taxpayers.

- 44. What do you see as the appropriate relationship between the OMB's Office of Federal Procurement Policy and the acquisition policy functions of the General Services Administration?

The Office of Federal Procurement Policy (OFPP) provides overall direction for the government-wide procurement policies, regulations, procedures, and forms for executive agency acquisitions that are subject to the Federal Acquisition Regulation (FAR). I understand that GSA represents the civilian agencies on the Federal Acquisition Regulation Council, and thus partners with OFPP to carry out the Administration's procurement priorities. This partnership means GSA's acquisition policy functions benefit all federal agencies.

I understand that GSA and OMB both have an important role to play together to deliver an efficient and effective procurement system. GSA's mission is to be the central procurement

arm of the government by helping agencies obtain the goods, services and solutions to execute their mission. Given GSA's vast experience providing acquisition support to agencies across government, it should be a valuable partner in OFPP's work to lead and shape Federal procurement policy and implement the Administration's policy.

45. What role do you believe GSA should play in helping agencies leverage the federal procurement process to combat climate change?

GSA has an important role to play in tackling the climate crisis. As the government's buyer, GSA can leverage the power of government procurement to help foster a sustainable government and markets. The agency offers a variety of resources and acquisition solutions that make it easy for federal agencies to buy sustainable products, services, and solutions. While individual agencies are ultimately responsible for making climate-related purchasing decisions at the order-level, GSA could offer resources to offer viable options to individual buyers in considering sustainability and climate impacts when making purchasing decisions.

46. GAO has identified increased use of strategic sourcing as a means of saving tens of billions of dollars in federal procurement spending. Yet, use of strategic sourcing remains low in many agencies. What, if any, reforms would you suggest to increase the use of strategic sourcing without unduly limiting competition?

I understand that one primary reform to strategic sourcing would be to advocate for continued maturation of government-wide category management, which has largely replaced the principles of strategic sourcing. I would encourage reforms to policies and systems to allow for more robust collection and sharing of pricing, subcontractor, and purchase card data. These changes will allow category management practitioners to better understand their options and ensure they're getting the best value for their money.

47. If confirmed, what steps will you take to ensure category management and the common acquisition platform proceed in a way that minimizes administrative cost increases for vendors?

If confirmed, I look forward to working with GSA staff to ensure the Common Acquisition Platform will benefit the vendor community by eliminating or consolidating redundant systems and processes; simplifying and streamlining the vendor contract/catalog management processes to promote ease of use; and promoting data transparency and integrity across all sales channels.

48. The AbilityOne program provides important employment opportunities for people who are blind or severely disabled through federal procurements of goods and services from non-profits employing these individuals. However, it is often difficult for the program to determine whether these non-profits are actually employing sufficient numbers of severely disabled individuals to meet the program's requirements. If confirmed, what action will you take to ensure this program is helping people who truly need it?

We, as a government, have a responsibility to ensure that AbilityOne lives up to the promise of providing important employment opportunities for people who are blind or severely disabled and that includes providing adequate oversight to ensure that all non-profit agencies under AbilityOne are in compliance with program requirements. If confirmed, I look forward to working with the Commission and nonprofit agencies (NPAs) to ensure compliance with statutory and regulatory Program requirements is met.

49. Please describe how you would balance fulfilling the needs of agencies for goods and services against meeting social policy goals, such as those related to climate change.

GSA's mission of providing value and savings to support the functioning of government ultimately involves agencies making trade-offs between price and other factors, some required by law, such as the SBA's 8(a) program, which creates opportunities for small and disadvantaged businesses, while helping federal agencies meet their needs and others based on Administration priorities. GSA's job is to provide options and transparency to agencies making the final buying decisions about the products and services that best suit their need at the best value.

50. Do you believe that the federal procurement process is an appropriate place to attempt to influence social policy? If so, to what extent?

For years, federal procurement practices have played a role in helping achieve public policy objectives, such as supporting small business and socio-economic categories. Providing options and transparency to allow agency partners to strike the right balance to deliver their mission will continue to be a priority for GSA.

51. The Federal Acquisition Service (FAS) has seen sales growth of more than 30 percent over the last three years. Do you believe that is sustainable? Do you intend to set a target to identify savings generated annually for the taxpayer?

I would like to see FAS sales continue to grow at a healthy rate. Focusing on balancing growth with staffing levels and maintaining acquisition quality, will be important for future success. If confirmed, I hope to work with FAS and OMB to set annual savings targets that are transparent and accessible.

52. In 2017, GSA consolidated the TTS into FAS in part to address certain management challenges and legal funding issues identified by the GSA IG and others.

- a. Do you believe that that consolidation was the right decision? Please explain.

The support and infrastructure provided by FAS has created a runway for maturity and evolution. From my perspective, it's important that each part of GSA has the right authorities and structure to support their mission.

- b. If confirmed, is it your intention to retain the current structure?

The need for digital services that meet the needs of both the agency's mission and the constituents they serve has never been greater. Improving digital services and accelerating IT modernization will be key to the long-term success of this country. Supporting the current focus from the Administration and across the federal landscape for technology as a key driver of change, will be my priority. It is my intention, if I have the pleasure to serve, to ensure GSA is set up for operational success, while also ready and positioned with technology at the forefront.

53. Do you believe TTS, and within TTS, both the Centers of Excellence and 18F, should operate on a break-even basis? If yes, what measures would you take to ensure these entities cover their costs?

I believe that TTS — like all parts of GSA — should be responsible stewards of public funds. I also know from firsthand experience that 18F has saved the government many multiples of their cost in savings and cost avoidance. To me, cost recovery is a tool to ensure value for agencies and the public, not an end in itself. If confirmed, my intention as Administrator would be to work with the Chief Financial Officer, General Counsel, Federal Acquisition Service, the OMB, and Congress to ensure that all of our programs have the right funding structure and internal controls to support delivery for our agency partners, and to ensure that we are getting the most return on public investment.

54. With regard to the interaction between TTS and FAS, do you believe TTS needs assisted acquisition authority, or do you believe it is more cost-effective and efficient to rely on FAS's Assisted Acquisition Services staff?

It is my understanding that TTS has matured its capability to conduct procurement over the last few years by partnering and leveraging the acquisition expertise within the FAS. The partnership has led to continued positive delegations of additional procurement authority. Today, TTS has sufficient procurement authority to conduct the acquisitions in support of its mission while continuing to partner within FAS to even further mature its capabilities. Furthermore, TTS brings a unique cross-functional approach to assisted acquisitions, providing its partner agencies not only with acquisition professionals who are experts with modern procurement practices but also technology experts in the fields of engineering, product management, and human-centered design.

55. While with TTS, you worked on outreach to State and local government entities, under what circumstances, what volume, and to what end do you believe it is appropriate and makes sense for GSA to be providing services at the State and local level? Are you concerned about State and local work crowding out federal work? Additionally, what authority do you believe GSA should use to conduct such work?

Prior to the COVID-19 pandemic, the federal government spent nearly \$100 billion on technology related spending for state and local governments, much of that to implement federal programs. Increasing cybersecurity threats that demand a smart, coordinated whole of government response are likely to add to that cost. The American people deserve a government that works and delivers services effectively, whether that happens at the

federal, state, or local level. Taxpayers deserve a government that spends money wisely. If GSA can help achieve these goals by supporting state and local governments, it should.

56. GSA currently serves as one of the four main civilian payroll providers in government and has advocated extensively for the NewPay program to stand up a software-as-a-service solution to replace aging, legacy IT at all four payroll providers. Do you believe this is the correct approach? Please explain.

As I understand, GSA is committed to leveraging modern technology to ensure safe, secure delivery of payroll services to its federal civilian customers. The importance of establishing common data standards is a key driver to any IT modernization effort. When implemented correctly, shared services can drive greater efficiency, effectiveness, and consistently positive user experience across the spectrum of administrative functions. NewPay which, as I understand it, is meant to replace the existing siloed payroll systems, seems to hold a lot of promise, but like any new modernized system we need to ensure the proper resources are in place to successfully implement. I look forward to learning more about this project, if confirmed, and any opportunities or challenges related to its implementation.

57. Do you believe GSA should be a mandatory source for more goods or services within government? Please explain.

FAS is the mandatory source for some categories of spend (e.g. travel). Decisions about mandatory sources should be made as part of a government-wide decision framework and ecosystem. FAS will continue to iterate on the buying process to improve the experience for customers and vendors.

58. In April 2020, GSA waived the Trade Agreements and Buy American statute clauses for several Federal Supply Classes upon the determination that personal protective equipment was not available from Trade Agreement and Buy American statute compliant sources. This exception has been extended through September. Do you believe it remains necessary to continue sourcing PPE from countries like China, rather than from American producers and manufacturers in U.S.-allied countries?

I agree with the President that GSA should buy American whenever and wherever possible and do that consistent with existing treaty obligations. It's been well documented that the U.S. has experienced a severe shortage of personal protective equipment (PPE) needed by healthcare workers fighting the COVID-19 pandemic. If confirmed, I look forward to teaming up with the Office of Management and Budget (OMB), as well as the U.S. Trade Representative, to focus on building back better and address these very questions.

59. Section 889 of the FY 2019 NDAA bars the federal government from doing business with any entity that uses any telecom equipment or services from six Chinese companies "as a substantial or essential component of any system, or as a critical technology as part of any system" regardless of whether that system is related to the entity's work for the federal government.

- a. How will you ensure GSA can meet the needs of federal agencies, while ensuring compliance with this provision?

Ensuring that the Federal government's supply chain is safe and secure from foreign interference and that agencies feel confident in the products and services that GSA provides is of the highest priority. If confirmed, I will ensure that GSA complies with all federal laws and regulations.

- b. How will you respond if GSA and the federal government do not have sufficient purchasing power in an industry, such as the vehicle industry, to incentivize entities to not use banned technology?

Conducting extensive industry outreach to communicate the objectives and requirements necessary for firms that want to do business with the US Government must be a priority. By ensuring clarity and open communication channels, I would hope to help GSA's industry partners make informed decisions. I look forward to learning more about the impact Section 889 may have on GSA and our industry partners, and, if necessary, expanding outreach and engagement to find alternative solutions.

- c. How do you believe GSA should conduct oversight of entities that represent compliance with section 889 requirements?

I am very concerned about the potential for foreign adversaries to exploit our federal systems and those of our contractors. Specifically, to the threat from China which Section 889 was enacted to address, my concerns would be with the ability of our contractors and suppliers to have full visibility on their supply chains and understand the provenance of the components and subcomponents of their systems. This is especially challenging for the smaller business and many of the new companies we hope to bring into the federal marketplace. If confirmed, I would look forward to the opportunity to work with this committee on how we can support our vendor community and still protect our infrastructure from all foreign threats.

Cybersecurity and Information Technology

60. GSA's mission statement includes "deliver[ing] the best value in [...] technology services to government and the American people." Is the proper role of GSA to deliver technology services to federal agencies or to assist those agencies in acquiring technology services? Please explain.

GSA's goal is to lead the charge in modernizing the government's approach to buying and deploying technology products and services. Whether it is facilitating the deployment of innovative and effective technology solutions or designing acquisition vehicles that meet government agencies' technology needs of today and tomorrow, GSA's role is to help federal agencies deliver on their missions and serve the public in the most effective, efficient, and sustainable way possible.

61. What do you view to be the most significant current and emerging cyber security threats facing our nation? What role does GSA have in addressing these threats?

Cybersecurity threats are constantly evolving, and GSA has an important role to play in combating these threats alongside other Federal partners, especially when it comes to supply chain risk management. Additionally, GSA has an opportunity through the Technology Modernization Funding (TMF) to make investments in modernizing high priority systems, bringing agencies up to a common standard for cybersecurity, improving citizen facing tools, and building shared capabilities and common solutions, while retiring antiquated legacy technology systems. If confirmed, I will work with GSA staff to prioritize close collaboration with various cybersecurity-related partner agencies, OMB, Congress, and industry partners to support federal cyber security efforts and strengthen supply chain risk management.

62. With your experience founding and leading the State and Local Government Practice at 18F, what is your view of the role of 18F in helping recruit private sector technology talent to assist federal agencies?

The Technology Transformation Services (TTS) at GSA, which houses 18F, regularly recruits private sector technology talent to support agency modernization efforts. Those private sector hires serve tours of duty in government to advise and assist agencies with improving the outcomes of government IT projects. Specifically, 18F recruits for roles for agile cross-functional teams, such as design, product, and developers. 18F uses the recruitment of tech talent to constantly ensure they are bringing the most innovative and best practices from the private sector into the federal government. 18F also hires federal employees who have experience in modern software development practices. Having a team of private sector talent mixed with federal talent allows 18F to better service federal, state, and local governments, something I experienced first-hand during my time of service on that team.

63. While working at 18F, you stated your goal was “to deliver better digital services to more people, at a lower cost to taxpayers and with lower risk of failure.” If confirmed, what will be your immediate and longer-term priorities for 18F?

My tour of duty at 18F ended shortly before the COVID-19 crisis. I am certain that the operating environment across government has changed dramatically so my first priority would be to understand the current challenges and opportunities the team face delivering to federal, state, and local partners.

Growing 18Fs reach and spreading their practices more widely across the government will pay dividends for the public and taxpayers. Training and empowering government employees as product owners to lead software development projects, carefully balancing build vs. buy decisions; prioritizing the use of “agile contract formats,” creating iterative feedback loops in which providing value to users is the primary measure of success should continue to be top priorities. The pandemic also exposed profound weaknesses in the

technology systems relied on by state and local governments to administer federal programs such as unemployment insurance systems. As every level of government looks to build a more resilient digital infrastructure and better prepare for the next crisis, 18F is well positioned to play an important role in setting those modernization efforts up for success.

Within TTS, there are also opportunities for building and expanding reusable components and shared services that can be used across government. Finally, TTS's consultative teams — PIF, 18F, and COE — are increasingly helping agencies with service design and organizational design to help accelerate their modernization efforts.

64. How should GSA work with agencies to improve the acquisition of enhanced technological capabilities?

GSA should be the government's one-stop-shop for the acquisition of cost-effective, sustainable technology to enable agencies to carry out their missions. The goal is to lead the charge in modernizing the government's approach to technology products and services, which includes acquisition. GSA should also help educate agencies on build vs. buy opportunities and identify the most cost effective and high value approach for acquiring the services they need.

65. What factors limit the adoption of innovative business practices and IT solutions in the federal government? How can these factors be addressed?

An important element of digital transformation is technology, but it also requires changing outdated processes and practices. If confirmed, I look forward to leading a cultural change within the agency and encourage and empower teams to continually challenge the status quo, experiment, iterate and continuously improve.

66. GSA manages the Technology Modernization Fund (TMF) and reviews and approves projects that are funded in consultation with the TMF Board. What considerations should be included in evaluations of projects to ensure modernization projects prioritize cybersecurity?

Investments that modernize IT will almost always bolster cybersecurity, as outdated systems typically have greatly increased risks. I understand that the TMF released guidance indicating that one of the primary focuses of funding for the ARP funds will be cybersecurity. I look forward to learning more details about this program, if confirmed, and ensuring the focus moving forward will be on investments that move the government to a consistent baseline of maturity in cybersecurity and privacy protections, including addressing gaps uncovered in the recent SolarWinds incident.

67. Recently, OMB and GSA announced flexibility for repayment options for projects paid for out of the TMF.

- a. What is your understanding of the legal authority to make this decision?

As I understand, the enactment of the Modernizing Government Technology (MGT) Act authorized the TMF. As such, it provided GSA, in consultation with OMB, with the ability to establish the terms of repayment at levels sufficient to ensure the solvency of the Fund. With the recent emergency funding as provided through the ARP, the Administration is maximizing the flexibility of the TMF in order to be able to respond with urgency to the current crisis. I look forward to learning more, and welcome having further conversations with you or other Members of the committee on this topic, if given the opportunity to serve.

- b. What is your understanding of the conditions under which less than full repayment would be granted?

I have not been involved in the decision-making or planning of the use of additional funds to the TMF, however, I look forward to working closely with the Office of the Federal CIO, OMB, and the TMF Board and Program Management Office to ensure that the TMF enables the most impactful projects across the Federal Government.

Government-wide Policy

68. Recently, stewardship of regulations.gov passed from EPA to GSA. While progress has been made to improve the usability and security of the website, it still falls short in many areas. What do you believe are the most critical next steps in improving regulations.gov? Do you believe the current funding model will be sufficient?

Transparency and public involvement in government are staples of democracy. When an agency is promulgating a rule, it is essential that the process be open to the public and that they have an opportunity to provide their views to the agency. If confirmed, I look forward to working with GSA staff and partner agencies to constantly innovate on the citizen experience to provide more capability for regulations.gov and deter bots from posting fake comments. I know this is an issue that is of interest to this committee, and I look forward to working with you on this further.

69. How do you view the role of GSA's Office of Government-wide Policy? Do you see opportunities for the office to increase the value it brings to government?

The Office of Government-wide Policy (OGP) is set up to ensure that government-wide policies encourage agencies to develop and use the best, most cost-effective management practices. OGP has a great opportunity to increase its value by leveraging smart policy and data analytics to drive impact on key Administration priorities, including helping agencies better manage their assets and measure their operational performance.

V. Accountability

Whistleblower Protections

70. Protecting whistleblowers and their confidentiality is of the utmost importance to this Committee.
- a. Please describe any previous experience with handling whistleblower complaints. What steps did you take to ensure those individuals did not face retaliation and that their claims were thoroughly investigated?

As Missouri Secretary of State internal complaints were investigated according to procedures designed to ensure fair treatment of all parties while protecting the interests of the public.

- b. If confirmed, what steps will you take to ensure that whistleblower complaints are handled appropriately at GSA?

If confirmed, I'll work to create an environment of trust where agency employees feel safe speaking up about issues encountered in the workplace and where whistleblower complaints are fully investigated and, as appropriate, publicly reported.

- c. If confirmed, what steps will you take to ensure that whistleblowers at GSA do not face retaliation, that whistleblower identifiers are protected, and that complaints of retaliation are handled appropriately?

I look forward to assessing the current processes and procedures in place and working with the GSA Inspector General to ensure that whistleblowers are protected and that complaints of retaliation are handled appropriately.

Cooperation with Inspectors General

71. What is your view of the role of the GSA Office of Inspector General (OIG)? Please describe what you think the relationship between the GSA Administrator and the OIG should be. If confirmed, what steps would you take as Administrator to establish a working relationship with the Inspector General?

I respect the important role played by the Inspector General in providing independent, objective audits and investigations into GSA operations and programs and look forward to meeting regularly with the IG and exploring how best to establish a close working relationship to ensure GSA is delivering the best possible value to the public and taxpayers.

72. If confirmed, do you commit to ensuring that all recommendations made by the GSA Inspector General are reviewed, responded to, if necessary, and, unless the agency justifies its disagreements with the recommendations, implemented to the fullest extent possible within a reasonable time period?

Yes.

73. If confirmed, do you commit without reservation to ensuring the GSA OIG receives timely access to agency records and to interview agency employees?

Yes.

74. If confirmed, what steps will you take to ensure all GSA offices and employees cooperate fully and promptly with OIG requests?

If confirmed, I will work to identify any needed improvements or additional guidance to ensure that GSA employees cooperate fully and promptly with OIG. Transparency, accountability, and integrity are values I will bring to the Administrator role if confirmed, and I will lead by example and cooperate and respond to OIG as promptly as possible.

75. In January 2021, GSA's Office of Inspector General issued an alert memorandum detailing that GSA was impeding oversight of its COVID-19 activities. Specifically, the OIG found that GSA established a centralized review and approval process of all OIG audit inquiries that has compromised the integrity of information provided by GSA personnel. Additionally, GSA attempted to restrict and limit the audit team's access to information and resources. The OIG found that these actions have made it impossible to identify areas of improvement in the COVID response. If confirmed, what steps will you take to improve transparency into GSA's COVID-19 response?

If confirmed, I will look forward to exploring ways to improve the transparency of GSA operations, including those related to COVID-19 response.

Cooperation with GAO

76. If confirmed, do you commit without reservation to ensuring GAO receives timely, comprehensive responses to requests for information, including for records and meetings?

Yes.

77. If confirmed, do you commit to fully cooperate in a timely manner with any audits, investigations, and other reviews and related requests for information from GAO?

Yes.

78. If confirmed, what steps would you take to facilitate and encourage timely cooperation by federal agencies with GAO?

I value the GAO's responsibilities of assisting Congress to carry out their legislative, oversight, and financial controls of federal agencies' programs and operations, in an effort to make them more efficient and effective. If confirmed, I intend to meet with the

Comptroller General to understand GAO's relationship with GSA, and explore how best to address any recommended improvements or additional guidance to ensure that GSA employees cooperate with the GAO.

79. If confirmed, what steps will you take to ensure all GSA functions and employees cooperate fully and promptly with GAO requests?

If confirmed, I will work to identify any needed improvements or additional guidance to ensure that GSA employees cooperate fully and promptly with GAO. Transparency, accountability, and integrity are values I will bring to the Administrator role if confirmed, and I will lead by example and cooperate and respond to GAO as promptly as possible.

VI. Relations with Congress

80. Do you agree without reservation to comply with any request or summons to appear and testify before any duly constituted committee of Congress if you are confirmed?

Yes.

81. Do you agree without reservation to make any subordinate official or employee available to appear and testify before, or provide information to, any duly constituted committee of Congress if you are confirmed?

Yes.

82. Do you agree without reservation to comply fully, completely, and promptly to any request for documents, communications, or any other agency material or information from any duly constituted committee of the Congress if you are confirmed?

Yes, in accordance with the relevant laws and policies in place.

83. If confirmed, how will you make certain that you will respond in a timely manner to Member requests for information?

For me, having a good working relationship with Congress is a priority, and providing timely responses to Members assists with that goal. If confirmed, I will work with GSA staff to assess current processes and procedures and ensure they allow us to respond to Members as expeditiously as possible.

84. If confirmed, will you direct your staff to adopt a presumption of openness where practical, including identifying documents that can and should be proactively released to the public, without requiring a Freedom of Information Act request?

Yes, in accordance with the laws and policies in place.

85. If confirmed, will you keep this Committee apprised of new information if it materially impacts the accuracy of information your agency's officials have provided us?

Yes, in accordance with the laws and policies in place.

VII. Assistance

86. Are these answers completely your own? If not, who has provided you with assistance?

Yes, the answers are my own and based on technical assistance provided by GSA staff.

87. Have you consulted with GSA, or any other interested parties? If so, please indicate which entities.

Yes, GSA staff provided technical assistance in responding to these questions.

I, Robin Carnahan, hereby state that I have read the foregoing Pre-Hearing Questionnaire and that the information provided therein is, to the best of my knowledge, current, accurate, and complete.

DocuSigned by:

BB16B4E7421E4B8...
(Signature)

This 20th day of May, 2021

**Chairman Gary C. Peters
Post-Hearing Questions for the Record
Submitted to Robin Carnahan**

**Nominations of Robin Carnahan to be Administrator, General Services Administration;
Jen Easterly to be Director, Cybersecurity and Infrastructure Security Agency, DHS; and
Chris Inglis to be National Cyber Director
Thursday, June 10, 2021**

1. The General Services Administration is responsible for interpreting the Fly America Act, which sets forth requirements for the use of U.S.-flag carriers when federal employees and their dependents, contractors, grantees, and property engage in United States Government financed foreign air travel. If confirmed, will you commit to ensuring that GSA interprets and implements the Fly America Act to maximize the use of services provided by U.S. air carriers?

ANSWER: Yes, if confirmed, I commit to working with this Committee with respect to GSA's responsible and effective interpretation and implementation of the Fly America Act.

**Ranking Member Rob Portman
Post-Hearing Questions for the Record
Submitted to Robin Carnahan**

**Nominations of Robin Carnahan to be Administrator, General Services Administration;
Jen Easterly to be Director, Cybersecurity and Infrastructure Security Agency, DHS; and
Chris Inglis to be National Cyber Director
Thursday, June 10, 2021**

1. Do you think there are opportunities to improve ethics and transparency in government contracting? If so, how?

ANSWER: I believe there are a number of ways that the government could make improvements in contracting, especially when it comes to transparency around how businesses can work with government, how taxpayer dollars are spent, and how the procurement process works in general. Increasing transparency and simplifying the procurement process for stakeholders and the public can help lead to greater confidence in the system and more accountability from public officials. If confirmed, I look forward to partnering with the Committee on these efforts.

2. What can be done to reduce sole source contracting? What ethical concerns do you see with overbroad use of such authority?

ANSWER: Effective competition should be at the center of the government's procurement policies to ensure integrity, fairness, and openness in the procurement

process, as well as timely delivery for agency buyers and best value for taxpayers. If confirmed, I would welcome the opportunity to partner with the Committee on the appropriate use of sole source contracting.

3. Can you describe a recent governmental IT modernization effort that failed and what you would have done differently?

ANSWER: Unfortunately, it is not hard to find examples of failed government IT modernization efforts. GAO has consistently pointed to this as a challenging area for the federal government, releasing [report](#) after [report](#) identifying common challenges. GSA can play an important role in helping to identify common patterns and structural barriers to the successful execution of IT modernization projects - and work to address them.

As GAO has made clear, the lack of access to upfront capital can be a major impediment, particularly when modernizing legacy systems. The creation of the Technology Modernization Fund (TMF) was created in part to address that concern. If confirmed, I would look forward to collaborating closely with this Committee on the effective investment of TMF funds.

Ensuring that government agencies have sufficient in-house technology talent and access to government technology teams, like the Technology Transformation Services or US Digital Service, is another important component of setting technology modernization projects up for success. By empowering dedicated cross-functional teams to use, and oversee vendor teams using, modern delivery practices like user-centered design, agile development, incremental and continuous delivery, and automated testing, along with agile procurement and budgeting practices, agencies can reduce the risk and cost associated with IT modernization projects and speed the delivery of better results.

Besides putting the experience and needs of the public and system users at the center of all IT modernization efforts, clearly defining program goals and metrics for success, allowing teams enough flexibility to meet those goals, and requiring them to regularly deliver incremental value is the best way to ensure projects stay on track for success. You have my commitment that, if confirmed, I will work relentlessly to ensure that GSA, and the partner agencies it supports, are doing this every day.

4. Earlier this week, GSA briefed the Senate Homeland Security and Governmental Affairs Committee on GSA's Fiscal Year 2022 Budget Request. GSA expects the Administration's proposal to replace the average internal combustion engine government vehicle with an electric vehicle will cost the taxpayer an average of an additional \$27,000 more per vehicle. Of that number, \$20,000 would be for the additional cost of the vehicle and \$7,000 for the cost of charging infrastructure. To replace the existing federal fleet of 450,000 vehicles, this presents a total *additional* cost of more than \$12 billion on top of the cost of internal combustion vehicle replacement costs.

- a. Do you believe a \$27,000 premium paid for by the taxpayer is acceptable for the purchase of each new electric vehicle? Why or why not? What do you believe is an acceptable premium?

ANSWER: GSA's primary role in this area is to support partner agencies in procuring the vehicles needed to support their missions. Striking the right balance between the upfront cost of a vehicle and supporting the agency's mission will require regular and ongoing communication with agency partners.

At the same time, GSA should continuously monitor the market and be prepared to respond to changes. In recent months, we have seen major American car companies commit to an all-electric future. As the marketplace continues to transition, GSA should use its buying power to ensure taxpayers are getting the best possible value for vehicles it purchases.

- b. Do you believe American taxpayers it is acceptable for taxpayers to pay increased life-cycle costs for electric vehicles compared to internal combustion vehicles if it achieves the Biden Administration's federal fleet electrification priority?

ANSWER: I think that life-cycle costs are an important consideration for every investment an agency makes, whether that be real estate, technology, or products. In my experience, there is often an over-focus on initial costs and not enough focus on longer-term costs.

If confirmed, I would welcome the chance to look at the life-cycle costs of EVs, in particular, and work with this Committee to ensure we are striking the right balance.

- c. In pursuing the Biden Administration's priority to electrify the federal fleet, how will you balance emissions goals with taxpayer stewardship?

ANSWER: Throughout my career in public service, I have always prioritized effective stewardship of taxpayer dollars. If confirmed, I would want to make sure that GSA is always negotiating the best deal possible, period.

On this specific issue, I think GSA will need to balance agency mission needs, market availability, reduced environmental impact, and life-cycle costs - and I would welcome the opportunity to collaborate with the Committee on this.

Senator James Lankford
Post-Hearing Questions for the Record

Submitted to Robin Carnahan

**Nominations of Robin Carnahan to be Administrator, General Services Administration;
Jen Easterly to be Director, Cybersecurity and Infrastructure Security Agency, DHS; and
Chris Inglis to be National Cyber Director
Thursday, June 10, 2021**

Questions:

1) On telework and remote work:

- o GSA's mission is "to provide stewardship of the way the government uses and provides real estate, acquisition services, and technology." There is an opportunity in the days and months ahead to transform how the federal government approaches real property management.

What steps will you take to evaluate the federal government's real property needs for a more remote workforce?

ANSWER: It's my understanding that every federal agency is now in the process of developing plans for the reentry of employees and contractors to federal facilities, based on guidance provided by the Office of Management and Budget, in collaboration with the Office of Personnel Management and GSA.

I further understand that part of the planning will include consideration of increased telework and remote work opportunities for the federal workforce, based on the experiences of agencies over the last 15 months. The guidance also encourages agencies to begin thinking about ways to reimagine their workspaces.

From my perspective, this presents an important opportunity for GSA to work with agencies to deliver new, more efficient and innovative workspaces for the future, while at the same time benefit from cost savings from rightsizing the federal real estate portfolio. It also means GSA will need to develop new tools and services that better support a remote workforce.

The good news is that, as I understand it, GSA has a seat at the table alongside all of these agencies as they're pursuing this planning. That strikes me as the right first step. From there, if confirmed, I would want to engage with agencies to find opportunities for collaboration and co-location. It will also be important for GSA to sit down with agencies to review their current real estate portfolio and identify opportunities based on lease expiration dates, modernization needs, and new mission requirements. Concurrently, it will be important for GSA to engage early and often with local communities to make sure they are aware of and can incorporate local plans into GSA's portfolio planning efforts.

- o GSA's "Workplace 2030" initiative is reviewing the lessons learned over the past 15 months to meet the increased needs of a more remote workforce.

GSA needs to be ahead of the curve to support other agencies in a hybrid and remote work model. What steps does GSA need to take to ensure they can effectively support a federal workforce that is a mix of on-site and remote?

ANSWER: Organizations across all sectors are grappling with what their future demand for real estate will be based on potential changes to their workforces and workspaces in the months and years ahead, and particularly the challenge of leading a hybrid workforce.

From my vantage point, if confirmed, I think there are two things in particular I would want to see GSA do. First, GSA should serve as a model for new policies, practices, and solutions, and use feedback from those pilot projects to scale best practices across government. Second, GSA should actively engage with leading private sector partners to both understand what other organizations are doing, and to ensure that GSA is establishing new services and solutions that best serve partner agencies.

There is no doubt that these changes will require some rebalancing and investment in both federal facilities and in new and different technologies than those in use today. In the months ahead, I would expect GSA to work with customer agencies to help them in their planning efforts to determine what the future of work looks like for their agency, jointly create those plans, and help address their challenges.

- 2) I have heard several from CBP officials about issues with GSA's management of Ports of Entry. I'm concerned that our POEs are funded through the Federal Building Fund and have to compete with Federal buildings like courthouses and offices for funding. The needs of Federal courthouses are significantly different than the needs of our ports, which facilitate trade and travel and play a vital role in our nation's economy and security.

- o Are you aware of the issues between CBP and GSA?

ANSWER: I am aware of the unique and important role that land ports of entry (POEs) play in national security and international commerce. I am also aware of the challenges GSA has had in gaining full access to the rents it collects from agencies in the Federal Buildings Fund, and how the lack of full access has adversely affected GSA's ability to modernize its facilities to effectively serve many of its customer agencies, including the Department of Homeland Security.

- o Have you studied whether GSA's current management of our ports is the most effective way to do so?

ANSWER: I have not studied the issue, but I am aware that GSA manages a large and diverse real estate portfolio, which includes POEs, courthouses, laboratories, and the needs of law enforcement agencies, among others.

If confirmed, I will request briefings from the appropriate agency officials to learn more about this issue. I would also welcome the opportunity to engage with this Committee and study the issue further.

- o What steps should GSA take to improve the financing and management of ports of entry?

ANSWER: I think it is very important that GSA make smart and strategic investments with the rent that it collects to support its partner agencies. I also understand there has been bipartisan support for modernizing POEs.

If confirmed, I would want to make sure that GSA has a robust process in place to prioritize investments across its full portfolio of customer agencies, and that this process is informed by engagement with our customer agencies.

3) On Real Property Management:

- o Federal real property management is on the GAO High Risk list. The FAST Act established a Public Buildings Reform Board to identify and sell no less than five high-value real property assets. GAO notes that GSA, in conjunction with the Board, should complete the sale of OMB-approved high-value assets as required by the FAST Act.

What steps will you take to work with the Board and OMB to sell excess, high-value properties?

ANSWER: If confirmed, I look forward to engaging with stakeholders involved in the disposal of real property, including the Board and OMB, to ensure that we are meeting our statutory obligations and delivering excellent value to the American people. I know that the ultimate goal is to improve the management of our federal property in a transparent and collaborative way. I recognize GSA's important role in leading the Federal Government in optimizing its real property portfolio through effective disposition and utilization strategies, and I welcome the opportunity to work with Congress to administer our statutory obligations effectively.

- o There are tremendous cost savings in owning a building versus renting. The most notable example being the Department of Transportation building, which we rented for 15 years at \$50 million for a total of \$750 million. We then bought the building for about another \$750 on top of what we had already paid in rent. How will you prevent that situation from ever happening again?

ANSWER: I am aware of some of the challenges the Federal Government faces when it comes to the management of real property, but share your interest in GSA making sensible, strategic investments in the federal real property portfolio. If confirmed, I would engage with this Committee, as well as with GSA's other Committees of jurisdiction, to ensure that GSA is making those investments in places where there is a long-term or specialized federal need. I look forward to

working with Congress to make sure that the agency prioritizes smart and strategic investments that would help the Federal Government move from costly leased space to owned space.

**Written Statement of Jen Easterly
Nominee for Director of the Cybersecurity and Infrastructure Security Agency
Department of Homeland Security**

**Before the
U.S. Senate Committee on Homeland Security and Governmental Affairs**

10 June 2021

Chairman Peters, Ranking Member Portman, distinguished Members of the Committee, I am honored to appear before you to discuss my nomination for Director of the Cybersecurity and Infrastructure Security Agency (CISA). I want to thank the President for nominating me, Secretary Mayorkas for his confidence in me, and Congressman Gallagher for his kind introduction, and more importantly for his and Senator King's superb leadership of the Cyberspace Solarium Commission.

I also want to thank my parents: my father, Noel Koch, a Vietnam veteran whose forebears fought in the Civil War to ensure that the nation experienced "a new birth of freedom;" and my mother, Dr. June Koch, an English professor and the daughter of immigrants from Russia and Poland who came to America to enjoy that freedom. Both led lives of public service, instilling in me the importance of service and of actively participating in our great democratic project—to form, continuously, a more perfect union. Their example inspired me to commit twenty-seven years of my life in service to our Nation, including more than two decades in the United States Army, leading Soldiers in peacetime and in combat. It also motivates my return to public service after four and a half years in the private sector at one of our nation's leading financial institutions.

Additionally, I want to thank my husband Jas for his love and support over the past seventeen years, through multiple moves and four separate deployments. As a fellow U.S. Army combat veteran, I also want to thank him for his service to our country. And I especially want to recognize our son Jet, the light and joy of our life, who aspires to one day be President.

Twenty years ago, the attacks of 9/11 fundamentally altered the course of my life, as it did for so many. As noted by Tom Kean, Co-Chairman of the 9/11 Commission, "We were unprepared. We did not grasp the magnitude of a threat that had been gathering over a considerable period of time. This was a failure of policy, of management, of capability, and, above all, a failure of imagination." If the past year has taught us anything, it is the obligation we have as leaders to anticipate the unimaginable.

While the digital revolution of the past several decades enabled unprecedented growth and innovation, the increased connectivity also introduced great peril: nation-states and non-state actors alike now leverage cyberspace with near impunity to threaten our security, our privacy, and our physical and digital infrastructure. Our adversaries combine hacking with malign influence operations to interfere in democratic processes. They breach major corporations to steal capital and intellectual treasure, target industrial control systems to disrupt critical infrastructure, and incapacitate entities large and small with the scourge of ransomware. Even as

we contend with the billions of daily intrusions against our networks by malicious actors, I believe that as a nation, we remain at great risk of a catastrophic cyber-attack.

Congress established CISA in 2018 as the country's operational entity for managing and mitigating such risk, working closely with partners at State, Local, tribal, and territorial level, as well as with the private sector to ensure the security and resilience of our critical infrastructure.

Within the federal cyber ecosystem, CISA is the "quarterback," charged with protecting and defending federal civilian government networks; leading asset response for cyber incidents; and ensuring that timely and actionable information is shared across federal, non-federal, and industry partners.

In this context, I also thank this Committee for your leadership in establishing CISA, my friend Chris Krebs for his superb work in standing up the Agency, and Acting Director Wales and the dedicated men and women of CISA for their tireless efforts defending our infrastructure against a myriad of significant and serious threats, and ensuring secure, interoperable emergency communications. If confirmed, it will be the greatest honor of my career to join their incredible team, to continue building the culture and workforce of CISA, and to strengthen its capacity and capability to defend today and secure tomorrow.

The best quarterback, however, can't win a game alone; cyber is and must always be a team sport. CISA fulfills its lead operational role for national cyber and infrastructure resilience in collaboration with other agencies at every level of government and with our industry and international partners. A critical element of this ecosystem is the National Cyber Director, who will ensure a coherent and unified federal effort as the President's principal cyber advisor. If we are both confirmed, I look forward to working, once again, with Mr. Inglis. I also look forward to a productive and transparent partnership with this Committee.

I thank the Committee for considering my nomination and look forward to your questions.

REDACTED

HSGAC BIOGRAPHICAL QUESTIONS FOR EXECUTIVE NOMINEES

1. Basic Biographical Information

Please provide the following information.

<i>Position to Which You Have Been Nominated</i>					
<u>Name of Position</u>			<u>Date of Nomination</u>		
Director, Cybersecurity and Infrastructure Security Agency			April 22, 2021		

<i>Current Legal Name</i>			
<u>First Name</u>	<u>Middle Name</u>	<u>Last Name</u>	<u>Suffix</u>
Jennie	Margaret	Easterly	

<i>Addresses</i>					
<u>Residential Address</u> (do not include street address)			<u>Office Address</u> (include street address)		
			Street: 1 New York Plaza		
City: New York	State: NY	Zip: 10038	City: New York	State: NY	Zip: 10004

<i>Other Names Used</i>						
<u>First Name</u>	<u>Middle Name</u>	<u>Last Name</u>	<u>Suffix</u>	<u>Check if Married Name</u>	<u>Name Used From</u> (Month/Year) (Check box if estimate)	<u>Name Used To</u> (Month/Year) (Check box if estimate)
Jennie	Margaret	Koch		X	Est <input type="checkbox"/>	Est <input type="checkbox"/>
					06/1968	04/2004

<i>Birth Year and Place</i>	
<u>Year of Birth</u> (Do not include month and day.)	<u>Place of Birth</u>
1968	Philadelphia, Pennsylvania

<i>Marital Status</i>					
Check All That Describe Your Current Situation:					
Never Married	Married	Separated	Annulled	Divorced	Widowed
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

<i>Spouse's Name (current spouse only)</i>			
<u>Spouse's First Name</u>	<u>Spouse's Middle Name</u>	<u>Spouse's Last Name</u>	<u>Spouse's Suffix</u>
Jason	Tighe	Easterly	

<i>Spouse's Other Names Used (current spouse only)</i>						
<u>First Name</u>	<u>Middle Name</u>	<u>Last Name</u>	<u>Suffix</u>	<small>Check if Maiden Name</small>	<u>Name Used From</u> (Month/Year) (Check box if estimate)	<u>Name Used To</u> (Month/Year) (Check box if estimate)
N/A					Est <input type="checkbox"/>	Est <input type="checkbox"/>

<i>Children's Names (if over 18)</i>			
<u>First Name</u>	<u>Middle Name</u>	<u>Last Name</u>	<u>Suffix</u>
N/A			

I have one child under the age of 18.

2. Education

List all post-secondary schools attended.

<u>Name of School</u>	<u>Type of School</u> (vocational/technical/trade school, college/university/military college, correspondence/distance/extension/ online school)	<u>Date Began</u> <u>School</u> (month/year) (check box if estimate)	<u>Date Ended</u> <u>School</u> (month/year) (check box if estimate) (check "present" box if still in school)	<u>Degree</u>	<u>Date</u> <u>Awarded</u>
West Point	United States Military Academy	07/86 <input type="checkbox"/> Est	05/90 <input type="checkbox"/> Est <input type="checkbox"/> Present	B.S.	05/90
Oxford University	University	09/90 <input type="checkbox"/> Est	06/92 <input type="checkbox"/> Est <input type="checkbox"/> Present	M.A.	05/00
Military Intelligence Officer Basic Course	Military Education	09/92 <input checked="" type="checkbox"/> Est	03/93 <input checked="" type="checkbox"/> Est <input type="checkbox"/> Present	N/A	N/A
Military Intelligence Officer Advanced Course	Military Education	04/96 <input type="checkbox"/> Est	09/96 <input type="checkbox"/> Est <input type="checkbox"/> Present	N/A	N/A
Combined Arms Staff and Service School	Military Education	1997 <input checked="" type="checkbox"/> Est	1997 <input checked="" type="checkbox"/> Est <input type="checkbox"/> Present	N/A	N/A
Command and General Staff Course	Military Education	2004 <input checked="" type="checkbox"/> Est	2004 <input checked="" type="checkbox"/> Est <input type="checkbox"/> Present	N/A	N/A

3. Employment

(A) List all of your employment activities, including unemployment and self-employment. If the employment activity was military duty, list separate employment activity periods to show each change of military duty station. Do not list employment before your 18th birthday unless to provide a minimum of two years of employment history.

<u>Type of Employment</u> (Active Military Duty Station, National Guard/Reserve, USPHS Commissioned Corps, Other Federal employment, State Government (Non-Federal Employment), Self-employment, Unemployment, Federal Contractor, Non-Government Employment (excluding self-employment), Other)	<u>Name of Your Employer/Assigned Duty Station</u>	<u>Most Recent Position Title/Rank</u>	<u>Location</u> (City and State only)	<u>Date Employment Began</u> (month/year) (check box if estimate)	<u>Date Employment Ended</u> (month/year) (check box if estimate) (check "present" box if still employed)
Non-Government Employee	Morgan Stanley	Managing Director	New York, NY	02/17 Est <input type="checkbox"/>	Present Est <input type="checkbox"/>
Non-Government Employee	Biden-Harris Transition	Volunteer, Cyber Policy Team Lead	Washington, D.C.	09/20	01/21
Federal Employee	National Security Council	Special Assistant to the President and Senior Director for Counterterrorism/SES	Washington, D.C.	10/13 Est <input type="checkbox"/>	12/16 Est <input type="checkbox"/>
Federal Employee	National Security Agency	Deputy for Counterterrorism/SES	Fort Meade, MD	09/11 Est <input type="checkbox"/>	10/13 Est <input type="checkbox"/>
Active Military Duty Station	U.S. Army/Fort Meade, MD	Deputy for Counterterrorism/O-5	Fort Meade, MD	04/11	09/11
Active Military Duty Station	U.S. Army/International Security Assistance Force	Cyber Advisor/O-5	Kabul, AF	09/10 Est <input type="checkbox"/>	04/11 Est <input type="checkbox"/>
Active Military	U.S. Army/Fort Meade, MD	Training	N/A	06/10	09/10
Active Military Duty Station	U.S. Army/Fort Meade, MD	Battalion Commander/ O-5	Fort Meade, MD	06/08 Est <input type="checkbox"/>	06/10 Est <input type="checkbox"/>
Active Military Duty Station	U.S. Army/Fort Meade, MD	Director, NSA Fellow/O-5	Fort Meade, MD and Iraq	09/07 Est <input type="checkbox"/>	06/08 Est <input type="checkbox"/>

Active Military Duty Station	U.S. Army/Multi-National Forces, Iraq	Chief, Cryptologic Services Group/O-5	Baghdad, Iraq	11/06 Est <input type="checkbox"/>	08/07 Est <input type="checkbox"/>
Active Military	U.S. Army/Fort Meade, MD	Training	N/A	07/06	11/06
Active Military Duty Station	U.S. Army/Fort Meade, MD	Brigade Operations Officer/O-4	Fort Meade, MD	07/05 Est <input type="checkbox"/>	07/06 Est <input type="checkbox"/>
Active Military Duty Station	U.S. Army/Fort Meade, MD	Battalion Executive Officer/O-4	Fort Meade, MD	07/04 Est <input type="checkbox"/>	06/05 Est <input type="checkbox"/>
Active Military Duty Station	U.S. Army/White House	Executive Assistant/O-4	The White House, D.C.	06/02 Est <input type="checkbox"/>	06/04 Est <input type="checkbox"/>
Active Military Duty Station	U.S. Army/West Point	Assistant Professor/O-3 and O-4	West Point, NY and Kosovo	01/00 Est <input type="checkbox"/>	05/02 Est <input type="checkbox"/>
Active Military	U.S. Army	Leave	N/A	11/99	01/00
Active Military Duty Station	U.S. Army/XVIII Airborne Corps	Army Officer/O-3	Fort Bragg, NC and Bosnia	10/96 Est <input type="checkbox"/>	11/99 Est <input type="checkbox"/>
Active Military Duty Station	U.S. Army/Military Intelligence School	Army Officer/O-3	Fort Huachuca, AZ	04/96 Est <input type="checkbox"/>	09/96 Est <input type="checkbox"/>
Active Military Duty Station	U.S. Army/25 th Infantry Division	Army Officer/O-2 and O-3	Schofield Barracks, Hawaii and Haiti	04/93 Est <input type="checkbox"/>	03/96 Est <input type="checkbox"/>
Active Military Duty Station	U.S. Army/Military Intelligence School	Army Officer/O-2	Fort Huachuca, AZ	09/92 Est <input type="checkbox"/>	03/93 Est <input type="checkbox"/>

(B) List any advisory, consultative, honorary or other part-time service or positions with federal, state, or local governments, not listed elsewhere.

<u>Name of Government Entity</u>	<u>Name of Position</u>	<u>Date Service Began</u> (month/year) (check box if estimate)	<u>Date Service Ended</u> (month/year) (check box if estimate) (check "present" box if still serving)
N/A		Est <input type="checkbox"/>	Est Present <input type="checkbox"/> <input type="checkbox"/>

4. Potential Conflict of Interest

(A) Describe any business relationship, dealing or financial transaction which you have had during the last 10 years, whether for yourself, on behalf of a client, or acting as an agent, that could in any way constitute or result in a possible conflict of interest in the position to which you have been nominated.

In connection with the nomination process, I have consulted with the Office of Government Ethics and the Department of Homeland Security's Designated Agency Ethics Official to identify any potential conflicts of interest. Any potential conflicts of interest will be resolved in accordance with the terms of an ethics agreement that I will sign and transmit to the Department's Designated Agency Ethics Official, which will be provided to this Committee. I am not aware of any other potential conflicts of interest.

(B) Describe any activity during the past 10 years in which you have engaged for the purpose of directly or indirectly influencing the passage, defeat or modification of any legislation or affecting the administration or execution of law or public policy, other than while in a federal government capacity.

None.

5. Honors and Awards

List all scholarships, fellowships, honorary degrees, civilian service citations, military medals, academic or professional honors, honorary society memberships and any other special recognition for outstanding service or achievement.

Rhodes Scholarship, 1990
 Council on Foreign Relations International Affairs Fellowship, 2002
 George S. Franklin Fellowship, 2002
 Director, National Security Agency Fellowship, 2007
 New America Foundation Senior International Security Fellow, 2018
 Visiting Fellow, National Security Institute at George Mason University's Antonin Scalia School of Law, 2018
 Aspen Institute Finance Leaders Fellow, 2018
 Council on Foreign Relations, Lifetime Member, 2008 and Term Member, 2000
 French-American Foundation Young Leader, 2003
 Council for U.S. – Italy Young Leader, 2008
 James W. Foley Legacy Foundation American Hostage Freedom Award, 2018
 MAKER @ Morgan Stanley, 2020
 Bradley W. Snyder Changing the Narrative Award, 2020

Military Awards:

Legion of Merit, 2011
 Bronze Star Medal (2 awards), 2011, 2007
 Defense Meritorious Service Medal (2 awards), 2010, 2004
 Meritorious Service Medal (4 awards), 2010, 2002, 1999, 1997
 Army Commendation Medal (3 awards), 2006, 1996, 1995
 Joint Service Achievement Medal, 1995
 Army Achievement Medal (2 awards), 2000, 1994
 Joint Service Commendation Medal, 2007
 Afghanistan Campaign Medal, 2011
 Humanitarian Service Medal, 1995
 Armed Forces Expeditionary Medal, 1995
 National Defense Service Medal, 1990
 NATO Medal (2 awards), 1997, 2011
 Military Outstanding Volunteer Medal, 2001
 Iraq Campaign Medal, 2007
 Kosovo Campaign Medal, 2000
 United Nations Mission in Haiti Medal, 1995
 Knowlton Award, 2005
 Senior Parachutist Badge, 1999
 Airborne Badge (Distinguished Honor Graduate), 1990
 Presidential Service Badge, 2002
 Air Assault Badge, 1988

6. Memberships

List all memberships that you have held in professional, social, business, fraternal, scholarly, civic, or charitable organizations in the last 10 years.

Unless relevant to your nomination, you do NOT need to include memberships in charitable organizations available to the public as a result of a tax-deductible donation of \$1,000 or less, Parent-Teacher Associations or other organizations connected to schools attended by your children, athletic clubs or teams, automobile support organizations (such as AAA), discounts clubs (such as Groupon or Sam's Club), or affinity memberships/consumer clubs (such as frequent flyer memberships).

<u>Name of Organization</u>	<u>Dates of Your Membership</u> (You may approximate.)	<u>Position(s) Held</u>
Morgan Stanley Foundation	March 2017 to Present	Member, Board of Trustees
Nuru International	April 2017 to Present	Member, Board of Directors

James W. Foley Legacy Foundation	September 2018 to Present	Member, Board of Directors
Theorem Media	April 2019 to Present	Member, Board of Directors
Council on Foreign Relations	2008 to Present 2000 to 2005	Lifetime Member Term Member
American Association of Rhodes Scholars	1992 to Present	Member
French American Foundation	2003 to Present	Young Leader
Aspen Institute	June 2018 to Present	Finance Leaders Fellow
New America Foundation	April 2018 to Present	Senior International Security Fellow
National Security Institute at George Mason University's Antonin Scalia School of Law	September 2018 to Present	Visiting Fellow
Firstwave	2008 to Present	Member
Hostage U.S.	2018 to Present	Advisory Board Member
Council for U.S. and Italy	2008	Young Leader
Omicron Delta Epsilon International Society in Economics	2001	Member
Omicron Delta Kappa Leadership Honor Society	1990	Member
Phi Kappa Phi Honor Society	1989	Member

7. Political Activity

(A) Have you ever been a candidate for or been elected or appointed to a political office?

<u>Name of Office</u>	<u>Elected/Appointed/ Candidate Only</u>	<u>Year(s) Election Held or Appointment Made</u>	<u>Term of Service (if applicable)</u>
N/A			

(B) List any offices held in or services rendered to a political party or election committee during the last ten years that you have not listed elsewhere.

<u>Name of Party/Election Committee</u>	<u>Office/Services Rendered</u>	<u>Responsibilities</u>	<u>Dates of Service</u>
N/A			

(C) Itemize all individual political contributions of \$200 or more that you have made in the past five years to any individual, campaign organization, political party, political action committee, or similar entity. Please list each individual contribution and not the total amount contributed to the person or entity during the year.

<u>Name of Recipient</u>	<u>Amount</u>	<u>Year of Contribution</u>
N/A		

8. Publications and Speeches

(A) List the titles, publishers and dates of books, articles, reports or other published materials that you have written, including articles published on the Internet. Please provide the Committee with copies of all listed publications. In lieu of hard copies, electronic copies can be provided via e-mail or other digital format.

<u>Title</u>	<u>Publisher</u>	<u>Date(s) of Publication</u>
Recruiting, Development, and Retention of Cyber Warriors https://smallwarsjournal.com/blog/journal/docs-temp/482-conti-easterly.pdf	Small Wars Journal	June 2010, w/Greg Conti
The Islamic State and the End of Lone-Wolf Terrorism https://foreignpolicy.com/2017/05/23/the-islamic-state-and-the-end-of-lone-wolf-terrorism/	Foreign Policy	May 2017, w/Josh Geltzer
More Die in Bathtubs Than in Terrorism. It's Still Worth Spending Billions to Fight It https://www.cnn.com/2017/05/21/opinions/deadly-bathtub-compared-to-terrorism-opinion-geltzer-easterly/index.html	CNN	May 2017 w/Josh Geltzer
Mr. President, Don't Forget Other Americans Held Unjustly Overseas https://www.cnn.com/2017/06/13/opinions/dont-forget-hostages-opinion-easterly-geltzer	CNN	June 2017 w/Josh Geltzer
Trump and Obama Have Something in Common When it Comes to U.S Hostages Overseas https://www.washingtonpost.com/news/global-opinions/wp/2018/06/22/trump-and-obama-have-something-in-common-when-it-comes-to-u-s-hostages-held-overseas/	Washington Post	June 2018 w/Josh Geltzer, Luke Hartig, and Chris Costa
Empathy Matters: Leadership in Cyber https://www.justsecurity.org/64850/empathy-matters-leadership-in-cyber/	Just Security	July 2019, w/Whitney Kassel
Nation Must Act Now to Ensure Fair Elections in November https://www.usatoday.com/story/opinion/2020/08/19/fair-elections-risk-nation-must-act-now-military-veterans-column/5598664002/	USA Today	August 2020, w/Greg Behrman et al

Invictus: The Poetry of a Pandemic https://www.linkedin.com/pulse/invictus-poetry-pandemic-jen-easterly/	LinkedIn	April 2020
The Last Human Freedom https://www.linkedin.com/pulse/last-human-freedom-jen-easterly/	LinkedIn	April 2020
Reflections on Memorial Day 2020 https://www.linkedin.com/pulse/reflections-memorial-day-2020-jen-easterly/	LinkedIn	May 2020
Tied in a Single Garment of Destiny https://www.linkedin.com/pulse/tied-single-garment-destiny-jen-easterly/	LinkedIn	June 2020

(B) List any formal speeches you have delivered during the last five years and provide the Committee with copies of those speeches relevant to the position for which you have been nominated. Include any testimony to Congress or any other legislative or administrative body. These items can be provided electronically via e-mail or other digital format.

Title/Topic	Place/Audience	Date(s) of Speech
Morgan Stanley Minute: Cybersecurity in the Connected Age https://www.morganstanley.com/morgan-stanley-minute/cyber-security?vid=6046486469001	Morgan Stanley Website Video	July 2019
Morgan Stanley Minute: Deconstructing Deepfakes https://www.morganstanley.com/morgan-stanley-minute/deconstructing-deepfakes?vid=6152672802001	Morgan Stanley Website Video	April 2020
Fireside Chat - Countering Terrorism in the Age of Social Media https://www.youtube.com/watch?v=zpjS7Wh5KcM	San Francisco, CA; Cloudflare Summit	September 2016
Glasgow Information Technology Director's Leadership Dinner	Glasgow, Scotland	June 2017
Fireside Chat on Leadership	San Diego, California; Morgan Stanley Client Event	November 2017
Cyber 9-12, Fireside Chat	Columbia School of International & Political Affairs; New York, NY	November 2017

How Can the U.S. Ensure it Wins the Cyber War of 2028? https://www.youtube.com/watch?v=EykbbwUL3Y0	Washington, D.C.; New America Foundation Future of War Conference	April 2018
Cybersecurity's New Game of Risk https://www.youtube.com/watch?v=ETX6F3_Ri7I	Aspen, Colorado; Fortune Brainstorm Tech	July 2018
Annual Counterterrorism Lecture, West Point, 2018 https://ctc.usma.edu/jen-easterly-delivers-address-cadets-annual-ctc-yearling-lecture/	West Point, NY; West Point Class of 2021	December 2018
Safeguarding Your Data in an Increasingly Complex World	New York, NY; Morgan Stanley Client Investment Management Leadership Conference	January 2019
Fireside Chat on Leadership with GEN (Retired) Stanley McChrystal	Palm Beach, Florida; Morgan Stanley Client Event	January 2019
West Point to the West Wing to Wall Street: Leadership in a Complex World	West Point, NY; Jean Bartik Computing Symposium	January 2019
Safeguarding Data in an Increasingly Complex World	New York, NY; NYPD Cyber Intelligence and Counterterrorism Conference	February 2019
Modern Warfare Institute Podcast: Women in National Security https://mwi.usma.edu/mwi-podcast-women-national-security/	Modern Warfare Institute, West Point, NY	March 2019
Defeating ISIS: What are the Lessons for the Future? https://www.youtube.com/watch?v=zK5QUUqiDRY	Washington, D.C.; New American Foundation Future Security Forum	April 2019
Fireside Chat on Leadership in Cyber	New York, NY; Columbia SIPA Cyber Risk to Financial Stability Conference	April 2019
Beyond the Breach Podcast: Leadership and Resilience in the Digital Age https://player.fm/series/beyond-the-breach	Podcast	2019
Remarks on Cybernation https://www.youtube.com/watch?v=NJNfMpydKcE	Colorado Springs, CO; Joint Service Academy Cyber Security Summit	April 2019
Safeguarding Data in an Increasingly Complex World	New York, NY; Institutional Insurance Group	May 2019
Panel on Cyber Threats to the Payments System	New York, NY; Federal Reserve Bank of NY Payments Risk Committee	June 2019

Safeguarding Data in an Increasingly Complex World	Austin, Texas; Texas Teachers Retirement System	June 2019
Safeguarding Data in an Increasingly Complex World	Montreal, Canada: Canada FinTech Forum	October 2019
Women in Tech Show: Cybersecurity and Financial Services https://thewomenintechshow.com/2020/02/03/cybersecurity-and-financial-services-with-jen-easterly/	Orlando, FL; Podcast	October 2019
The Imagination Coefficient, Leadership in Counterterrorism & Cyber https://www.youtube.com/watch?v=Tu6KbrD--Sc	Orlando, FL; Grace Hopper Celebration	October 2019
Safeguarding Data in an Increasingly Complex World	Montreal, Canada: Google-Morgan Stanley Women in Technology Event	November 2019
A Veteran's Journey to Morgan Stanley https://www.youtube.com/watch?v=kUsGJJvQTNg	Morgan Stanley YouTube Channel	Posted November 11, 2019
Morgan Stanley's 85 th Anniversary: Epilogue https://www.youtube.com/watch?v=fdErGSL09O0	Morgan Stanley YouTube Channel	Posted September 16, 2020
Are you Cyber Secure? (Panel)	Virtual; NASSCOM Technology & Leadership Forum	February 2021

To the best of my abilities, I have taken steps to recall and report the formal speaking engagements I participated in for the specified period of time. On many occasions, I provided informal remarks, participated in panel discussions or otherwise spoke without written remarks prepared in advance. If additional materials are identified, those materials will be reported promptly to the Committee.

(C) List all speeches and testimony you have delivered in the past ten years, except for those the text of which you are providing to the Committee.

Nothing additional to report.

<u>Title</u>	<u>Place/Audience</u>	<u>Date(s) of Speech</u>
N/A		

9. Criminal History

Since (and including) your 18th birthday, has any of the following happened?

- Have you been issued a summons, citation, or ticket to appear in court in a criminal proceeding against you? (Exclude citations involving traffic infractions where the fine was less than \$300 and did not include alcohol or drugs.)
No.
- Have you been arrested by any police officer, sheriff, marshal or any other type of law enforcement official?
No.
- Have you been charged, convicted, or sentenced of a crime in any court?
No.
- Have you been or are you currently on probation or parole?
No.
- Are you currently on trial or awaiting a trial on criminal charges?
No.
- To your knowledge, have you ever been the subject or target of a federal, state or local criminal investigation?
No.

If the answer to any of the questions above is yes, please answer the questions below for each criminal event (citation, arrest, investigation, etc.). If the event was an investigation, where the question below asks for information about the offense, please offer information about the offense under investigation (if known).

N/A

A) Date of offense:

a. Is this an estimate (Yes/No):

B) Description of the specific nature of the offense:

C) Did the offense involve any of the following?

- 1) Domestic violence or a crime of violence (such as battery or assault) against your child, dependent, cohabitant, spouse, former spouse, or someone with whom you share a child in common: **Yes / No**
- 2) Firearms or explosives: **Yes / No**
- 3) Alcohol or drugs: **Yes / No**

D) Location where the offense occurred (city, county, state, zip code, country):

E) Were you arrested, summoned, cited or did you receive a ticket to appear as a result of this offense by any police officer, sheriff, marshal or any other type of law enforcement official: **Yes / No**

- 1) Name of the law enforcement agency that arrested/cited/summoned you:
 - 2) Location of the law enforcement agency (city, county, state, zip code, country):
- F) As a result of this offense were you charged, convicted, currently awaiting trial, and/or ordered to appear in court in a criminal proceeding against you: **Yes / No**
- 1) If yes, provide the name of the court and the location of the court (city, county, state, zip code, country):
 - 2) If yes, provide all the charges brought against you for this offense, and the outcome of each charged offense (such as found guilty, found not-guilty, charge dropped or "nolle pros," etc). If you were found guilty of or pleaded guilty to a lesser offense, list separately both the original charge and the lesser offense:
 - 3) If no, provide explanation:
- G) Were you sentenced as a result of this offense: **Yes / No**
- H) Provide a description of the sentence:
- I) Were you sentenced to imprisonment for a term exceeding one year: **Yes / No**
- J) Were you incarcerated as a result of that sentence for not less than one year: **Yes / No**
- K) If the conviction resulted in imprisonment, provide the dates that you actually were incarcerated:
- L) If conviction resulted in probation or parole, provide the dates of probation or parole:
- M) Are you currently on trial, awaiting a trial, or awaiting sentencing on criminal charges for this offense: **Yes / No**
- N) Provide explanation:

10. Civil Litigation and Administrative or Legislative Proceedings

(A) Since (and including) your 18th birthday, have you been a party to any public record civil court action or administrative or legislative proceeding of any kind that resulted in (1) a finding of wrongdoing against you, or (2) a settlement agreement for you, or some other person or entity, to make a payment to settle allegations against you, or for you to take, or refrain from taking, some action. Do NOT include small claims proceedings.

No.

<u>Date Claim/Suit Was Filed or Legislative Proceedings Began</u>	<u>Court Name</u>	<u>Name(s) of Principal Parties Involved in Action/Proceeding</u>	<u>Nature of Action/Proceeding</u>	<u>Results of Action/Proceeding</u>
N/A				

(B) In addition to those listed above, have you or any business of which you were an officer, director or owner ever been involved as a party of interest in any administrative agency proceeding or civil litigation? Please identify and provide details for any proceedings or civil litigation that involve actions taken or omitted by you, or alleged to have been taken or omitted by you, while serving in your official capacity.

No.

<u>Date Claim/Suit Was Filed</u>	<u>Court Name</u>	<u>Name(s) of Principal Parties Involved in Action/Proceeding</u>	<u>Nature of Action/Proceeding</u>	<u>Results of Action/Proceeding</u>
N/A				

(C) For responses to the previous question, please identify and provide details for any proceedings or civil litigation that involve actions taken or omitted by you, or alleged to have been taken or omitted by you, while serving in your official capacity.

N/A

11. Breach of Professional Ethics

(A) Have you ever been disciplined 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? Exclude cases and proceedings already listed.

No.

<u>Name of Agency/Association/ Committee/Group</u>	<u>Date Citation/Disciplinary Action/Complaint Issued/Initiated</u>	<u>Describe Citation/Disciplinary Action/Complaint</u>	<u>Results of Disciplinary Action/Complaint</u>
N/A			

(B) Have you ever been fired from a job, quit a job after being told you would be fired, left a job by mutual agreement following charges or allegations of misconduct, left a job by mutual agreement following notice of unsatisfactory performance, or received a written warning, been officially reprimanded, suspended, or disciplined for misconduct in the workplace, such as violation of a security policy?

No.

12. Tax Compliance

(This information will not be published in the record of the hearing on your nomination, but it will be retained in the Committee's files and will be available for public inspection.)

REDACTED

13. Lobbying

In the past ten years, have you registered as a lobbyist? If so, please indicate the state, federal, or local bodies with which you have registered (e.g., House, Senate, California Secretary of State).

No.

14. Outside Positions

☒ See OGE Form 278. (If, for your nomination, you have completed an OGE Form 278 Executive Branch Personnel Public Financial Disclosure Report, you may check the box here to complete this section and then proceed to the next section.)

For the preceding ten calendar years and the current calendar year, report any positions held, whether compensated or not. Positions include but are not limited to those of an officer, director, trustee, general partner, proprietor, representative, employee, or consultant of any corporation, firm, partnership, or other business enterprise or any non-profit organization or educational institution. Exclude positions with religious, social, fraternal, or political entities and those solely of an honorary nature.

<u>Name of Organization</u>	<u>Address of Organization</u>	<u>Type of Organization</u> (corporation, firm, partnership, other business enterprise, other non-profit organization, educational institution)	<u>Position Held</u>	<u>Position Held From</u> (month/year)	<u>Position Held To</u> (month/year)

15. Agreements or Arrangements

☒ See OGE Form 278. (If, for your nomination, you have completed an OGE Form 278 Executive Branch Personnel Public Financial Disclosure Report, you may check the box here to complete this section and then proceed to the next section.)

As of the date of filing your OGE Form 278, report your agreements or arrangements for: (1) continuing participation in an employee benefit plan (e.g. pension, 401k, deferred compensation); (2) continuation of payment by a former employer (including severance payments); (3) leaves of absence; and (4) future employment.

Provide information regarding any agreements or arrangements you have concerning (1) future employment; (2) a leave of absence during your period of Government service; (3) continuation of payments by a former employer other than the United States Government;

and (4) continuing participation in an employee welfare or benefit plan maintained by a former employer other than United States Government retirement benefits.

<u>Status and Terms of Any Agreement or Arrangement</u>	<u>Parties</u>	<u>Date</u> (month/year)

16. Additional Financial Data

All information requested under this heading must be provided for yourself, your spouse, and your dependents. (This information will not be published in the record of the hearing on your nomination, but it will be retained in the Committee's files and will be available for public inspection.)

REDACTED

REDACTED

SIGNATURE AND DATE

I hereby state that I have read the foregoing Statement on Biographical and Financial Information and that the information provided therein is, to the best of my knowledge, current, accurate, and complete.

A handwritten signature in black ink, consisting of a stylized 'J' followed by a series of loops and a final flourish.

This 29th day of April, 2021

REDACTED

UNITED STATES OFFICE OF
GOVERNMENT ETHICS

May 5, 2021

The Honorable Gary C. Peters
Chairman
Committee on Homeland Security
and Governmental Affairs
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

In accordance with the Ethics in Government Act of 1978, I enclose a copy of the financial disclosure report filed by Jennie Easterly, who has been nominated by President Biden for the position of Director, Cybersecurity and Infrastructure Security Agency, Department of Homeland Security.

We have reviewed the report and have obtained advice from the agency concerning any possible conflict in light of its functions and the nominee's proposed duties. Also enclosed is an ethics agreement outlining the actions that the nominee will undertake to avoid conflicts of interest. Unless a date for compliance is indicated in the ethics agreement, the nominee must fully comply within three months of confirmation with any action specified in the ethics agreement.

Based thereon, we believe that this nominee is in compliance with applicable laws and regulations governing conflicts of interest.

Sincerely,

DAVID APOL

Digitally signed by DAVID
APOL
Date: 2021.05.05 13:37:11
-04'00'

David J. Apol
General Counsel

Enclosures REDACTED



April 25, 2021

Joseph B. Maher
Designated Agency Ethics Official
U.S. Department of Homeland Security
2707 Martin Luther King, Jr. Avenue, SE
Washington, DC 20528

Dear Mr. Maher:

The purpose of this letter is to describe the steps that I will take to avoid any actual or apparent conflict of interest in the event that I am confirmed for the position of Director for the Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security. It is my responsibility to understand and comply with commitments outlined in this agreement.

SECTION I – GENERAL COMMITMENTS

As required by the criminal conflicts of interest law at 18 U.S.C. § 208(a), I will not participate personally and substantially in any particular matter in which I know that I have a financial interest directly and predictably affected by the matter, or in which I know that a person whose interests are imputed to me has a financial interest directly and predictably affected by the particular matter, unless I first obtain a written waiver, pursuant to 18 U.S.C. § 208(b)(1), or qualify for a regulatory exemption, pursuant to 18 U.S.C. § 208(b)(2). I understand that the interests of the following persons are imputed to me:

- Any spouse or minor child of mine;
- Any general partner of a partnership in which I am a limited or general partner;
- Any organization in which I serve as an officer, director, trustee, general partner, or employee; and
- Any person or organization with which I am negotiating or have an arrangement concerning prospective employment.

In the event that an actual or potential conflict of interest arises during my appointment, I will consult with an agency ethics official and take the measures necessary to resolve the conflict, such as recusal from the particular matter or divestiture of an asset.

If I have a managed account or otherwise use the services of an investment professional during my appointment, I will ensure that the account manager or investment professional obtains my prior approval on a case-by-case basis for the purchase of any assets other than cash, cash equivalents, investment funds that qualify for the regulatory exemption for diversified mutual funds and unit investment trusts at 5 C.F.R. § 2640.201(a), obligations of the United States, or municipal bonds.

I will receive a live ethics briefing from a member of the ethics office after my confirmation but not later than 15 days after my appointment pursuant to the ethics program regulation at 5 C.F.R. § 2638.305. Within 90 days of my confirmation, I will submit my

Certification of Ethics Agreement Compliance which documents my compliance with this ethics agreement.

I understand that as an appointee I will be required to sign the Ethics Pledge (Exec. Order No. 13989) and that I will be bound by it. Among other obligations, I will be required to recuse from particular matters involving specific parties involving my former employer or former clients for a period of two years after I am appointed, with the exception of federal, state and local government.

I will not modify this ethics agreement without your approval and the approval of the U.S. Office of Government Ethics pursuant to the ethics agreement requirements contained in the financial disclosure regulation at 5 C.F.R. § 2634.803(a)(4).

SECTION 2 – MORGAN STANLEY

Upon confirmation, I will resign from my position with Morgan Stanley. I hold unvested restricted stock units through the Equity Incentive Compensation Plan (EICP). I also have an unvested deferred cash bonus receivable, which is held through the Morgan Stanley Compensation Incentive Plan (MSCIP).

Pursuant to the standard provisions of these plans, upon my resignation, my restricted stock units and my deferred cash bonus receivable will vest. TheEICP restricted stock units will convert to common shares of Morgan Stanley stock, which I will divest as soon as practicable but not later than 90 days after my confirmation. I will not participate personally and substantially in any particular matter that to my knowledge has a direct and predictable effect on the financial interests of Morgan Stanley until I have divested the stock, unless I first obtain a written waiver, pursuant to 18 U.S.C. § 208(b)(1), or qualify for a regulatory exemption, pursuant to 18 U.S.C. § 208(b)(2). I have verified that I will be able to carry out the divestiture within the timeframe described above. The MSCIP deferred cash bonus receivable will be fixed as of the date of my resignation and paid to me within 30 days. In the event that I divest my Morgan Stanley stock before receiving this bonus, I will not participate personally and substantially in any particular matter that to my knowledge has a direct and predictable effect on the ability or willingness of Morgan Stanley to make this payment, unless I first obtain a written waiver, pursuant to 18 U.S.C. § 208(b)(1).

In addition, pursuant to the impartiality regulation at 5 C.F.R. § 2635.502, for a period of one year after my resignation, I will not participate personally and substantially in any particular matter involving specific parties in which I know that Morgan Stanley is a party or represents a party, unless I am first authorized to participate, pursuant to 5 C.F.R. § 2635.502(d).

SECTION 3 – ADDITIONAL NON-FEDERAL POSITIONS

Upon confirmation, I will resign from my positions with the following entities:

- Morgan Stanley Foundation
- Nuru International

- James W. Foley Legacy Foundation
- Theorem Media
- New America Foundation
- National Security Institute at GMU Antonin Scalia Law School
- The Aspen Institute

My position with PT Fund, Inc. (Biden-Harris Transition Team) ended in January 2021. Pursuant to the impartiality regulation at 5 C.F.R. § 2635.502, for a period of one year after my position with each of these entities ended, I will not participate personally and substantially in any particular matter involving specific parties in which I know that entity is a party or represents a party, unless I am first authorized to participate, pursuant to 5 C.F.R. § 2635.502(d).

SECTION 4 – SPOUSE EMPLOYMENT

My spouse is employed by Empire State Development/New York State Department of Economic Development in a position for which he receives a fixed annual salary. Pursuant to the impartiality regulation at 5 C.F.R. § 2635.502, for as long as my spouse continues to work for Empire State Development/New York State Department of Economic Development, I will not participate personally and substantially in any particular matter involving specific parties in which I know Empire State Development/New York State Department of Economic Development is a party or represents a party, unless I am first authorized to participate, pursuant to 5 C.F.R. § 2635.502(d).

SECTION 5 – OTHER FINANCIAL INTERESTS

As soon as practicable but not later than 90 days after my confirmation, I will divest my interests in the entities listed in Appendix A. With regard to each of these entities, I will not participate personally and substantially in any particular matter that to my knowledge has a direct and predictable effect on the financial interests of the entity until I have divested it, unless I first obtain a written waiver, pursuant to 18 U.S.C. § 208(b)(1), or qualify for a regulatory exemption, pursuant to 18 U.S.C. § 208(b)(2). I have verified that I will be able to carry out the divestitures within the timeframe described above.

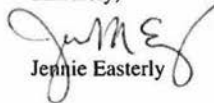
I understand that I may be eligible to request a Certificate of Divestiture for qualifying assets and that a Certificate of Divestiture is effective only if obtained prior to divestiture. Regardless of whether I receive a Certificate of Divestiture, I will ensure that all divestitures discussed in this agreement occur within the agreed upon timeframes and that all proceeds are invested in non-conflicting assets. I understand that I must timely submit my request for a Certificate of Divestiture to allow for adequate time for OGE to process the Certificate of Divestiture, and in order to divest assets within the agreed upon timeframe.

I (including my spouse and dependent children if applicable) will not repurchase any asset I was required to divest without consulting with my agency ethics official and the U.S. Office of Government Ethics.

SECTION 6 – PUBLIC POSTING

I have been advised that this ethics agreement and the Certification of Ethics Agreement Compliance will be posted publicly, consistent with the public information law at 5 U.S.C. § 552, on the website of the U.S. Office of Government Ethics with ethics agreements of other Presidential nominees who file public financial disclosure reports.

Sincerely,



Jennie Easterly

APPENDIX A – OTHER FINANCIAL INTERESTS TO BE DIVESTED WITHIN 90 DAYS

AbbVie, Inc. (ABBV)
 Allergan Plc (AGN)
 AMC Networks Inc. (AMCX)
 Autodesk, Inc. (ADSK)
 Biogen Inc. (BIIB)
 Broadcom, Inc. (AVGO)
 Cerence, Inc. (CRNC)
 Citrix Systems, Inc. (CTXS)
 Comcast Corp. (CMCSA)
 Cree, Inc. (CREE)
 Discovery, Inc. (DISCA)
 DocuSign, Inc. (DOCU)
 Dolby Laboratories, Inc. (DLB)
 Facebook, Inc. (FB)
 FireEye, Inc. (FEYE)
 Freeport-McMoRan, Inc. (FCX)
 Guardant Health, Inc. (GH)
 ImmunoGen, Inc. (IMGN)
 International Business Machines Corp. (IBM)
 Ionis Pharmaceuticals, Inc. (IONS)
 Johnson Controls International Plc (JCI)
 L3 Harris Technologies, Inc. (LHX)
 Liberty Broadband Corp. (LBRDA)
 Liberty Media Corp. (FWONK)
 Liberty Media Corp. (FWONA)
 Liberty Media Corp. Liberty SiriusXM (LSXMA)
 Liberty Media Corp. Liberty SiriusXM (LSXMK)
 Lions Gate Entertainment Corp. (LGF.B)
 LogMeIn, Inc. (LOGM)
 Medtronic Plc (MDT)
 Morgan Stanley (MS)
 National Oilwell Varco, Inc. (NOV)
 NOW, Inc. (DNOW)
 Nuance Communications Inc. (NUAN)
 Nucor Corp. (NUE)
 Occidental Petroleum Corp. (OXY)
 Pentair Plc (PNR)
 Qurate Retail, Inc. (QRTEA)
 Seagate Technology Plc (STX)
 TE Connectivity Ltd. (TEL)
 Twitter, Inc. (TWTR)
 UnitedHealth Group, Inc. (UNH)
 Vanguard Health Care Index Fund ETF Class Shares (VHT)
 Vertex Pharmaceuticals, Inc. (VRTX)
 Western Digital Corp. (WDC)

**U.S. Senate Committee on Homeland Security and Governmental Affairs
Pre-hearing Questionnaire
For the Nomination of Jen Easterly to be Director,
Cybersecurity and Infrastructure Security Agency, Department of Homeland Security**

I. Nomination Process and Conflicts of Interest

1. Did the President or anyone else give you specific reasons why the President nominated you to be the next Director of the Cybersecurity and Infrastructure Security Agency (CISA) at the Department of Homeland Security (DHS or the Department)?

I have not had the opportunity to discuss my nomination with the President.

2. Were any conditions, expressed or implied, attached to your nomination? If so, please explain.

No.

3. Have you made any commitments with respect to the policies and principles you will attempt to implement as Director? If so, what are they, and to whom were the commitments made?

No.

4. Are you aware of any business relationship, dealing, or financial transaction that could result in a possible conflict of interest for you or the appearance of a conflict of interest? If so, please explain what procedures you will use to recuse yourself or otherwise address the conflict. And if you will recuse yourself, explain how you will ensure your responsibilities are not affected by your recusal.

In connection with the nomination process, I consulted with the Office of Government Ethics and the Department of Homeland Security's Designated Agency Ethics Official to identify any potential conflicts of interest. Any potential conflicts of interest were resolved in accordance with the terms of an ethics agreement that I signed and transmitted to the Department's Designated Agency Ethics Official, and which was subsequently provided to this Committee. I am not aware of any other potential conflicts of interest.

5. Please provide the name of any individual, law firm, consulting firm, lobbying firm, public relations firm, or other entity you have formally retained, contracted, or consulted with regarding this nomination, including any amounts paid in fees or otherwise.

I did not retain, contract with, or consult with any individual, law firm, consulting firm, lobbying firm, public relations firm, or other entity regarding this nomination.

II. Background of the Nominee

6. What specific background, experience, and attributes qualify you to be Director of CISA?

Over the past thirty-one years, I have served in operational security roles in both the government and the private sector, building and leading complex organizations in peacetime and in combat to safeguard our nation and our critical infrastructure. Specifically, I established and led the Army's first cyber operations battalion, served as the Deputy Chief of Access Operations in the National Security Agency's (NSA's) highly technical Tailed Access Operations organization, and was selected to be part of a small team responsible for designing and building United States Cyber Command (CYBERCOM). In addition, I served as the Deputy for Counterterrorism at the NSA and as the Senior Director for Counterterrorism at the National Security Council (NSC), responsible for leading the development and coordination of global counterterrorism and hostage policy. Over the past nearly four and a half years, I served as a senior technology and cybersecurity leader in a global investment bank, building an organization to defend the firm from cyber threats in an increasingly complex and dynamic threat environment, a platform which I expanded over the past 18 months to ensure the firm's readiness to any business-disrupting operational incident. As the Firm's Head of Resilience and the Fusion Resilience Center, I am responsible for ensuring that the firm is prepared for and able to respond to the full range of threats, from cyber-attacks and cyber-enabled fraud to technology incidents, weather events, geopolitical unrest, terrorist attacks and infectious disease. In this capacity, I was also responsible for co-leading the firm's response to COVID-19, focused on ensuring the health and safety of our 80,000+ workforce and the resilience of our business.

Through each of these experiences, I gained a deep knowledge of how to effectively lead highly complex operational teams to deal with increasingly complex threats, to include the criticality of building a strong and vibrant culture to enable the recruitment and retention of the best talent as well as strong partnerships to enable a collaborative approach to confronting challenges.

7. How will your experience in the U.S. Army, the National Security Council, and your work in creating CYBERCOM inform your approach to leading CISA? How will the role of CISA Director differ from your prior roles in the military and intelligence communities?

My experiences in the Army, to include serving two tours in Iraq and a tour in Afghanistan, standing up the Army's first cyber operations battalion, and helping to create CYBERCOM; as well as my tours on the National Security Council, first as the Executive Assistant to National Security Advisor Condoleezza Rice and later as Special Assistant to President Obama and Senior Director for Counterterrorism, will inform my approach to leading CISA in several ways. These assignments have given me an ability to effectively build cultures of excellence to attract and manage talent; to develop operational capability and capacity in complex, evolving organizations; and to partner successfully with a myriad of stakeholders to enable mission success. They have also

given me a strong appreciation for the importance of sound policymaking as well as the criticality of solid intelligence to inform effective decision-making.

The role of CISA Director will naturally build on these experiences, to include my most recent experience in the private sector defending an element of our critical financial infrastructure. In terms of key differences, while I have worked closely with various members of the Department of Homeland Security over the years, I have not previously served in the Department; if confirmed, I will dedicate time early on to better understand the various components of the Department to ensure a productive and collaborative relationship with CISA. In addition, if confirmed, I will dedicate time to building partnerships with State, Local, Tribal, and Territorial (SLTT) government and private sector critical infrastructure through CISA's nation-wide regional presence in a more direct and focused manner than my previous roles.

8. Please describe:

a. Your leadership and management style.

I believe that while your title may make you a manager, your people make you a leader. Inspiring them, caring for them, and empowering them is the key to building a culture of excellence. I aspire to always lead with empathy, authenticity, and humility, and to create environments of high-trust, ownership, and strong accountability through transparency, inclusion, and continuous communication, built upon a solid foundation of the values instilled in me by my parents and by my time as a West Point cadet: integrity, honor, respect, selfless service, and moral courage.

b. Your experience managing personnel.

I have led Soldiers at the platoon, company, and battalion level, in peacetime and in combat. As Chief of the Cryptologic Services Group in Iraq during the surge, I led hundreds of Soldiers, Sailors, Airmen, Marines, and National Security Agency (NSA) civilians providing strategic intelligence to combat teams around the country. As a senior civilian in the government, I served as the Deputy Director of Counterterrorism at the NSA and as the Senior Director for Counterterrorism at the National Security Council. In the private sector, I've managed a highly diverse, global operational team with a presence in 8 countries around the world.

c. What is the largest number of people who have worked under your supervision?

As Head of Firm Resilience at Morgan Stanley, I am charged with overseeing efforts to ensure the security and resilience of a firm with over 80,000 employees and consultants around the globe; I currently directly manage over 160 personnel. As a Battalion Commander, I was directly charged with the care of over 300 Soldiers and separately was responsible for the direct supervision of over 200 Soldiers, Sailors, Marines, Airmen, and NSA Civilians during my first combat tour in Iraq.

9. Please give examples of times in your career when you disagreed with your superiors and advocated your position. Describe circumstances in which you were successful and in which you were unsuccessful.

As a Battalion Commander, I had a disagreement with my Brigade Commander over how to most effectively recruit and retain cyber talent, specifically, that attracting the most technical talent into the Army's first cyber operations battalion was a very different challenge than attracting and retaining talent to serve in conventional Army units where he had spent his career, and that it required innovative ways of thinking about culture, talent management, and career development. While we never completely saw eye-to-eye on the topic, I continuously advocated for my mission and my Soldiers, and was ultimately able to build a strong esprit de corps and attract excellent technical talent, to include by effectively embedding our teams into NSA's technical mission offices to ensure effective cross-training and real-world operational experience.

More recently, at Morgan Stanley, I disagreed with my manager over workforce strategy for our Cybersecurity Fusion Center, specifically the need to build a global follow-the-sun model, as opposed to trying to manage 24/7 cyber threats and vulnerabilities in a shift-working model between North America and our center in the Europe, Middle East, and Africa (EMEA) region. I worked with our team to build a strong business case for an Asia-based location and ultimately was approved to establish a separate Fusion center in Singapore. I separately advocated to my manager that we make a change in our organizational operating model that would allow us to build a more cohesive threat intelligence team, as opposed to two separate teams, one focused on strategic intelligence, the other focused on more tactical level intelligence. In this case, I was not successful, though we made the situation work, albeit less efficiently.

10. Do you seek out dissenting views and encourage constructive critical dialogue with subordinates? Please provide examples of times in your career when you have done so.

Absolutely, I strongly believe that the key to making the best decisions and solving the hardest problems comes from creating an environment of psychological safety where every person, regardless of rank or tenure, feels that they can express their views freely and respectfully. I believe that "constructive confrontation" is the key to establishing ownership and buy-in across the workforce and to preventing groupthink.

Throughout my career, I sought to encourage such constructive dialogue by actively soliciting dissenting views and encouraging red teaming of potential decisions. In particular, over the past four-plus years in the private sector, I convened numerous leadership offsites with my subordinates specifically focused around cultivating a constructive dialogue on organizational priorities, strategy, and culture. These sessions fostered intense engagement without being overly tense, and always led to better outcomes in terms of organizational direction.

11. Please list and describe examples of when you made politically difficult choices that you thought were in the best interest of the country or your organization.

During my time as the Senior Director for Counterterrorism at the NSC, I participated in several policy decisions focused on countering the threat from ISIS to the U.S. and our allies, to include the decision to take action against terrorist groups operating in Syria, and separately the decision to maintain a counterterrorism platform in Afghanistan, rather than completely draw down the U.S. presence to just the Embassy. I advocated for both of these decisions because I believed they were in the best interests of the country given the significant global threat from ISIS, notwithstanding a strong political desire to avoid getting mired in Syria and to end the war in Afghanistan. Both of these positions were ultimately supported by the President.

12. What would you consider your greatest success as a leader?

During the Iraq Surge, from 2006-2007, I deployed to Baghdad to serve as the Chief of the Cryptologic Services Group, responsible for providing national-level signals intelligence to the warfighter. Part of my responsibilities was to deploy and operationalize a new, high-technology system, known as Real-Time Regional Gateway (RTRG), to enable the National Security Agency to provide relevant, actionable intelligence, not in weeks or days, but rather in hours and minutes. Effectively implementing the system and providing capability to every Brigade Combat Team in theater was an enormous operational and logistical challenge, and one that experienced several failures along the way. Ultimately, we fully deployed the system and provided a capability to detect and disrupt terrorist bomb-making networks much more effectively. The system enabled warfighters to take thousands of insurgents off the battlefield and save the lives of countless troops and Iraqi civilians.

13. What do you consider your greatest failure as a leader? What lessons did you take away from that experience?

As the Senior Director for Counterterrorism at the NSC, among my responsibilities was the U.S. hostage portfolio. In this role, I focused on ensuring the U.S. government had the policies and capabilities in place to safely recover Americans held hostage by terrorist groups. During my tenure, a failed rescue attempt ultimately led to the brutal murders by ISIS of several young Americans, including Jim Foley, Steven Sotloff, Peter Kassig and Kayla Mueller. The families of these Americans were outraged that the government had not done enough to bring their children home safely; their anguish ultimately led the President to direct a complete review of our hostage policy, an effort which my team was charged with leading.

Over a nine-month period, my team and I led an intense review process, working with partners across the federal government, with international allies, and perhaps most importantly, with former hostages and families of hostages, to include those who had lost their loved ones at the hands of ISIS. We focused on building new organizational structures that would more effectively ensure the safe recovery of Americans held hostage, to include the Hostage Recovery Fusion Cell, the Hostage Response Group, and the Special Presidential Envoy for Hostage Affairs. And importantly, we focused on

building a new policy that would put an emphasis on working transparently and collaboratively with hostage families, acknowledging that no one has a greater stake in the safe recovery of a hostage than their family. It was an incredibly intense, challenging, and emotionally draining experience, but perhaps my most rewarding in that we were able to create something that ultimately made a real difference, supporting the safe recovery of dozens of Americans held hostage over the past six years. For leading that effort, I was subsequently recognized with the American Hostage Freedom Award by the James W. Foley Legacy Foundation, one of my most cherished honors.

Key lessons from this experience reinforced for me the importance of having the right policies, organizational structures, and capabilities to deal with our most complex threats; and the criticality of collaboration, transparency, and information-sharing to solve our toughest problems. The experience also highlighted for me the very real human impact that national policies can have and the sacred responsibility to ensure we are always doing the right thing to protect American citizens at home and around the world.

14. During your career, has your conduct as a government employee ever been subject to an investigation or audit by an agency Inspector General, Office of Special Counsel, Department of Justice, agency Equal Employment Opportunity office or investigator, or any other federal investigative entity? If so, please describe the nature of the allegations/conduct and the outcome of the investigation(s) or audit(s).

No.

III. Role of the Director, CISA

15. Please describe the role and mission of CISA and what you believe it should be. What steps will you take to get CISA from its current state to the optimal future state?

CISA's core mission areas are to protect and defend federal networks to ensure their security and resilience; to identify and manage physical and cyber risk to critical infrastructure, working closely with stakeholders across all levels of government and with the private sector; and to ensure public safety, national security and emergency preparedness communities can seamlessly and securely communicate.

If confirmed, I will focus on enhancing CISA's capabilities to support these critical missions through investments in the right technologies and strengthening the public-private partnerships that are necessary to defend our nation from myriad threats. Perhaps, most importantly, I will work to build and strengthen CISA's workforce by recruiting and retaining top talent.

16. In your opinion, is CISA currently fulfilling its cybersecurity responsibilities? If not, what would you do differently as Director, if confirmed?

As a relatively new agency, CISA has done a commendable job of building its capability and capacity to fulfill its cybersecurity responsibilities. While I have not witnessed this

evolution from inside the federal government, I have seen it as a private citizen serving as a senior operational leader in one of the nation's systemically important banks, benefiting from CISA's technical guidance and support throughout the pandemic and across multiple cyber threat streams. If confirmed, I would build on the good work done by Director Krebs and Acting Director Wales and the men and women of CISA to continue to advance CISA's mission, building its workforce, its capabilities, and its partnerships to fulfill its cybersecurity responsibilities.

17. In your opinion, is CISA currently fulfilling its responsibilities for critical infrastructure security? If not, what would you do differently as Director, if confirmed?

As noted above, as a private citizen serving as a senior operational leader in one of the nation's critical infrastructure owners, my team has benefited from CISA's technical guidance and support throughout the pandemic and across multiple threat streams. If confirmed, I would build on the good work done by Director Krebs and Acting Director Wales and the men and women of CISA to continue to advance CISA's mission, building its workforce, its capabilities, and its partnerships to fulfill its critical infrastructure security responsibilities.

In addition, if confirmed, I will focus on implementing the new Sector Risk Management Agency provision included in the recent National Defense Authorization Act. This provision requires a review of the current framework for securing critical infrastructure. I will ensure that CISA works with its federal partners to carry out a thorough review and submit recommendations to the President for making improvements, as appropriate.

18. Today, more than 20 agencies across the federal government have roles and responsibilities associated with U.S. cyber capabilities. What is your understanding of CISA's role within that ecosystem? What role do you believe CISA should ideally play?

Congress authorized CISA as the country's national cyber defense center, the operational entity responsible and accountable for the protection and defense of civilian government networks, and for managing risk to State, Local, tribal, and territorial (SLTT) government networks and to our nation's critical infrastructure in close partnership with the private sector. Within the federal cyber ecosystem, CISA is the "quarterback" on the federal cybersecurity team, charged with operationalizing defensive cybersecurity strategy and policy; serving as the lead for asset response during cyber incidents; and ensuring that relevant threat information is shared effectively across the Federal government, with SLTT partners, and with industry. As a trusted partner to the private sector, CISA is best positioned to be the front door for the U.S. Government's engagement with industry on cybersecurity.

In my view, cyber is a team sport, one that requires leaders to cultivate operational collaboration and productive relationships up, down, and across all levels of our cyber ecosystem. CISA fulfills its lead role for national cyber resilience in collaboration with other agencies at every level of government and all sectors.

19. Do you believe CISA should be more actively involved in securing individual agencies' networks?

Yes, and I think that the recent authorities and resources provided to CISA by the Congress, as well as the responsibilities given to CISA in the recent Executive Order on "Improving the Nation's Cybersecurity" represent a recognition of the need for CISA to play a more active role in securing civilian agencies' networks. Given the complexity of the technology environment across 102 federal civilian agencies, the uneven allocation of resources dedicated to securing these networks, and the increasingly dangerous and dynamic threat environment, I believe that giving CISA greater authority and responsibility to manage federal government networks will ultimately improve their security.

20. Please describe your understanding of the role and responsibilities of the CISA Director with respect to private sector entities. If confirmed, what steps would you take to establish and maintain relationships with the private sector?

While private sector entities are responsible for maintaining, operating, and securing their own networks, systems, and infrastructure, CISA serves as a valuable partner to the private sector, providing threat information, assessments, technical guidance, and educational resources to inform and assist private sector entities in managing risk. As a trusted partner to the private sector, CISA is best positioned to be the front door for the U.S. government's engagement with industry on cybersecurity. I've witnessed this first-hand as a senior operational leader in the private sector and benefited from it. If confirmed, I would leverage my recent private sector experience to build on the positive relationships CISA has established with the private sector, cultivating and strengthening these partnerships through such entities as the Critical Infrastructure Partnership Advisory Council and the various sector coordinating councils and information sharing and analysis centers.

21. Under the National Defense Authorization Act of 2021, Congress established a National Cyber Director and an accompanying office in the White House.

- a. What do you believe the respective roles of CISA, and the new Office of the National Cyber Director should be?

As I understand it, the Office of the National Cyber Director is responsible for overseeing and coordinating Federal government activities to implement national cyber policy and strategy. As the President's principal advisor on cybersecurity policy and strategy, the National Cyber Director is the "coach" of the federal cybersecurity team, charged with building coherence across the federal cyber ecosystem, and ensuring that all relevant departments and agencies, to include CISA, have the authorities and resources needed to effectively execute mission.

CISA is the country's national cyber defense center. To continue the analogy, CISA is the "quarterback" on the federal cybersecurity team, charged with

operationalizing cybersecurity strategy and policy as it relates to securing networks at all levels of government and our nation's critical infrastructure in close partnership with the private sector.

- b. If confirmed, how do you plan to coordinate with the new National Cyber Director?

I have known Chris Inglis, the nominee for National Cyber Director, for over a decade and worked closely with him during my time at the National Security Agency. I have tremendous respect for his intellect, integrity, and leadership ability. Since we were nominated for our respective roles, we have been in close contact to discuss the challenges and opportunities ahead of us, and how we will work together if confirmed. If we are both confirmed, I expect our relationship to be transparent and collaborative, involving regular coordination.

22. Please describe your understanding of CISA's cybersecurity role and responsibilities as compared to the responsibilities of each of the following positions (separately):

- a. National Cyber Director:

The NCD is responsible for overseeing the implementation of national cybersecurity policy and strategy and for coordinating Federal government activities to build preparedness and resilience across Federal, State, local and tribal entities, as well as with the private sector. CISA is responsible for the overall operationalization of defensive cybersecurity policy and strategy and serves as the front door for the U.S. government's operational engagement with industry on cybersecurity.

- b. The Deputy National Security Advisor for Cyber and Emerging Technology; and

The DNSA for Cyber and Emerging Tech is responsible for leading the interagency coordination and development of cybersecurity policies, strategies, and priorities, aligning them across the breadth of U.S. national security. CISA is a key contributor to the interagency process, and separately leads asset response in the event that a Cyber Unified Coordination Group is formed under the auspices of Presidential Policy Directive 41.

- c. The Federal Chief Information Security Officer.

The Federal CISO is responsible for designing and overseeing the implementation of cybersecurity policies and practices, including effective cybersecurity performance measures for the federal government to align with the Federal Information Security Management Act (FISMA). The Federal CISO is a close partner of CISA in its operational role to protect and defend federal government networks.

IV. Policy Questions

CISA Mission & Priorities

23. What do you believe are the most pressing internal and external challenges currently facing CISA? Which challenges will you prioritize and what do you plan to do to address those challenges?

Internally, I believe the biggest challenges involve ensuring the CISA workforce is fully staffed with the right talent to enable it to effectively execute its mission. If confirmed, I will make this a top priority, ensuring that we have the talent management processes in place to effectively recruit, hire, onboard, train, recognize, and retain top talent.

Externally, the biggest challenges facing CISA come from an increasingly complex and dynamic threat environment, from nation-states and cyber-criminals to domestic violent extremists and terrorists who pose a danger to the security and resilience of our government and our critical infrastructure. In just the last six months, we've witnessed a series of significant cyber campaigns by both nation-states and criminal actors to exploit vulnerabilities and compromise both federal networks and critical infrastructure. If confirmed, I will focus on building the capability and capacity of CISA to deal with these myriad threats, prioritizing the implementation of additional authorities and resources recently provided by the Congress in the National Defense Authorization Act of 2021 and the American Rescue Plan Act to build CISA's ability to respond to cyber threats and incidents. In addition, I will prioritize the implementation of critical tasks recently given to CISA by the President in his Executive Order on Improving the Nation's Cybersecurity.

24. In your view, what are the highest priorities for enhancing cybersecurity and critical infrastructure security? Why?

The three highest priorities in terms of both urgency and importance for enhancing cybersecurity and critical infrastructure security are: 1) ensuring CISA has the resources it needs, in terms of people, budget, and authorities; 2) ensuring CISA has the operational and technical visibility it needs to support the protection and defense of federal government networks; and 3) ensuring CISA has the strong partnerships it needs at Federal, State, Local and Tribal level, and with private industry, to enable robust operational collaboration to ensure the security and resilience of critical infrastructure. These three elements, resources, in particular talent; operational visibility; and partnerships are critical for strengthening CISA's capability and capacity to effectively execute its mission.

25. What parts, if any, of CISA's mission do you believe need more emphasis?

The massive SolarWinds breach of U.S. Government and private sector networks discovered late last year, along with more recent successful compromises of federal and private sector systems, illuminates the urgency of efforts to more effectively secure federal networks and for the private sector to improve its security and resilience. These efforts are core to CISA's mission and require continued emphasis.

26. Based on your prior federal service, what is CISA's reputation and relationship with each of the following, and what would you do to improve its reputation and relationship with them? (Please respond to each individually.)

a. The Defense Department and the Intelligence Community

As I understand it, CISA has an increasingly positive reputation with the Defense Department and the Intelligence Community, in particular based on productive relationships forged during the 2020 elections with the Federal Bureau of Investigation, the National Security Agency, and CYBERCOM. If confirmed, I would leverage my longstanding relationships with the Intelligence Community and the Department of Defense to continue to strengthen these partnerships.

b. Other departments and agencies

As I understand it, CISA has built productive relationships across the interagency, though more work needs to be done here to build trust and confidence in CISA's capabilities to support the protection and defense of agency networks. The new authorities and resources recently provided by the Congress to CISA will help, to include by enabling CISA to proactively hunt for intruders on civilian federal government networks as well as to provide shared services based on security-by-design for these agencies.

c. State and local governments

While I've had limited interaction at the State and local level, throughout the past several months, the feedback I've received from State and local government on CISA has been very positive, in particular CISA's efforts to assist these entities in ensuring the security and safety of their elections. Looking ahead, expanding CISA's footprint across the country will be critical to institutionalize and maximize its network of partnerships. As I understand it, CISA is already moving ahead with placing State Cybersecurity Coordinators across the country, deepening its longstanding relationships from coast to coast. Separately, I believe that the proposed Cyber Response and Recovery Fund would further strengthen these partnerships, augmenting CISA's ability to provide assistance to state, local, tribal, and territorial governments.

d. Private companies

Based on my experience in the private sector over the past four-plus years, CISA has a very positive reputation, and is seen as a trusted advisor and partner in assisting private sector entities in managing risks to their systems, networks, and infrastructure. If confirmed, I would work to strengthen these partnerships, continuing to build CISA's reputation as a trusted interlocutor and as the front door for industry engagement.

27. Based on your prior federal service, do you have an opinion on CISA's current resources and whether they are in line with its statutory responsibilities? Please explain.

At this point, I do not have a fully informed opinion on whether CISA is properly resourced to execute its statutory responsibilities, though my sense is that CISA may need additional resources. I understand that as directed in the National Defense Authorization Act, the Secretary of Homeland Security is conducting a comprehensive review of CISA's ability to execute its mission, to include whether additional budget or personnel are required. If confirmed, I will work closely with the Secretary on this review to ensure that CISA has the resources it needs to succeed.

28. If confirmed, how would you work with other agencies with responsibilities for cybersecurity and infrastructure security to implement these priorities? How would you work with private sector entities to implement these priorities?

If confirmed, I would work closely and collaboratively with other agencies who have responsibilities for cybersecurity and infrastructure security. With its strong and deep network of partnerships, CISA is the ideal nexus for the government to mobilize action and advance cyber resilience across all sectors and at every level of government. CISA's role in leading national efforts to secure the 2020 election illustrates what can be accomplished through strong partnerships, a clear vision, and an appropriate sense of urgency.

With respect to private sector entities, if confirmed, I would leverage my recent private sector experience to build on the positive relationships CISA has established with the private sector, cultivating and strengthening these partnerships through such entities as the Critical Infrastructure Partnership Advisory Council, the various sector coordinating councils, and the information sharing and analysis centers.

Management & Workforce

29. Do you believe there currently is adequate accountability for federal cybersecurity? If not, how would you seek to increase accountability, if confirmed?

As a private citizen, I don't have a full sense of whether there is currently adequate accountability for federal cybersecurity though the recent serious compromises of federal networks suggest that more work needs to be done to clarify roles and responsibilities in this space. In this context, I believe that CISA should be held accountable for the protection and defense of federal government networks and provided the resources and authorities to execute this mission, ultimately serving as the operational CISO for federal networks. In executing this mission, CISA would work closely with the Federal CISO, who is responsible for designing and overseeing the implementation of cybersecurity policies and practices, including effective cybersecurity performance measures to align with the Federal Information Security Management Act (FISMA). CISA would also work closely with the National Cyber Director who is accountable to the President for overseeing the implementation of national cybersecurity policy and strategy and for coordinating Federal government activities to build preparedness and resilience across Federal, State, local and tribal entities, as well as with the private sector.

30. How would you assess the current organizational structure around cybersecurity governance within the federal government? What, if anything, do you think should change?

As a private citizen, I'm unable to make a well-informed assessment of the current organizational structure around cybersecurity governance within the federal government. Though, from a private sector perspective, I have observed that the government sometimes presents an uncoordinated and fragmented approach to the private sector. To this end, I think the role of the National Cyber Director can help bring coherence and cohesion to the various entities within the federal government charged with cybersecurity responsibilities, with CISA serving as the front door to the private sector and SLTT governments. If confirmed, I look forward to working closely with the National Cyber Director.

31. What measurements would you use to determine whether your office is successful?

I strongly believe that we must measure what matters. If confirmed, I will develop key measures of performance and effectiveness across each operational division, aligned to the overall strategy. In addition to such measurements across each operational division, I would also develop metrics focused on the workforce, to include recruitment and retention of talent, ensuring that CISA is fully staffed with diverse talent and that attrition of high-performers is consistently low; as well as metrics focused on the material improvement of federal cybersecurity, to include increased visibility across federal networks of potential threats and vulnerabilities, reduction in response time for implementation of binding operational directives and emergency directives issued by CISA, and reduction in the compromise of federal government and critical infrastructure networks.

32. What do you consider to be the principal management challenges facing CISA? How will you address these challenges if confirmed?

As a private citizen, I don't have extensive insight into the principal management challenges facing CISA. However, my initial observation is that CISA, as a young cybersecurity agency, must focus on streamlining hiring processes necessary to recruit and retain top talent and maturing business processes. If confirmed, I will make an early assessment of such challenges and devise a plan to address them expeditiously.

33. How will you address the challenge of recruiting, hiring, training, and retaining personnel with cybersecurity and other critical expertise?

- a. Do you believe that CISA has sufficient cybersecurity personnel?

At this point, I do not have a fully informed opinion on whether CISA has sufficient cybersecurity personnel, though my sense is that CISA may need additional personnel to effectively execute its mission, to include fully operationalizing the additional authorities and responsibilities implicated in the NDAA and the

President's recent Executive Order. I understand that as directed in the National Defense Authorization Act, the Secretary of Homeland Security is conducting a comprehensive review of CISA's ability to execute its mission, to include whether additional personnel are required. If confirmed, I will work closely with the Secretary on this review to ensure that CISA has the resources it needs to succeed.

- b. Do you think CISA's current hiring authorities are sufficient? If confirmed, are there additional authorities you would pursue?

If confirmed, I would make it an early priority to fully understand how CISA leverages current hiring authorities and determine whether additional authorities are required. I look forward to learning more about how CISA can utilize the Department's Cyber Talent Management System, which was designed to afford greater flexibility to the process of hiring and managing cyber talent and which will likely go into effect later this year. As I understand it, the biggest challenge currently facing CISA involves the length of time required to hire individuals, which has led to the loss of qualified personnel. It is imperative that we reduce this hiring time significantly to recruit and retain the talent CISA needs to succeed.

- c. The federal government has few entry level cybersecurity positions. What if anything would you do to address that?

I believe it is essential to create a pipeline of diverse talent from the entry-level, exploring creative opportunities, including internship programs and apprenticeship programs. If confirmed, I would make it an early priority to fully understand the CISA workforce, to include how CISA manages career development.

Cybersecurity

34. How would you assess the federal government's cybersecurity posture?

As evidenced by years of compromises of federal networks and the recent SolarWinds breach, I assess the federal government's cybersecurity posture to be inadequate. One of the most illuminating reference points here comes from a 2019 bipartisan report from the Permanent Subcommittee on Investigations of the Homeland Security and Government Affairs Committee which documented the failure of eight federal agencies, to include the Department of Homeland Security, to address vulnerabilities in their information technology infrastructure. Separately, in 2018, OMB and DHS determined that 71 of 96 agencies participating in the risk assessment process have cybersecurity programs that are either at risk or high risk. Clearly, much work needs to be done here; the urgency and importance of this mission is one of the key driving factors motivating my desire for this position.

35. What do you view to be the most significant current and potential cybersecurity threats facing our nation?

If 2020 taught us anything, it is to expect the unexpected and anticipate the unimaginable. Even as we contend with the millions of daily intrusions against our networks by a range of malicious cyber threat actors, to include those actively exploiting the COVID-19 pandemic in an explosion of fraud, I believe that as a nation, we remain at great risk of a catastrophic cyber-attack.

While the digital revolution of the past two decades helped enable unprecedented economic growth and innovation, increased connectivity also introduced great peril: significant and growing vulnerabilities threaten our privacy and data security, our infrastructure, and our national and economic security.

Over the past decade, at least three major trends shaped an increasingly complex and dangerous threat landscape: (1) the number of Nation-States with offensive cyber-attack capabilities rose to over 30 countries and is likely to increase further in the near term; (2) commoditization of the criminal marketplace for cyber tools and services, fueling the widespread proliferation of cybercrime; and (3) the increasingly blended nature of cyber threats, with nation states behaving like cyber criminals, and cyber criminals empowered with sophisticated nation-state cyber tools.

Combined, these factors create an environment in which nation-states and non-state actors alike continue to leverage cyberspace to threaten our security and our way of life, online and off: combining hacking with malign influence operations to interfere in democratic processes; breaching major corporations to steal data, including intellectual property, to enable espionage; targeting industrial control systems across electric utilities, manufacturing plants, and oil refineries to disrupt critical infrastructure operations; brazenly stealing huge amounts of capital from banks around the globe; and incapacitating entities large and small with the scourge of ransomware.

36. The United States continues to face significant cyberattacks including the SolarWinds, Microsoft Exchange, Pulse Connect, and Colonial Pipeline compromises. Many of these attacks are attributable to nation-state adversaries.
 - a. If confirmed as the Director of CISA, how will you ensure victims, federal and non-federal, receive necessary technical assistance given the increased demand for CISA's services?

If confirmed, I will work to ensure that CISA has the resources and capability to provide technical assistance and support to entities before they experience an incident and to victims of cyber-attacks which request its services. Given the increased demand for these services, CISA must be able to recruit and rapidly hire top talent and implement the additional resources provided to CISA as part of the American Rescue Plan Act. CISA must also continue to develop strong partnerships across the federal government and with the private sector to ensure that information about significant cyber incidents is shared expeditiously to warn and prevent the exploitation of future potential victims. CISA provides an excellent platform for sharing information about threats and mitigation measures to entities across the

government and industry, something I experienced and sought to take full advantage of in my current private sector firm.

- b. Do you believe CISA offers adequate services to victims? What, if anything, would you change about CISA's offerings?

As a private citizen, I don't have a full sense of whether CISA is able to offer adequate services. If confirmed, I would make it an early priority to understand these offerings fully to determine whether any changes are required.

- c. What do you believe is CISA's responsibility to ensure less-resourced victims (e.g., K-12, small businesses, and institutions of higher education) are prepared to respond to the next cyberattack?

If confirmed, I will work to ensure that less-resourced victims are better prepared to respond to cyberattacks primarily by ensuring that these entities have the resources they need to understand the threat environment and take basic steps to protect themselves. As over 90% of successful cyber-attacks start with a phishing email, educating stakeholders about the basics of cyber hygiene is critical to empowering them to secure their networks. If confirmed, I will leverage the CISA platform to serve as the nation's chief cyber evangelist for the importance of cyber hygiene and a culture that emphasizes security.

- d. What should be CISA's role in supporting compromised defense or other national security networks, if any?

CISA is not the lead agency for securing national security networks, but if confirmed, I will ensure we are ready to engage our interagency partners, provide any assistance as needed, and share threat indicators and other information to protect all networks. I will ensure we are working in close partnership with the Department of Defense, which oversees defense networks, and the National Security Agency, the national manager for national security systems, to ensure our guidance and direction is mutually reinforcing and maximizes consistency, whenever possible.

37. If confirmed, what steps do you intend to take to improve the nation's cybersecurity, both with respect to the government and private networks?

As noted above, if confirmed, my highest priorities for improving the nation's cybersecurity include: 1) ensuring CISA has the resources it needs, in terms of people, budget, and authorities to execute its mission; 2) ensuring CISA has the operational and technical visibility it needs to support the protection and defense of federal government networks and 3) ensuring CISA has the strong partnerships it needs at Federal, State, Local and Tribal level, and with private industry, to enable robust operational collaboration.

38. What do you believe is the appropriate role for CISA to play in securing private networks?

While private sector entities are responsible for maintaining, operating, and securing their own networks, systems, and infrastructure, CISA serves as a valuable partner to the private sector, providing threat information, assessments, technical guidance, and educational resources to inform and assist private sector entities in managing risk. As a trusted partner to the private sector, CISA is best positioned to be the front door for the U.S. government's engagement with industry on cybersecurity. I've witnessed this firsthand as a senior operational leader in the private sector and benefited from it. As noted above, if confirmed, I would leverage my recent private sector experience to build on the positive relationships CISA has established with the private sector, cultivating and strengthening these partnerships, to include through the various sector coordinating councils and information sharing and analysis centers.

39. Please describe your views on the appropriate role of private sector entities in working with CISA to improve our nation's cybersecurity.

As I have witnessed over the past four-plus years, the private sector, which owns and operates most of the nation's critical infrastructure, plays a vital role in working with CISA to improve the nation's cybersecurity, sharing information about threats to enable a collective defense. In addition, rapid reporting of cyber incidents by private sector entities can help identify significant incidents and mitigate the impact of certain threat campaigns on future victims.

Separately, private sector entities, in particular software companies, cloud service providers, and cybersecurity vendors that have extensive visibility given their access into networks around the globe, have very valuable insights into threats and vulnerabilities that would help inform CISA's ability to anticipate and mitigate the impact of threats on federal government networks as well as on critical infrastructure.

If confirmed, I will build on existing efforts to improve operational collaboration so that the unique insights of these private sector companies can directly inform CISA's defensive cyber operations.

40. CISA is responsible for a number of cybersecurity information sharing initiatives.

- a. How do you define success for cybersecurity information sharing across the public and private sectors?

If confirmed, I intend to assess the volume and quality of information shared by the private sector with the federal government, and the feedback received by the private sector about the volume and quality of information shared by the public sector. In both cases, quality will be defined by how timely, actionable, and contextualized the information is and whether it is leveraged to effectively mitigate threats and vulnerabilities.

- b. What do you believe is CISA's responsibility to share cybersecurity information with the private sector?

As I've witnessed during my time in the private sector, CISA plays an incredibly important and valuable role in sharing cybersecurity information with the private sector, to include threat information and technical guidance to inform the private sector's ability to prevent, detect, and respond to cyber threats and vulnerabilities.

- c. Please describe your plans, if confirmed, for how CISA will improve cybersecurity threat information sharing, including ensuring that the information is timely and actionable for recipients to integrate into their cybersecurity defensive capabilities.

If confirmed, I would focus on deeper operational collaboration between the public and private sector, placing a greater emphasis on providing the private sector with context and prioritization.

41. What do you see as CISA's role in negotiating and maintaining partnerships with other countries on cybersecurity? What opportunities do you see for increased cooperation to combat international cybersecurity threats?

Cyber incidents do not start and stop at our physical borders; as such, international cooperation is imperative. CISA is uniquely positioned to share information, coordinate, and collaborate with our international partners. If confirmed, I would look forward to building vibrant operational partnerships with our allies, working closely with the State Department and the National Cyber Director.

42. DHS's statutory authority to operate the EINSTEIN intrusion detection and prevention system expires at the end of 2022.

- a. Do you believe this program is effective?

Based on recent significant compromises of federal government networks, I think work needs to be done to improve the program, to include shifting the fundamental focus from perimeter defense to a defense-in-depth network architecture built on zero-trust principles.

- b. Do you believe the added value of the ability to use classified indicators justifies the additional expense compared with using commercial/subsorption indicators?

As a private citizen, I am unable to fully comment on the added value of the use of classified indicators; that said, based on my experience in the private sector, I believe that there is great value in what is offered through commercial services. If confirmed, I would take a close look at whether the additional expense of using classified indicators is prudent given what is now commercially available on the market.

- c. What are your plans for improving this program?

At this time, I do not have specific plans for improving the EINSTEIN program. It is critical to ensure that intrusion detection and prevention capabilities like EINSTEIN modernize to secure evolving technology platforms and the ways we access and store data. If confirmed, I will make it a top priority to understand how to improve EINSTEIN, to include what authorities are necessary beyond 2022.

- d. Are there legislative changes that need to be made to improve your ability to modernize this program and improve its effectiveness?

As a private citizen, I do not have enough insight into the program to understand what legislative changes CISA may need to enhance its ability to modernize and improve the EINSTEIN program. If confirmed, I will make it a top priority to understand how to improve the program and come back to you with my views.

43. Do you believe the federal government is too reliant on perimeter-based security? If so, how would you seek to improve end point security if confirmed?

Yes, I agree that the federal government is too reliant on perimeter-based security; it is critical that the federal government move to a defense-in-depth network architecture based on zero-trust principles of least privileged access and micro-segmentation, as well as the instantiation of end point detection and response (EDR) capabilities. The President's recent Executive Order on "Improving the Nation's Cybersecurity" directed federal agencies to deploy EDR technology to support proactive detection of cybersecurity incidents, active cyber hunting, containment and remediation, and incident response. If confirmed, I would work closely with federal agencies on the implementation of this important initiative to enable CISA to have the host-level visibility it needs to effectively protect and defend federal government networks.

44. CISA also runs the Continuous Diagnostics and Mitigation program.

- a. Do you believe this program is effective?

As a private citizen, I don't have a fully informed view of the program, though recent compromises of federal networks indicate that more can be done to improve the program's effectiveness.

- b. What changes would you make to improve the program, if confirmed?

As part of the President's recent Executive Order, agencies were directed to establish or update Memoranda of Agreement with CISA for the Continuous Diagnostics and Mitigation Program to ensure object level data are available and accessible to CISA, consistent with applicable law. Access to such fine-grained data will help improve the program, and in particularly CISA's visibility into federal networks and its concomitant

ability to protect and defend these networks by rapidly detecting and responding to threats and vulnerabilities.

45. Over multiple administrations, federal agencies have failed to comply with cybersecurity requirements under the Federal Information Security Modernization Act ("FISMA"). If confirmed, what will you do to address these long-standing vulnerabilities?

Under the current FISMA construct, departments and agencies are responsible for protecting their networks and complying with FISMA. CISA is responsible for administering the implementation of cybersecurity policy and practices at agencies through issuing compulsory directives, providing guidance, and providing tools and services that make it easier and less expensive for agencies to increase the security and resilience of their networks. If confirmed, I look forward to better understanding the state of current vulnerabilities across federal networks and appropriately using the full range of CISA's authorities to further secure our government networks.

46. Do you believe that FISMA reporting is an effective tool to evaluate the federal government's cybersecurity? What, if any, legislative changes need to be made to improve it?

I do believe that FISMA reporting is a useful tool to help evaluate federal government cybersecurity. At this time, I don't have a sense of whether legislative changes need to be made to FISMA reporting requirements to improve the ability to understand the state of federal government cybersecurity. If confirmed, I will commit to studying this issue and coming back with any recommendations.

47. Last year, DHS's own cybersecurity program was rated ineffective under FISMA. As the agency charged with administering FISMA requirements government-wide, DHS should be a model for other executive agencies. How will you address those weaknesses in the Department's program?

I strongly agree that as the agency responsible for administering FISMA requirements across the federal government, DHS must lead by example. If confirmed, I look forward to working closely with the Secretary and the Department's Chief Information Officer (CIO), ensuring that the Department has the tools and services it needs to increase the cybersecurity and resilience of its networks.

48. Supply chain security is an important part of every federal acquisition at every agency. In your view, what role should CISA play in working to improve supply chain security across the federal government?

Improving supply chain security is a whole-of-Government effort, and I understand there are a number of ongoing initiatives in this space, to include requirements recently promulgated in the President's Executive Order on improving the nation's cybersecurity. CISA should contribute its expertise in cybersecurity and critical infrastructure supply chain analysis to these efforts, to include collaborating on policy options to help improve

supply chain security not only for the federal government but more broadly for the Nation as a whole.

Additionally, I understand that this Committee played a key role in authorizing the Federal Acquisition Security Council (FASC) several years ago. My understanding is CISA is a member of the FASC, supports information sharing among federal agencies, and plays a lead role in carrying out the Secretary's authority to issue a removal or exclusion order, if necessary, to civilian federal agencies for specific information and communications technology.

49. CISA has responsibility for supporting State and Local Governments as well as private sector cybersecurity – including supply chain security. How do you believe CISA is best able to support non-federal entities with supply chain risk management?

CISA provides a valuable forum for public-private engagement on supply chain risk management, such as through the Information Communications Technology Supply Chain Risk Management Task Force, and by providing best practices and guidance, as well as shared analytics.

50. CISA has been given a number of new responsibilities in the recent Cyber Executive Order to improve federal cybersecurity.

- a. Do you believe that CISA has the resources, capacity, and authorities to execute these new responsibilities?

As a private citizen, I do not have a full sense of whether CISA has the resources, capacity, and authorities to fully execute the new responsibilities provided to it in the recent Cyber Executive Order, though I believe that additional resources may be required. If confirmed, I will aim to rapidly determine whether such resources are necessary and share any recommendations with the Committee.

- b. If confirmed, how would you prioritize these efforts (please provide a ranked order list of how you would prioritize CISA's various cyber responsibilities). Are there additional actions you feel CISA can take to improve the security of federal networks?

I believe the recent Cyber Executive Order provides an excellent roadmap for materially improving the security of federal networks. If confirmed, I would prioritize CISA's work focused on the following key elements: 1) ensuring CISA's own programs, services, and capabilities are fully functional with cloud-computing environments and principles of zero-trust architecture; 2) working with stakeholders to increase visibility across federal government networks to enable proactive detection and mitigation of cyber threats and vulnerabilities through the deployment of endpoint detection and response capabilities; 3) working with stakeholders to develop a standard set of operational procedures and playbooks to be used in planning and conducting cybersecurity vulnerability and incident response activity; 4) establishing a framework to collaborate on incident response and activities related to federal government cloud technology; and 5) working with key

partners to develop security principles governing Cloud Service Providers for incorporation into agency modernization efforts.

In terms of additional actions, if confirmed, I would make an assessment of what else CISA may need to do to improve the security of federal networks and provide any recommendations.

Incident Prevention, Detection, Response, and Recovery

51. What is your assessment of CISA's current capabilities to prevent incidents? If confirmed, how will you work to improve them?

As judged from recent compromises of federal government networks, I assess that CISA's capability to prevent cyber incidents needs improvement. If confirmed, I will work closely with departments and agencies, implementing the additional authorities, responsibilities, and resources recently provided to CISA to improve its ability to prevent incidents.

52. What is your assessment of CISA's current capabilities to detect incidents? If confirmed, how will you work to improve them?

As judged from recent compromises of federal government networks, I assess that CISA's capability to detect cyber incidents needs improvement. If confirmed, I will work closely with departments and agencies, implementing the additional authorities, responsibilities, and resources recently provided to CISA to improve its ability to detect incidents.

53. What is your assessment of CISA's current capabilities to respond to cyberattacks? If confirmed, how will you work to improve these capabilities?

My understanding is that CISA's current capabilities to respond to cyberattacks are increasingly effective, though the additional resources provided in the American Rescue Plan Act and additional authorities provided in the National Defense Authorization Act should materially improve CISA's incident response capabilities. If confirmed, I look forward to overseeing the effective implementation of these capabilities.

54. What do you view as CISA's role in supporting non-federal entities (e.g., private sector, state/local government agencies) that are responding to or recovering from a cyberattack?

CISA plays an important role in supporting non-federal entities responding to or recovering from a cyberattack with technical assistance and incident response capabilities, if requested. Even if CISA does not provide such voluntary assistance, it is important that CISA be provided awareness of significant cyber incidents to enable it to warn other potential victims of threats and vulnerabilities to enable them to protect themselves.

Critical Infrastructure & Election Security

55. One of DHS's most challenging missions is protecting physical and cyber critical infrastructure across 16 individual and unique sectors. In most of these sectors, DHS has little or no operational or regulatory authority and must rely on partnerships with other federal agencies, state and local governments, and private infrastructure owners and operators.

- a. How, if at all, would you recommend CISA change its approach to critical infrastructure protection?

At this time, I do not have specific recommendations on whether or how CISA should change the approach to critical infrastructure protection. If confirmed, I would make an early assessment of CISA's role and come back with any recommendations. From the perspective of a private citizen, I do think it is important for critical infrastructure owners and operators to make CISA aware of cyber incidents that may cause serious harm to national or economic security, so that CISA can provide technical assistance if requested; warn other potential victims as appropriate; and work with relevant stakeholders to analyze and assess the implications of cascading threats.

- b. What steps do you think are necessary to strengthen communication and two-way information sharing with private sector owners and operators, while also safeguarding sensitive information?

As I understand it, CISA has done a commendable job of building communication and strengthening information sharing with the private sector over the past several years. That said, I believe there is room for further improvement, including moving from public private partnerships to public private operational collaboration by: 1) ensuring that CISA provides timely, actionable, and contextualized information to its stakeholders; 2) ensuring that CISA provides regular feedback to stakeholders who share information with it on the quality and value of that information; and 3) ensuring that CISA maintains the trust of its private sector stakeholders by safeguarding sensitive data, carefully balancing the need to warn potential victims about emerging threats while protecting privileged information. I understand Congress has provided CISA with authorities to safeguard sensitive information, such as Protected Critical Infrastructure Information. If confirmed, I look forward to ensuring that these authorities are being implemented in the most effective way and seeking new authorities from Congress if needed.

- c. Which sectors do you think are most critical to protect and how should CISA prioritize among them?

By definition, sectors designated as critical are each so vital to the United States that their incapacity and destruction would have a debilitating impact on our national security, our economic security, or our public health and safety. That said, I generally agree that if everything is critical, nothing is critical, and that leaders must prioritize our most critical assets. To that end, I would point to assets where intellectual property theft or disruption could have catastrophic consequences and to

what are considered the "lifeline" functions – water, energy, transportation, and communications – as particularly critical to the security and safety of the nation.

- d. If confirmed, what steps will you take to assess risks to various sectors and align CISA's efforts to those areas of greatest risk?

As I understand it, CISA's National Risk Management Center (NRMC) worked with the critical infrastructure community to highlight the National Critical Functions, acknowledging that the interconnectedness of the sectors and the sophistication of threats and hazards means that the consequences of an attack or imminent threat do not impact only one sector. The NRMC brings the private sector, government agencies, and other key stakeholders together to identify, analyze, prioritize, and manage the most significant risks—cyber, physical, supply chain and more—to these important functions.

If confirmed, I would ensure that the NRMC is fully resourced to enable the success of this important mission to ensure that CISA's efforts are fully aligned to address the areas of greatest risk.

56. Do you believe the federal government should be more actively involved in ensuring cybersecurity of private companies, including critical infrastructure? For example, do you support a regulatory approach to private sector cybersecurity and if so, how do you envision such an approach working?

As the vast majority of the nation's networks, including its critical infrastructure, is owned and operated by the private sector, it is imperative that the federal government cultivates partnerships with the private sector that promote operational collaboration and a collective defense of our nation. I generally agree and have witnessed first-hand during my time in the private sector, that regulation can play a useful role in incentivizing best cybersecurity practices; that said, overly complex and unharmonized regulatory regimes can be unhelpfully burdensome and result in perverse incentives—checklist compliance vice material operational improvements.

57. What do you consider to be the top emerging threats to U.S. critical infrastructure? If confirmed, how will you position CISA to be ready to address them?

Evolving threats related to emerging technologies such as advanced computing, artificial intelligence, and 5G and future mobile communications platforms will present new risks to U.S. critical infrastructure. In its most recent Annual Threat Assessment, the U.S. Intelligence Community noted, "U.S. leadership in emerging technologies is increasingly challenged, primarily by China." Additionally, "new technologies, rapidly diffusing around the world, put increasingly sophisticated capabilities in the hands of small groups and individuals as well as enhancing the capabilities of nation states."

If confirmed, I will utilize the resources of CISA's National Risk Management Center and the U.S. Intelligence Community to better understand emerging threats to U.S. critical

infrastructure. CISA should strengthen its collaboration with the private sector to build security into its culture, capabilities, and processes as much as possible and identify strategies for mitigating emerging risk as soon as possible. Additionally, I will ensure that as CISA invests in capabilities for securing government and private sector networks that it factors emerging threats into those decisions.

58. Do you think the current DHS statutory authorities and programs are adequate for ensuring the cybersecurity of U.S. critical infrastructure? If not, what changes do you think are needed?

At this point, as a private citizen, I am unable to judge whether current statutory authorities and programs are adequate for ensuring the security of U.S. critical infrastructure. I understand that Congress recently provided CISA with new authorities to improve its ability to ensure the cybersecurity of U.S. critical infrastructure. If confirmed, I look forward to ensuring CISA is implementing all of its authorities in the most effective manner and commit to coming back to you if I believe that changes to authorities or programs are indeed required to further empower CISA.

59. How do you plan to balance the challenges that CISA faces protecting critical infrastructure with private sector ownership of most of this infrastructure, if confirmed?

As the vast majority of critical infrastructure is owned and operated by the private sector, CISA plays an important role in partnering with the private sector to support them with voluntary technical assistance, guidance, information-sharing, and incident response capabilities.

60. What is the biggest challenge the Department faces as it works with election agencies and election service providers to bolster election infrastructure cybersecurity?

If confirmed, I would intend to engage early on with the election community to understand their needs and work to ensure that CISA is postured to fulfill them. As I understand it, CISA has good relationships with election agencies and election service providers and has seen significant improvements in the security of state election systems, but additional work needs to be done at the local level. I look forward to identifying ways CISA can expand its information sharing and support to election agencies and election service providers at all levels of government.

61. What do you consider to be the greatest threats against our nation's election infrastructure?

I believe the greatest threats to our nation's election infrastructure come from cyber-attacks, specifically from ransomware deployed by criminal gangs potentially acting as a proxy of nation-states or for their own material gain. The proliferation of ransomware is truly a scourge and one that will require a whole-of-society approach to effectively enable the disruption of the ransomware business model. If confirmed, I look forward to leveraging CISA's capabilities to help prevent ransomware attacks through guidance and

best practices and to mitigate their impacts through technical assistance and support. Another major threat to election infrastructure comes from misinformation and disinformation; if confirmed, I would continue to position CISA to deal with such threats, as it did during the 2020 elections.

62. In your opinion, what is the appropriate role of the federal government in securing election infrastructure?

Fair and free elections are a hallmark of American democracy; the American people's confidence in the value of their vote is principally reliant on the security and resilience of the infrastructure that makes the Nation's elections possible. Accordingly, an electoral process that is both secure and resilient is a vital national interest and, as I understand it, one of CISA's highest priorities. State and local governments administer elections. CISA's role is to work closely and collaboratively with those on the front lines of elections—state and local governments, election officials, federal partners, and vendors—ensuring that they have the technical support, guidance, information, and resources to enable them to effectively manage risks to their election infrastructure.

63. If confirmed, how will you ensure CISA fulfills its role in addressing threats to election infrastructure? Please describe how CISA will assist the Department in securing the nation's election infrastructure in preparation for the 2022 midterm elections and thereafter.

CISA did an excellent job working with State and Local entities to help protect election infrastructure during the 2020 elections. As part of this effort, CISA forged productive relationships with election officials at all levels. CISA also forged highly collaborative partnerships with key elements of the U.S. government, including NSA, FBI, and CYBERCOM, as well as the private industry, to ensure the security and resilience of critical infrastructure. If confirmed, I would build on these successful partnerships and lessons learned to ensure the security of the 2022 midterms elections and those in coming years.

Chemical Security

64. What do you consider to be the greatest threat facing the chemical sector? If confirmed, how would you address those threats?

The Chemical Sector is an integral component of the U.S. economy that manufactures, stores, uses, and transports potentially dangerous chemicals upon which a wide range of other critical infrastructure sectors rely. Securing these chemicals against a growing and evolving risk landscape requires vigilance from both the private and public sectors. A number of factors, stemming from environmental, technological, human, and physical causes may affect the critical infrastructure security and resilience posture of the chemical industry and its stakeholders. Separate from extreme natural hazards that can create dangerous conditions involving hazardous chemical materials, the greatest threat facing the sector likely stems from attacks by sophisticated cyber threat actors that can

disrupt, destroy, or manipulate industrial control systems (ICSs). The combination of reliance on these ICSs for chemical manufacturing process control with the potential for run-away reactions without proper controls and the secondary risks associated with accidental release of hazardous materials makes cybersecurity an indispensable part of operational safety and security. If confirmed, I would ensure that CISA, given DHS's role as the Sector Risk Management Agency for the chemical sector, is working closely with the sector to manage the risk of such threats, developing tools and resources for assessing facility security and resilience and collaborating with public and private sector partners to ensure that chemical facility owners and operators receive important information about man-made and natural threats and hazards that pose the greatest risk to the Nation's critical chemical facilities.

65. The Chemical Facility Anti-Terrorism Standards (CFATS) program expires on July 27, 2023. What is your assessment of the effectiveness of that program?

As a private citizen, I am unable to assess the effectiveness of the CFATS program; if confirmed, I will conduct an assessment of the program and come back with my observations.

66. The President's proposed budget for FY 2021 proposed eliminating the CFATS program and replacing it with significantly increased funding for Protective Security Advisors, "to provide voluntary support for chemical production facilities without the unnecessary burden of regulatory requirements, placing the chemical sector on par with all the other critical infrastructure sectors for which CISA has oversight."

- a. Do you agree with that recommendation?

As a private citizen, I generally agree that overly burdensome regulatory regimes can be counterproductive; that said, I do not have enough details on the CFATS program to say whether or not I agree with the recommendation at this time. I do agree that increased funding for Protective Security Advisors will be important and useful in providing support to chemical production facilities in ensuring their security and resilience. That said, as witnessed in the recent ransomware attack against pipelines, voluntary standards may not be enough to ensure the implementation of necessary measures.

- b. If not, why do you believe the chemical sector should be subject to higher regulatory scrutiny than other sectors when it comes to security, such as electric, water, and financial infrastructure?

As noted above, I don't currently have enough information about the CFATS program to say whether the chemical sector should be subject to higher regulatory scrutiny than other sector when it comes to security. If confirmed, I will study the issue and provide my views on the matter.

67. What, if any, changes would you make to the CFATS program if confirmed?

As a private citizen, I don't currently have enough information about the CFATS program to say what changes I would make to it. If confirmed, I will study the issue and provide my views on the matter.

68. How does the proposed Ammonium Nitrate Security Program intersect with existing CFATS regulations?

The ANSP Notice of Proposed Rulemaking seeks to reduce the likelihood of a terrorist attack involving ammonium nitrate by requiring purchases and sellers to apply for an Ammonium Nitrate Registered User Number with CISA, with each applicant vetted against the Terrorist Screening Database (TSDB). While both the ANSP and CFATS are focused on the security of the chemical sector, CFATS is focused specifically on security at facilities vice ANSP which is focused on purchasers and sellers of chemicals.

69. This August will mark one decade since DHS published the pending ANSP proposed rule. If confirmed, what would you seek to do with regard to the proposed rule?

As a private citizen, I don't currently have enough information to say what should be done with the proposed rule. If confirmed, I will study the issue and provide my views on the matter.

Intelligence, Misinformation, and Disinformation

70. Nation-state actors are increasingly using domestic networks to conduct foreign espionage campaigns. What is CISA's role in mitigating the exploitation of our country's information infrastructure and if confirmed, how would you help thwart this persistent activity?

CISA works with the U.S. Intelligence Community, the Federal Bureau of Investigation, and private industry stakeholders to ensure system owners and network defenders are aware of threats including from nation state actors and what actions they can take to mitigate them. CISA is responsible for working closely with U.S. communications companies, internet service providers, managed service providers, and cloud computing companies to enhance the security of these platforms from nation state threats. Protecting sensitive information, including sensitive intellectual property, is part of CISA's core mission related to securing U.S. critical infrastructure. Through the newly authorized Joint Cyber Planning Office and other efforts, CISA can strengthen operational collaboration with the private sector to better thwart foreign espionage campaigns. Also, when incidents do occur, CISA serves as the lead on asset response to help victims mitigate the impact.

71. Please describe your understanding of CISA's role with respect to the DHS Office of Intelligence and Analysis (I&A). If confirmed, how do you plan to improve the relationship between CISA and I&A?

I understand that CISA works closely with DHS I&A, which is the Department's element of the U.S. intelligence community. If confirmed, I would spend time better understanding the relationship between CISA and I&A to ensure it is optimized. I do think it is critical for CISA to have access to the best cyber threat intelligence to enable it to prepare for and respond effectively to threats to federal government networks and critical infrastructure. If confirmed, I will ensure that is the case.

72. Please describe your understanding of CISA's role with respect to the broad intelligence and military community, particularly with respect to the National Security Agency.

CISA works in close partnership with the Department of Defense, which oversees defense networks, and the National Security Agency, the national manager for national security systems, to ensure that technical guidance and direction is mutually reinforcing and maximizes consistency, whenever possible. Separately, CISA's role as quarterback for the cyber defense of the federal government and as the front door for industry partnerships on cybersecurity and infrastructure security is enhanced through close working relationships with the Intelligence Community, including the National Security Agency, which can provide intelligence and early warning about threats and vulnerabilities based on its foreign intelligence collection mission.

73. Do you believe that the lines between military and civilian cybersecurity responsibilities are appropriately drawn?

At this point, I do not have enough information to judge whether the lines between military and civilian cybersecurity responsibilities are indeed appropriately drawn though my sense is that they are. If confirmed, I will revert with any observations on the need to further clarify these lines.

74. What role does CISA play in addressing the threat of malign foreign influence campaigns?

As I understand it, CISA worked during the 2020 elections to help the American people better understand the scope and scale of malign foreign influence and how citizens can play a role in reducing the impact of it on their organizations and communities. I understand that CISA continues to carry out these activities as it relates to the targeting of elections and critical infrastructure. CISA works in close coordination with interagency partners, social media companies, academia, and international partners to build resilience against malign foreign influence activities.

75. What are your views on the role of CISA in addressing misinformation and disinformation?

I believe that CISA can play a valuable role in helping the American people understand the scope and scale of misinformation and disinformation targeting elections and critical infrastructure in particular, building national resilience through public awareness, and

engaging subject matter experts and trusted voices across society to enable a whole-of-society approach.

76. While misinformation and disinformation efforts have recently focused on election interference, it is clear that misinformation is ubiquitous, and adversaries utilize information operations on a regular basis on a variety of issues. What actions would you take to ensure that the Department is postured to address misinformation and disinformation both around specific events (such as elections or the COVID-19 pandemic) and as a general threat?

I agree that misinformation is ubiquitous and can threaten critical infrastructure. If confirmed, I would conduct an assessment of CISA's activities in this space to ensure is the agency is effectively resourced to address the threats of misinformation and disinformation—to include adverse use of emerging technologies like artificial intelligence to create deepfakes—both around specific threats and more generally as it relates to broad threats to critical infrastructure.

77. What actions will you take to ensure that CISA and DHS have the right policies and programs in place to address misinformation and disinformation regarding elections, specifically, and online, writ-large?

CISA's efforts in this space must ensure the protection of privacy, free speech, and civil liberties. If confirmed, I would ensure that CISA consults closely with the DHS Privacy Office and DHS Office for Civil Rights and Civil Liberties on all activities. Moreover, I understand that CISA works closely with civil society groups, researchers, and state and local government officials, and in close collaboration with the FBI's Foreign Influence Task Force, the U.S. Department of State, the U.S. Department of Defense, and other agencies across the federal government. If confirmed, I would conduct an assessment of CISA's activities to ensure it has the right policies, programs, and cohesive stakeholder relationships in place to address the threats of misinformation and disinformation targeting critical infrastructure.

V. Accountability

Whistleblower Protections

78. Protecting whistleblowers and their confidentiality is of the utmost importance to this Committee.
- Please describe any previous experience with handling whistleblower complaints. What steps did you take to ensure those individuals did not face retaliation and their claims were thoroughly investigated?

I have had no previous experience handling whistleblower complaints.
 - If confirmed, what steps will you take to ensure whistleblower complaints are handled appropriately at CISA?

If confirmed, I will review policies and procedures in place at CISA related to the handling of whistleblower complaints to ensure they are handled appropriately and in accordance with all applicable federal laws and regulations.

- c. If confirmed, what steps will you take to ensure whistleblowers at CISA do not face retaliation, whistleblower identities are protected, and complaints of retaliation are handled appropriately?

Whistleblowers are entitled to protection under the law. If confirmed, I will review policies and procedures in place at CISA related to the handling of whistleblower complaints to ensure whistleblowers are protected to the fullest extent possible under applicable federal laws and regulations.

Cooperation with Inspectors General

79. What is your view of the role of the DHS Office of Inspector General (OIG)? Please describe what you think the relationship between the CISA Director and the OIG should be. If confirmed, what steps would you take to establish a working relationship with the Inspector General?

I believe that the DHS Office of Inspector General (OIG) plays an important role in ensuring transparency and accountability across the Department. If confirmed as the CISA Director, I will establish a productive working relationship with the OIG to ensure that their efforts are fully supported.

80. If confirmed, do you commit to ensuring that all recommendations made to CISA by the DHS Inspector General are reviewed, responded to, if necessary, and, unless the agency justifies its disagreements with the recommendations, implemented to the fullest extent possible within a reasonable time period?

Yes.

81. If confirmed, do you commit without reservation to ensuring the DHS OIG receives timely access to agency records and to interview agency employees?

Yes, in accordance with all applicable federal laws and regulations.

82. If confirmed, what steps will you take to ensure your office and employees cooperate fully and promptly with OIG requests?

If confirmed, I will review policies and procedures in place at CISA related to the handling of OIG requests to ensure they are handled appropriately and in accordance with all applicable federal laws and regulations.

Cooperation with GAO

83. If confirmed, do you commit without reservation to ensuring GAO receives timely, comprehensive responses to requests to DHS, including for records, meetings, and information?

Yes, in accordance with all applicable federal laws and regulations.

84. If confirmed, do you commit to fully cooperate in a timely manner with any audits, investigations, and other reviews and related requests for information from GAO?

Yes, in accordance with all applicable federal laws and regulations.

85. If confirmed, what steps will you take to ensure your office and employees cooperate fully and promptly with GAO requests?

If confirmed, I will review the policies and procedures in place at CISA that guide agency interactions with GAO to ensure GAO receives access to CISA in accordance with all applicable federal laws and regulations.

VI. Relations with Congress

86. Do you agree without reservation to comply with any request or summons to appear and testify before any duly constituted committee of Congress if you are confirmed?

Yes.

87. Do you agree without reservation to make any subordinate official or employee available to appear and testify before, or provide information to, any duly constituted committee of Congress if you are confirmed?

Yes.

88. Do you agree without reservation to comply fully, completely, and promptly to any request for documents, communications, or any other agency material or information from any duly constituted committee of the Congress or any five members of the Committee on Homeland Security and Governmental Affairs if you are confirmed?

Yes.

89. If confirmed, how would you make certain that you respond in a timely manner to Member requests for information?

I will take all necessary actions within my power to ensure that I respond in a timely manner to Member requests for information.

90. If confirmed, will you direct your staff to adopt a presumption of openness where practical, including identifying documents that can and should be proactively released to the public, without requiring a Freedom of Information Act request?

Yes.

91. If confirmed, will you keep this Committee apprised of new information if it materially impacts the accuracy of information your agency's officials have provided us?

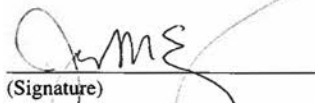
Yes.

VII. Assistance

92. Are these answers your own? Have you consulted with DHS or any other interested parties? If so, please indicate which entities.

These answers are my own, drawn from my own knowledge and experience. I consulted with appropriate officials at DHS and asked them to review all answers. I was free to accept or reject their feedback.

I, Jennie Margaret Easterly, hereby state that I have read the foregoing Pre-Hearing Questionnaire and that the information provided therein is, to the best of my knowledge, current, accurate, and complete.



(Signature)

This 4th day of June, 2021

**Senator Rand Paul
Post-Hearing Questions for the Record
Submitted to Jen Easterly**

**Nominations of Robin Carnahan to be Administrator, General Services Administration;
Jen Easterly to be Director, Cybersecurity and Infrastructure Security Agency, DHS; and
Chris Inglis to be National Cyber Director
Thursday, June 10, 2021**

1. On December 21, 2018, the Federal Acquisition Supply Chain Security Act of 2018 was enacted as Title II of P.L. 115-390.¹ Under the Federal Acquisition Supply Chain Security Act, the Secretary of Homeland Security, the Secretary of Defense, and the Director of National Intelligence are authorized to exclude from procurement or remove from existing systems any information technology or telecommunications equipment that are determined to pose some level of risk to the security of government data. Additionally, CISA is required by to be represented on the Federal Acquisition Security Council, which is tasked with making recommendations on exclusion and/or removal orders to the Secretary of Homeland Security, the Secretary of Defense, and the Director of National Intelligence.

Question: Would you agree that a potential procurement source that is otherwise qualified to contract with the government should not be excluded from consideration based solely or substantially on the fact of foreign ownership? In other words, do you agree that a company owned by a foreign interest does not *ipso facto* pose a national security threat to the U.S. government supply chain?

Yes. In fact, the law prohibits authorizing the issuance of an exclusion or removal order based solely on the fact of foreign ownership of a potential procurement source that is otherwise qualified to enter into procurement contracts with the federal government.

2. In testimony before the Senate Homeland Security and Government Affairs Committee in October 2018, Federal Bureau of Investigation (FBI) Director Christopher Wray discussed what the FBI describes as the “Going Dark” problem.² In short, the FBI does not want service providers like Google and Apple to offer confidential services because they may hinder efforts by law enforcement to collect and/or analyze private communications. The FBI has suggested that Congress should consider legislation forcing companies to build or enable “backdoor” access to such services; however, backdoors inherently degrade the security of these systems.

On May 15, 2018, Director of the National Counterintelligence and Security Center (NCSC) William Evanina testified³ that government officials and Members of Congress

¹ <https://www.congress.gov/bills/115/congress/house-bill/7327>

² <https://www.hsgac.senate.gov/imo/media/doc/Testimony-Wray-2018-10-10.pdf>

³ <https://www.intelligence.senate.gov/hearings/open-hearing-nomination-william-r-evanina-be-director-national-counterintelligence-and>

should avoid potentially “backdoored” services in favor of truly confidential “end-to-end” encrypted services.

Question: Do you support deliberately weakening end-to-end encrypted communications services? If so, how? And if so, for what purposes?

Absolutely not. Strong encryption is a foundational component of our cybersecurity and critical for the protection of our nation’s privacy and civil liberties.

Question: Have you at any time ever advocated for deliberately weakening end-to-end encryption as a part of your work at the National Security Council, the National Security Agency, or the U.S. Army?

While I never personally advocated for the deliberate weakening of end-to-end encryption during my service, there were occasions where an organization I served in would consider how to weaken systems used by foreign adversaries for national security purposes. The details of those specific cases are, of necessity, classified and not accessible to me, but were all, to the best of my knowledge, conducted within the scope of the government’s limited authorities with appropriate oversight and legal reviews.

Question: Do flaws impacting the confidentiality of popular encryption tools represent a national security threat?

Yes; I believe that anything that could potentially weaken the security of encrypted communications could pose a national security threat.

Question: Do you agree with former NCSC Director Evanina’s assertion that Members of Congress should use services with true end-to-end confidentiality?

Yes.

Question: Would you recommend that the U.S. armed forces and government agencies use services with true end-to-end confidentiality?

Yes.

Question: Would you recommend that the general public use services with true end-to-end confidentiality?

Yes.

Question: If your answers to the previous two questions (“Would you recommend that the U.S. armed forces and government agencies use services with true end-to-end confidentiality?” and “Would you recommend that the general public use services with true end-to-end confidentiality?”) differ – why do they differ?

N/A.

Question: Would you recommend that providers work to ensure that cell phones, messaging applications, and other services Americans rely on be “secure by default”?

Yes.

3. **Question:** What ideas and aspirations do you have to improve the management of the CISA with respect to identifying and eliminating waste, fraud or abuse?

Eliminating waste, fraud, or abuse would be a key priority of mine if I am confirmed as the Director of CISA. If confirmed, I would conduct an early and comprehensive review of all of CISA's management processes to ensure that mechanisms are in place to support efficient, effective and economical operations. In addition, I would engage early on with the Office of the Inspector General to establish a productive working relationship to ensure that their efforts to deter, identify and address fraud, abuse, mismanagement and waste are fully supported. Moreover, if confirmed, I would welcome the opportunity to work with your staff and the Government Accountability Office to ensure that the CISA is operating at peak efficiency and that CISA employees were being good stewards of Americans tax dollars.

4. **Question:** If confirmed, what will you do to ensure employees can and will disclose violations of law, rule, or regulation, and instances of fraud, waste, abuse and mismanagement within CISA to any or all appropriate sources, including Congress?

If confirmed, I would communicate clearly to the workforce in written policy and verbal guidance, and continually reinforce it at meetings with key leaders and the various divisions across CISA, that employees that have concerns with any violation of law, rule, or regulation, or instances of fraud, waste, abuse, or mismanagement should feel empowered to report their concerns to all appropriate sources, including the Congress. I will also make it clear that such abuse will not be tolerated and will be investigated and prosecuted to the full extent of the law, and emphasize that anyone who has the moral courage to raise their concerns should feel empowered to do so and not suffer fear of reprisal.

5. **Question:** As your nomination moves forward, will you commit to providing a written response to any further questions related to your nomination prior to your confirmation vote?

Yes.



The Honorable Gary Peters
Chairman, Senate Committee on Homeland
Security and Governmental Affairs
340 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Robert Portman
Ranking Member, Senate Committee on
Homeland Security and Governmental Affairs
340 Dirksen Senate Office Building
Washington, DC 20510

May 27, 2021

RE: Upcoming Confirmation Hearing for Jen Easterly as the Director of the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency

Dear Chairman Peters and Ranking Member Portman,

On behalf of the Analysis and Resilience Center for Systemic Risk (ARC), I am writing to express our support for Jen Easterly's nomination for the Director of the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA). ARC members are owners and operators of infrastructure formally designated by the Department of Homeland Security under Section 9 of Executive Order 13636 as systems where a cybersecurity incident could have catastrophic effects on economic and national security.

These "Section 9" firms founded the ARC as a non-profit, cross-sector organization to work with each other and with the U.S. Government to mitigate systemic risk to designated infrastructure. While the ARC partners with many agencies across the U.S. Government and the Intelligence Community, CISA's authorities and critical infrastructure focus make it central to the effort of identifying and mitigating systemic risks. As CISA's responsibilities and authorities increase, operational experience in the CISA Director is essential, as is the ability to nimbly apply CISA's capabilities in partnerships across the U.S. Government and the private sector.

Jen Easterly has a deep understanding of the U.S. Government's posture on cyber, as well as the private sector's exposure, operations, and needs earning her the trust and respect of her private sector colleagues. As Morgan Stanley's Head of Resilience and its Fusion Resilience Center, she leads teams responsible for preparing for and responding to the full range of threats, vulnerabilities, or incidents that threaten the Firm. Because of her leadership, Morgan Stanley is better prepared to manage operational risks and business disruptions. Given recent security events and the importance of public/private partnerships to ensure resilience in U.S. infrastructure, Ms. Easterly's leadership and credentials will enable her to successfully build on CISA's strong foundation.

The ARC and its members work closely with CISA and look forward to continued collaboration. The growing cyber threats demand a CISA leader who can grow the agency to align with the current and future cyber threat environment. Jen Easterly would bring much credibility to the role of Director and would be a force multiplier in driving better outcomes through public/private collaboration.

We urge the Senate Homeland Security and Governmental Affairs Committee to support Ms. Easterly's nomination by recommending her for Senate Confirmation.

Sincerely,

Scott DePasquale, President and CEO
The Analysis and Resilience Center for Systemic Risk

CHAMBER OF COMMERCE
OF THE
UNITED STATES OF AMERICA

CHRISTOPHER D. ROBERTI
SENIOR VICE PRESIDENT FOR
CYBER, INTELLIGENCE, AND SUPPLY
CHAIN SECURITY POLICY

1615 H STREET, N.W.
WASHINGTON, D.C. 20062-2000
202/463-5449
CROBERTI@USCHAMBER.COM

June 9, 2021

The Honorable Gary Peters
Chair
Committee on Homeland Security and
Governmental Affairs
United States Senate
Washington, DC 20510

The Honorable Rob Portman
Ranking Member
Committee on Homeland Security and
Governmental Affairs
United States Senate
Washington, DC 20510

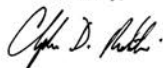
Dear Chairman Peters and Ranking Member Portman:

The U.S. Chamber of Commerce strongly supports the nomination of Jen Easterly to be Director of the Cybersecurity and Infrastructure Security Agency ("CISA"). Ms. Easterly has the experience needed to lead CISA in a time of significant growth and expansion of cyber threats to the United States.

Ms. Easterly has been on the front line of understanding, preparing, and defending a global enterprise from a range of threats. As head of Morgan Stanley's Fusion Resilience Center, Ms. Easterly led organizations in assessing, evaluating and understanding risk and operational disruption. Earlier in her career, Ms. Easterly was instrumental in the design and development of U.S. Cyber Command. She has also served in senior positions within the National Security Agency and National Security Council.

The Chamber expects the next CISA Director to be an imaginative problem-solver, articulate communicator, and effective representative for advancing the Agency's core mission of minimizing cyber risk. We have full confidence that Ms. Easterly embodies these characteristics, along with a unique ability to turn strategy into action. We urge the Committee to favorably report Ms. Easterly's nomination to the full Senate.

Sincerely,



Christopher D. Roberti

cc: Members of the Senate Committee on Homeland Security and Governmental Affairs

June 8, 2021

The Honorable Gary C. Peters
Chairman
Committee on Homeland Security and Government Affairs
United States Senate
Washington, DC 20510

The Honorable Rob Portman
Ranking Member
Committee on Homeland Security and Government Affairs
United States Senate
Washington, DC 20510

Re: Nomination of Jen Easterly to be Director, Cybersecurity and Infrastructure Security Agency, Department of Homeland Security (PN243)

Dear Chairman Peters and Ranking Member Portman:

We write today to unanimously express our strong support for the nomination of Jen Easterly to serve as the Director of the Cybersecurity and Infrastructure Security Agency at the Department of Homeland Security. We represent a bipartisan cross-section of national security experts and industry leaders, including current and former senior executives and former government officials with significant national security, technology, or cybersecurity responsibilities who have worked with or alongside Jen, in the White House, Department of Defense, Congress, the Intelligence Community, and industry.

Jen comes before your committee with a stellar background in both the public and private sectors. For more than four years, she has served in multiple senior executive and cybersecurity-related roles at Morgan Stanley, a Fortune 100 financial firm with global operations. As the current Head of Firm Resilience and the Fusion Resilience Center, Jen is responsible for ensuring that Morgan Stanley is prepared to respond effectively to business-disrupting risks and incidents that could impact the firm or the larger financial services sector. She was specifically hired by Morgan Stanley to build and lead the firm's Cybersecurity Fusion Center, the operational cornerstone of its cyber defense strategy, and more recently co-led Morgan Stanley's response to the COVID-19 pandemic. This deep private sector operational experience will be critical to her success leading CISA if she is confirmed by the Senate.

Jen's breadth of experience goes well beyond the private sector. She has served for nearly three decades in public service, including in the White House during both Republican and Democratic administrations, as a senior executive at the National Security Agency, and as a warfighter and intelligence professional in the U.S. Army. These experiences have prepared Ms. Easterly to make tough policy and operational decisions. Indeed, she was twice awarded the Bronze Star for meritorious service during combat tours in Iraq and Afghanistan, was hand-picked to build and lead the Army's first cyber battalion, and was selected to be part of the small team charged with the design and creation of U.S. Cyber Command.

Jen's private sector experience, combined with nearly three decades of leading intelligence and national security operations, make her exactly the kind of leader our nation needs at this moment. She has led complex organizations with global footprints in government and industry, understands the importance of responsible stewardship of taxpayer dollars, and can successfully lead the thousands of CISA employees across the country on day one. And she has directed operations both on the battlefield and in the executive suite, a critical ability at a time when our adversaries are increasingly looking to attack our government agencies and critical infrastructure companies, and when close collaboration between the government and the private sector is crucial to more effectively protecting our nation.

Most important, perhaps, is the fact that over the past three decades, Jen has earned the trust and respect of leaders in both the public and private sector, including owners and operators of our nation's critical infrastructure. Her experience taught her the need to bring effective and efficient business processes to bear on tough problems, as well as the importance of building strong relationships and trust between operators and overseers, whether between the executive and legislative branches, or between the c-suite and the boardroom. Simply put, we believe that her extensive operational experience, deep expertise in technology and cybersecurity, and stellar track record in both the public and private sectors will make Jen Easterly an ideal leader for CISA, if the Senate sees fit to provide its consent to her nomination.

Thank you for the opportunity to write to you today; we look forward to answering any questions you may have.

Sincerely,

GEN (Ret) Keith Alexander
Former Director, National Security Agency & Founding Commander, U.S. Cyber Command

Javed Ali
Former Senior Director for Counterterrorism, National Security Council, The White House

Michael Allen
Former Special Assistant to the President and Senior Director for Counter-Proliferation Strategy, National Security Council, The White House

Marene Allison
Chief Information Security Officer, Johnson & Johnson Services, Inc.

Dmitri Alperovitch
Chairman, Silverado Policy Accelerator

Wendy R. Anderson
Former Chief of Staff to Deputy Secretary of Defense, Department of Defense

Nikesh Arora
CEO and Chairman, Palo Alto Networks

Jeremy Bash
Former Chief of Staff, Department of Defense

John B. Bellinger III
Former Legal Adviser, Department of State

Peter Bergen
Vice President, International Security Program, New America

Ernest Bio
Former Chief Operating Officer, Defense Innovation Unit, Department of Defense

Joshua Bolten
Former Chief of Staff to the President, The White House

Bryson Bort
Senior Fellow, National Security Institute, GMU Law School

Reuben E. Brigety
Former U.S. Ambassador to the African Union

Lyndon Brown
Chief Strategy Officer, Pondurance

Kofi Bruce
Chief Financial Officer, General Mills

Cameron Burks
Vice President, Global Security, Adobe, Inc

Tom Burt
Corporate Vice President, Customer Security and Trust, Microsoft Corp.

Robert J. Butler
Former Deputy Assistant Secretary of Defense for Cyber and Space Policy, Department of Defense

Michael H. Campbell
CEO, Fusion Risk Management

Chris Castaldo
Chief Information Security Officer, Crossbeam

Michael Chertoff
Former Secretary of Homeland Security

Frank Cilluffo
Former Special Assistant to the President, The White House

Jared Cohen
Former Policy Planning Staff Member, Department of State

David Coher
Visiting Fellow, National Security Institute, GMU Law School

Matthew T. Cornelius
Executive Director, Alliance for Digital Innovation

Col (Ret.) Christopher P. Costa
Former Special Assistant to the President & Senior Director, National Security Council, The White House

John Costello
Former Deputy Assistant Secretary of Commerce for Intelligence and Security, Department of Commerce

Jason Crabtree
CEO, QOMPLX

Craig Cummings
General Partner, Moonshots Capital

Bryan Cunningham
Former Deputy Legal Adviser, National Security Council, The White House

J. Michael Daniel
Former Special Assistant to the President and Cybersecurity Coordinator, The White House

Janine Davidson
Former Undersecretary of the Navy, United States Navy

Brian de Vallance
Former Assistant Secretary of Legislative Affairs, Department of Homeland Security

Laura M. Deaner
Chief Information Security Officer, Northwestern Mutual

Robert L. Deitz
Former General Counsel, National Security Agency

David G. DeWalt
Founder, NightDragon Security

Brett DeWitt
Former Cybersecurity, Infrastructure Protection and Security Technologies Subcommittee Staff
Director, Committee on Homeland Security, United States House of Representatives

Donald R. Dixon
Co-Founder & Managing Director, ForgePoint Capital

Peter Dixon
CEO, Second Front Systems

Paula Doyle
Former Associate Deputy Director for Operations Technology, Central Intelligence Agency

R.P. Eddy
Former Director, Global Issues and Multilateral Affairs, National Security Council, The White
House

Brian J. Egan
Former Legal Advisor to the National Security Council and Deputy Counsel to the President,
The White House

Jeffrey W. Eggers, CDR USN (Ret.)
Former Special Assistant to the President for National Security Affairs, National Security
Council, The White House

Daniel R. Ennis
Former Director, NSA Threat Operations Center, National Security Agency

William Evanina
Former Director, National Counterintelligence Security Center

Karen S. Evans
Former Assistant Secretary, Cybersecurity, Energy Security and Emergency Response,
Department of Energy

Thomas A. Fanning
CEO, Southern Company

Jamil Farshchi
Chief Information Security Officer, Equifax

Don Faul
CEO, Athos

Guy L. Filippelli
Managing Partner, Squadra Ventures

Alexander M. Gallo
Executive Director, Common Mission Project

Michael Geffroy
Former General Counsel, Select Committee on Intelligence, United States Senate

Glenn S. Gerstell
Former General Counsel, National Security Agency

Amy Gilani
Chief Growth Officer, CounterCraft

John M. Gilligan
Former Chief Information Officer, United States Air Force

Ryan Gillis
Former Director of Cybersecurity Policy and Legislative Affairs, National Security Council, The White House

James P. Gorman
Chairman and CEO, Morgan Stanley

Zach Graves
Head of Policy, Lincoln Network

Ronald Green
Chief Security Officer, Mastercard

Eric A. Greenwald
Former Special Assistant to the President and Senior Director for Cyber Security, National Security Council, The White House

Andrew Grotto
Former Senior Director for Cyber Policy, National Security Council, The White House

W. Clay Grubb
CEO, Grubb Properties

Stephen J. Hadley
Former National Security Advisor to President George W. Bush, The White House

Davis Hake
Former Director for Federal Information Technology Security, National Security Council, The White House

General Michael Hayden
Former Director, Central Intelligence Agency

Francis Q. Hoang
Former Associate Counsel to the President, The White House

Chris P. Hsu
Former CEO, Hewlett Packard Enterprise Software & Micro Focus

Aaron Hughes
Former Deputy Assistant Secretary of Defense for Cyber Policy, Department of Defense

Joanne Isham
Former Deputy Director, National Geospatial Intelligence Agency

Jamil N. Jaffer
Former Associate Counsel to the President, The White House

Merit E. Janow
Dean, School of International and Public Affairs & Professor of Practice, International Economic Law & International Affairs, Columbia University

Frank R. Jimenez
Former General Counsel of the Navy, United States Navy

Clete D. Johnson
Former Senior Adviser for Cybersecurity and Technology, Office of the Secretary, Department of Commerce

Sean M. Joyce
Former Deputy Director, Federal Bureau of Investigation

Ely Kahn
Former Director of Cybersecurity Policy, National Security Council Staff, The White House

Geof Kahn
Managing Director of Federal Affairs and Global Cyber Policy Lead, Accenture

Lisa Kaplan
Founder, Alethea Group

Sarah Kauss
Founder, S'well Bottle

Andy Keiser
Former Senior Advisor, Permanent Select Committee on Intelligence, United States House of Representatives

Dr. Christopher Kirchhoff
Former Director for Strategy Planning, National Security Council

Douglas Kramer
Former Deputy Administrator, U.S. Small Business Administration

Christopher C. Krebs
Former Director, Cybersecurity and Infrastructure Security Agency, Department of Homeland Security

Paul B. Kurtz
Former Senior Director for Cyber Security and Special Assistant to the President for Critical Infrastructure Protection, The White House

Elena Kvachko
Chief Trust Officer, SAP

Robert M. Lee
CEO and Co-Founder, Dragos, Inc.

Vice Admiral (Ret) Mike LeFever, USN
Former Director, Strategic Operational Planning, National Counterterrorism Center

Michael Leiter
Former Director, National Counterterrorism Center

Robert Lentz
Former Deputy Assistant Secretary of Defense, Cyber, Identity, and Information Assurance, Department of Defense

James A. Lewis
Senior Vice President and Director, Strategic Technology Program, Center for Strategic and International Studies

William Lin
Managing Director, ForgePoint Capital

David Luckey
Former Director of Homeland Security and Counterterrorism Advisor to the Chairman,
Committee on Homeland Security and Governmental Affairs, United States Senate

Jane H. Lute
Former Deputy Secretary, Department of Homeland Security

John Maguire
Former Senior Advisor, Select Committee on Intelligence, United States Senate

Dr. Michele L. Malvesti
Former Senior Director for Combating Terrorism Strategy, National Security Council, The
White House

Jeanette Manfra
Former Assistant Director, Cyber and Infrastructure Security Agency, Department of Homeland
Security

Maj Gen (Ret.) James "Spider" Marks, United States Army
Former Commanding General of the Army Intelligence Center

Matthew Masterson
Former Senior Cybersecurity Advisor, Cybersecurity and Infrastructure Security Agency,
Department of Homeland Security

Dr. Adrian M. Mayers
Vice President and Chief Information Security Officer, Premiera Blue Cross

Barry R. McCaffrey
Former Director, Office of National Drug Control Policy, The White House

GEN (Ret.) Stanley A. McChrystal
Former Commander, International & Security Forces – Afghanistan

Bruce W. McConnell
Former Deputy Under Secretary for Cybersecurity, Department of Homeland Security

Mike McConnell
Former Director of National Intelligence

Mary B. McCord
Former Acting Assistant Attorney General for National Security, National Security Division,
Department of Justice

Michael C. McGarrity
Former Assistant Director, Counterterrorism Division, Federal Bureau of Investigation

Alexander Macgillivray
Former Deputy United States Chief Technology Officer, The White House

Cheri F. McGuire
Former Director, National Cyber Security Division/US-CERT, Department of Homeland Security

Coleman Mehta
Former Director of Legislative Affairs, National Security Council, The White House

Jenny Menna
Former Director, Critical Infrastructure Cyber Protection and Awareness, Department of Homeland Security

Doug Merritt
CEO, Splunk Inc.

Marten Mickos
CEO, HackerOne

Dr. James N. Miller
Former Under Secretary of Defense for Policy, Department of Defense

Mark Montgomery
Senior Director, Center on Cyber and Technology Innovation, Foundation for Defense of Democracies

Michael Morell
Former Deputy Director and Acting Director, Central Intelligence Agency

Katie Moussouris
Founder and CEO, Luta Security

John C. Nagengast
Former Principal Director for Corporate Strategy, National Security Agency

James C. O'Brien
Former Special Presidential Envoy for Hostage Affairs, Department of State

Matthew G. Olsen
Former Director, National Counterterrorism Center

Dr. Andy Ozment
Former Assistant Secretary for Cybersecurity, Department of Homeland Security

Christopher Painter
Former Coordinator for Cyber Issues, Department of State

Monica Pal
Former CEO, 4iQ Cyber Intelligence

Alan Paller
Founder, SANS Institute

Todd Y. Park
Former United States Chief Technology Officer, The White House

Brian G. Parr
Chief Security Officer, Citigroup

Dr. DJ Patil
Former United States Chief Data Scientist, The White House

Kelly Perdew
Co-Founder and Managing General Partner, Moonshots Capital

Sonja Hoel Perkins
Founder, The Perkins Fund, Broadway Angels, and Project Glimmer

Dr. Lenora Peters Gant
National Security Executive Senior Advisor, Howard University School of Business

General (Ret) David Petraeus
Former Director, Central Intelligence Agency

Neal Pollard
Former Manager, National Counterterrorism Center

Matthew Prince
Co-Founder & CEO, Cloudflare

Richard Puckett
Chief Information Security Officer and Global Head of Product Security, SAP

Kiran Raj
Former Deputy General Counsel, Department of Homeland Security

Sherri Ramsay
Former Director, NSA Threat Operations Center, National Security Agency

Nicholas Rasmussen
Former Director, National Counterterrorism Center

Col. (ret.) Gregory Rattray
Former Director for Cybersecurity, National Security Council, The White House

Alan Charles Raul
Former Vice Chairman, Privacy and Civil Liberties and Oversight Board

Jonathan Reiber
Former Speechwriter and Chief Strategy Officer for Cyber Policy, Office of the Secretary of Defense, Department of Defense

Philip Reiner
Former Senior Director for South Asia, National Security Council, The White House

Philip R. Reitingger
Former Deputy Under Secretary, National Programs and Protection Directorate, Department of Homeland Security

Daniel E. Rice
President, Thayer Leadership at West Point

Lindsay Rodman
Executive Director, Leadership Committee for Women in National Security

Mike Rogers
Former Chairman, Permanent Select Committee on Intelligence, United States House of Representatives

Eric Rosenbach
Former Assistant Secretary of Defense for Global Security and Homeland Defense, Department of Defense

Daniel J. Rosenthal
Former Director for Counterterrorism, National Security Council, The White House

Jim Rosenthal
CEO, BlueVoyant

Paul Rosenzweig
Former Deputy Assistant Secretary for Policy, Department of Homeland Security

Norman T. Roule
Former Component Chief, Directorate of Operations, Central Intelligence Agency

Steve Ryan
Founder and CEO, Trinity Cyber, Inc.

Tony Sager
Former Chief, Vulnerability Analysis & Operations Group, National Security Agency

Ted Schlein
Managing Partner, Kleiner Perkins

Dr. Phyllis Schneck
Former Deputy Under Secretary, Cybersecurity and Communications, Department of Homeland Security

Teresa H. Shea
Vice President, Cyber Offense Defense Experts (CODEX), Raytheon

Josette Sheeran
Executive Chair, The McCain Institute

Ambassador (Ret.) Justin Siberell
Former United States Ambassador to Bahrain

Anne-Marie Slaughter
Former Director of Policy Planning, Department of State

Dana Shell Smith
Former United States Ambassador to Qatar

Suzanne E. Spaulding
Former Under Secretary, National Protection and Programs Directorate, Department of Homeland Security

Matthew J. Spence
Former Deputy Assistant Secretary of Defense for Middle East Policy, Department of Defense

Michael B. Steinbach
Former Executive Assistant Director, National Security Branch, Federal Bureau of Investigation

Roberta G. Stempfley
Former Acting Assistant Secretary Cybersecurity and Communications, Department of Homeland Security

Camille Stewart
Former Senior Policy Advisor, Cyber, Infrastructure & Resilience Policy, Department of Homeland Security

Megan Stifel
Former Director for International Cyber Policy, National Security Council, The White House

Paul N. Stockton
Former Assistant Secretary of Defense for Homeland Defense, Department of Defense

Francis X. Taylor, BGen, USAF (Ret)
Former Under Secretary, Office of Intelligence and Analysis, Department of Homeland Security

Paul Tiao, Partner
Cybersecurity and Privacy Group, Hunton Andrews Kurth LLP

Vice Admiral Jan E. Tighe, USN Retired
Former Commander, Fleet Cyber Command

Kiersten E. Todt
Former Executive Director, Presidential Commission on Enhancing National Cybersecurity

Matthew Travis
Former Deputy Director, Cybersecurity & Infrastructure Security Agency, Department of Homeland Security

Amira Valliani
Former Advisor to the Deputy National Security Advisor for Strategic Communications, National Security Council, The White House

Beth Van Schaack
Leah Kaplan Visiting Professor of Human Rights, Stanford Law School

Suzanne Vautrinot, Major General USAF (ret).
Former Commander of Air Force Cyber, Air Force Network Operations, and 24th Air Force, United States Air Force

Stephen R. Vina
Former Chief Counsel for Homeland Security, Homeland Security and Governmental Affairs Committee, United States Senate

Bryan S. Ware
Former Assistant Director for Cybersecurity, Cybersecurity and Infrastructure Security Agency, Department of Homeland Security

Thomas Warrick
Former Deputy Assistant Secretary for Counterterrorism Policy, Department of Homeland Security

Matthew C. Waxman
Former Principal Deputy Director of Policy Planning, Department of State

William F. Wechsler
Former Deputy Assistant Secretary of Defense for Special Operations and Combatting Terrorism, Department of Defense

William Welch
Co-CEO, IronNet Cybersecurity

Linton Wells II
Former Acting Assistant Secretary of Defense for Networks and Information Integration, Department of Defense

Joe Whitely
Former General Counsel, Department of Homeland Security

Major General (Ret) Brett T. Williams
Former Director of Operations, United States Cyber Command, Department of Defense

Harry Wingo
Faculty, College of Information and Cyberspace, National Defense University

Admiral James A. Winnefeld, Jr, USN (retired)
Former Vice Chairman, Joint Chiefs of Staff, Department of Defense

J Alberto Yopez
Co-Founder & Managing Partner, ForgePoint Capital

Amit Yoran
Chairman & CEO, Tenable

N. Elad Yoran
CEO, Security Growth Partners

Sounil Yu
Former Chief Security Scientist, Bank of America

Juan C. Zarate
Former Deputy Assistant to the President and Deputy National Security Advisor for Combatting Terrorism, National Security Council, The White House

Lawrence K. Zelvin
Former Director, National Cybersecurity and Communications Integration Center, Department of Homeland Security

Statement for the Record

John C. (Chris) Inglis
Nominee for the National Cyber Director
Executive Office of the President

Before the
Committee on Homeland Security and Governmental Affairs
United States Senate

June 10, 2021

Chairman Peters, Ranking Member Portman, and distinguished Senators, I am honored to appear before you. I thank this committee for its support in the creation of this new role, the President for nominating me, and Senator King for his generous introduction. I also want to thank both Senator King and Congressman Gallagher for their work leading the Cyberspace Solarium Commission's efforts to improve our Nation's ability to fully realize its aspirations in and through the critical realm of cyberspace.

I want to recognize my family: I thank my parents Robert and Kathleen Inglis who gave their children the priceless gift of a home where service to others, respect, and accountability was expected and freely given as a foundation for life. And I thank my wonderful wife, Anna, and our children, Luciana, Paul and George for their love and support - which has inspired and sustained me through all of my adult life.

I am humbled by the privilege and opportunity to re-enter public service. And while the position of National Cyber Director may be new, I am mindful that the team I would join, should I be confirmed, is one that is already on the field, impressively diverse and broadly engaged. It is a team that includes public servants at federal, state and local levels, and private sector professionals whose collective efforts build, operate and defend the digital infrastructure upon which the delivery of critical services increasingly depends. I am particularly pleased to be able to testify alongside Jen Easterly the prospective Director of CISA and Robin Carnahan the prospective Administrator of GSA. Should we be confirmed, our collaboration will be an important element of any federal cyber strategy going forward.

If confirmed I expect that I should and will be held accountable to add context, leverage and strength to the distributed work of the full cyber team. To that end, the enabling legislation for the National Cyber Director has clearly laid out its core responsibilities. These include forging a coherent and unified federal effort; developing and overseeing the implementation of the National Cyber Strategy, ensuring the coordination of appropriate federal budgets, policy, plans, and procedures; fostering mutually beneficial public-private collaboration; and demonstrable improvements in the resilience, robustness and defense of the cyber ecosystem.

As the legislation acknowledges, these duties require robust engagement with both the private sector, which is on the front lines of this effort, and with the Congress, to whom the National

Cyber Director owes regular updates on cyber risk and the status of U.S. cybersecurity efforts. Additionally, the National Cyber Director occupies a highly visible position in U.S. Government -- one that should be expected to offer a clear, unified voice in public communications and advocacy.

Supporting lines of effort must necessarily address the fact that cyberspace is not built and operated by a single, centralized organization *and* that it is comprised of far more than technology. Essential collaboration and integration will heavily depend on how roles and responsibilities are defined and executed, while the success of a national strategy will depend as much on the skills of our people as on the technologies they employ.

Given those realities, we must ensure that: our technology is built and deployed with security foremost in mind, that the supply-chains that support them are free from security risk, that our people are cyber literate, and that roles, responsibilities and attendant accountability are sufficiently well-defined that we remove fissures and seams in cyber defenses that offer adversaries opportunities to find and exploit weakness.

As this committee and recent witnesses before you have so frequently discussed, SolarWinds, Hafnium, Colonial Pipeline, JBS, and other incidents all signal the urgent need to secure our national critical infrastructure. The pace of events and our adversaries deny us the luxury of biding our time before we seize back the initiative that has too long been ceded to criminals and rogue nations who determine the time and manner of their transgressions.

If confirmed, I will work closely with the Congress, the executive branch, the private sector, and state and local entities to stand up, harness and realize the expected benefits of the Office of the National Cyber Director.

I thank the Committee for considering my nomination and I look forward to your questions.

REDACTED

Version: 28 April 2021

HSGAC BIOGRAPHICAL QUESTIONS FOR EXECUTIVE NOMINEES

I. Basic Biographical Information

Please provide the following information.

<i>Position to Which You Have Been Nominated</i>	
<u>Name of Position</u>	<u>Date of Nomination</u>
National Cyber Director	

<i>Current Legal Name</i>			
<u>First Name</u>	<u>Middle Name</u>	<u>Last Name</u>	<u>Suffix</u>
John	Christopher	Inglis	

<i>Addresses</i>					
<u>Residential Address</u> (do not include street address)			<u>Office Address</u> (include street address)		
			Street: 605 Hillsmere Drive		
City: Annapolis	State: MD	Zip: 21403	City: Annapolis	State: MD	Zip: 21403

<i>Other Names Used</i>						
<u>First Name</u>	<u>Middle Name</u>	<u>Last Name</u>	<u>Suffix</u>	<u>Check if Maiden Name</u>	<u>Name Used From</u> (Month/Year) (Check box if estimate)	<u>Name Used To</u> (Month/Year) (Check box if estimate)
Chris		Inglis			10/1954 Est <input type="checkbox"/>	Present Est <input type="checkbox"/>
					Est <input type="checkbox"/>	Est <input type="checkbox"/>

<i>Birth Year and Place</i>	
Year of Birth (Do not include month and day.)	Place of Birth
1954	Baltimore, MD

<i>Marital Status</i>					
Check All That Describe Your Current Situation:					
Never Married	Married	Separated	Annulled	Divorced	Widowed
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

<i>Spouse's Name</i> (current spouse only)			
<u>Spouse's First Name</u>	<u>Spouse's Middle Name</u>	<u>Spouse's Last Name</u>	<u>Spouse's Suffix</u>
Anna Maria	Stanowski	Inglis	

<i>Spouse's Other Names Used</i> (current spouse only)						
<u>First Name</u>	<u>Middle Name</u>	<u>Last Name</u>	<u>Suffix</u>	<div>Check if Maiden Name</div>	<u>Name Used From</u> (Month/Year) (Check box if estimate)	<u>Name Used To</u> (Month/Year) (Check box if estimate)
Anna Maria	Rodrigues de Mattos	Stanowski		X	05/1951 <div>Est <input type="checkbox"/></div>	03/1978 <div>Est <input type="checkbox"/></div>
Anna Maria	Stanowski	Duncan			03/1978 <div>Est <input type="checkbox"/></div>	12/1983 <div>Est <input type="checkbox"/></div>
Anna Maria	Rodrigues de Mattos	Stanowski		X	12/1983	12/1986

<i>Children's Names (if over 18)</i>			
First Name	Middle Name	Last Name	Suffix
Luciana	Stanowski	Inglis	
Robert Paul	Stanowski	Inglis	
George Andrew	Stanowski	Inglis	

2. Education

List all post-secondary schools attended.

<u>Name of School</u>	<u>Type of School</u> (vocational/technical/trade school, college/university/military college, correspondence/distance/extension/online school)	<u>Date Began School</u> (month/year) (check box if estimate)	<u>Date Ended School</u> (month/year) (check box if estimate) (check "present" box if still in school)	<u>Degree</u>	<u>Date Awarded</u>
U.S. Air Force Academy	Military service academy	07/1972 <input type="checkbox"/> Est	06/1976 <input type="checkbox"/> Est <input type="checkbox"/> Present	B.S. Engineering	06/1976
U.A. Air Force Pilot Training	Military pilot training (primary and secondary jet)	08/1977	07/1978	Pilot	07/1978
Columbia University	University	08/1976 <input type="checkbox"/> Est	05/1977 <input type="checkbox"/> Est <input type="checkbox"/> Present	M.S. Engineering	05/1977
Johns Hopkins University	University	09/1982 <input type="checkbox"/> Est	05/1984 <input type="checkbox"/> Est <input type="checkbox"/> Present	M.S. Computer Science	05/1984
George Washington University	University	09/1986 <input type="checkbox"/> Est	05/1990 <input type="checkbox"/> Est <input type="checkbox"/> Present	Professional Degree Comp Science	05/1990

3. Employment

(A) List all of your employment activities, including unemployment and self-employment. If the employment activity was military duty, list separate employment activity periods to show each change of military duty station. Do not list employment before your 18th birthday unless to provide a minimum of two years of employment history.

<u>Type of Employment</u> (Active Military Duty Station, National Guard/Reserve, USPHS Commissioned Corps, Other Federal employment, State Government (Non- Federal Employment), Self- employment, Unemployment, Federal Contractor, Non- Government Employment (excluding self-employment), Other	<u>Name of Your Employer/ Assigned Duty Station</u>	<u>Most Recent Position Title/Rank</u>	<u>Location</u> (City and State only)	<u>Date Employment Began</u> (month/year) (check box if estimate)	<u>Date Employment Ended</u> (month/year) (check box if estimate) (check "present" box if still employed)
Active duty U.S. Military	U.S. Air Force Academy	Cadet	Colorado Springs, CO	07/1972 <input type="checkbox"/> Est	06/1976 <input type="checkbox"/> Est
Active duty U.S. Military	U.S. Air Force Columbia University	2 Lieutenant	NY, NY	06/1976 <input type="checkbox"/> Est	05/1977 <input type="checkbox"/> Est
Active duty U.S. Military	U.S. Air Force Hondo AFB, TX	2 Lieutenant	San Antonio, TX	06/1977 <input type="checkbox"/> Est	08/1977 <input type="checkbox"/> Est
Active duty U.S. Military	U.S. Air Force Williams AFB, AZ	1 Lieutenant	Chandler AZ	08/1977 <input type="checkbox"/> Est	10/1979 <input type="checkbox"/> Est
Active duty U.S. Military	U.S. Air Force Altus AFB	1 Lieutenant	Chandler AZ	10/1979 <input type="checkbox"/> Est	12/1979 <input type="checkbox"/> Est
Active duty U.S. Military	U.S. Air Force McGuire AFB	Captain	Mt Holly NJ	01/1980 <input type="checkbox"/> Est	05/1982 <input type="checkbox"/> Est
Active duty U.S. Military	U.S. Air Force U.S. Naval Academy	Captain	Annapolis MD	05/1982 <input type="checkbox"/> Est	07/1985 <input type="checkbox"/> Est
Traditional (part-time) Guardsmen	Air National Guard MD ANG	Brigadier General	Baltimore MD	07/1985 <input type="checkbox"/> Est	08/2006 <input type="checkbox"/> Est
National Security Agency Civilian Employee	National Security Agency Ft Meade MD	GG-14	Ft Meade MD	01/1986 <input type="checkbox"/> Est	07/1991 <input type="checkbox"/> Est
National Security Agency Civilian Employee	National Security Agency U.S. Military Academy	GG-14	West Point NY	07/1991 <input type="checkbox"/> Est	06/1992 <input type="checkbox"/> Est

National Security Agency Civilian Employee	National Security Agency Ft Meade MD	Senior Executive Service LVL 3	Ft Meade MD	06/1992 <input type="checkbox"/> Est	07/2003 <input type="checkbox"/> Est
National Security Agency Civilian Employee	National Security Agency U.S. Embassy London	Senior Executive Service LVL 3	London UK	07/2003 <input type="checkbox"/> Est	08/2006 <input type="checkbox"/> Est
National Security Agency Civilian Employee	National Security Agency Ft Meade MD	Senior Executive Service LVL 6	Ft Meade MD	08/2006 <input type="checkbox"/> Est	01/2014 <input type="checkbox"/> Est
Retiree (from U.S. Air Force and NSA) and Consultant	Self	N/A	Annapolis MD	01/2014 <input type="checkbox"/> Est	Present <input type="checkbox"/> Est
Visiting Professor U.S. Naval Academy	U.S. Naval Academy Cyber Department	Visiting Professor	Annapolis MD	07/2014 <input type="checkbox"/> Est	07/2016 <input type="checkbox"/> Est
Visiting Professor U.S. Naval Academy	Avance IT Systems U.S. Naval Academy Cyber Department	Visiting Professor	Annapolis MD	07/2016 <input type="checkbox"/> Est	Present <input type="checkbox"/> Est

(B) List any advisory, consultative, honorary or other part-time service or positions with federal, state, or local governments, not listed elsewhere.

<u>Name of Government Entity</u>	<u>Name of Position</u>	<u>Date Service Began</u> (month/year) (check box if estimate)	<u>Date Service Ended</u> (month/year) (check box if estimate) (check "present" box if still serving)
U.S. DoD Defense Science Board	Participant (2015-2019); Member 02/2019-02-2021	07/2015 <input type="checkbox"/> Est	02/2021 <input type="checkbox"/> Est <input type="checkbox"/> Present
U.S. National Intelligence University	Trustee	07/2017 <input type="checkbox"/> Est	02/2021 <input type="checkbox"/> Est <input type="checkbox"/> Present
U.S. Director of National Intelligence	Member Strategic Advisory Board	12/2014 <input type="checkbox"/> Est	02/2020 <input type="checkbox"/> Est <input type="checkbox"/> Present
U.S. Strategic Command	Member Strategic Advisory Board and Chair of USSTRATCOM SAG Intelligence Panel	05/2014	09/2020
U.S. Cyberspace Solarium Commission	Commissioner	02/2019	Present

4. Potential Conflict of Interest

(A) Describe any business relationship, dealing or financial transaction which you have had during the last 10 years, whether for yourself, on behalf of a client, or acting as an agent, that could in any way constitute or result in a possible conflict of interest in the position to which you have been nominated.

None.

(B) Describe any activity during the past 10 years in which you have engaged for the purpose of directly or indirectly influencing the passage, defeat or modification of any legislation or affecting the administration or execution of law or public policy, other than while in a federal government capacity.

As a Commissioner on the U.S. Cyberspace Solarium Commission I testified before the Senate and advocated for congressional support of the recommendations included in the March 2020 U.S. Cyber Solarium Report.

5. Honors and Awards

List all scholarships, fellowships, honorary degrees, civilian service citations, military medals, academic or professional honors, honorary society memberships and any other special recognition for outstanding service or achievement.

- 1976 Outstanding US Air Force Academy Cadet in Engineering Mechanics
- 1976 U.S. Air Force Academy Distinguished Graduate upon graduation (order of merit 31 of 930)
- 1978 Distinguished Graduate U.S. Air Force Pilot Training, Class 78-07 & Top Stick T37 Primary Jet Phase (Williams AFB)
- 1984 Clement's Award as the Outstanding Military Faculty Member for 1983-1984, U.S. Naval Academy
- 1992 Department of Army Outstanding Civilian Service Award
- 2000 Presidential Rank Award for Meritorious Service
- 2002 NSA Exceptional Civilian Service Award
- 2004 Presidential Rank Award for Distinguished Service
- 2009 Presidential Rank Award for Distinguished Service
- 2009 Boy Scouts of America, Distinguished Eagle Scout
- 2014 Director of National Intelligence Distinguished Service Medal
- 2014 The President's National Security Medal
- 2019 US Air Force Academy Distinguished Graduate Award
- 1976 – 2006 Military awards include the Air Force Distinguished Service Medal, Legion of Merit, Navy Commendation Medal, and Air Force Commendation Medal

6. Memberships

List all memberships that you have held in professional, social, business, fraternal, scholarly, civic, or charitable organizations in the last 10 years.

Unless relevant to your nomination, you do NOT need to include memberships in charitable organizations available to the public as a result of a tax deductible donation of \$1,000 or less, Parent-Teacher Associations or other organizations connected to schools attended by your children, athletic clubs or teams, automobile support organizations (such as AAA), discounts clubs (such as Groupon or Sam's Club), or affinity memberships/consumer clubs (such as frequent flyer memberships).

<u>Name of Organization</u>	<u>Dates of Your Membership</u> (You may approximate.)	<u>Position(s) Held</u>
National Cryptologic Museum Foundation	July 2014 – Present	Board member
Air Force Academy Falcon Foundation	July 2019 - present	Trustee
Boy Scouts of America, Baltimore Area Council	July 2016 – July 2019	Member Advisory Board
U.S. Air Force Academy Alumni Association	June 1976 - present	Member
U.S. Naval Academy Alumni Association	July 1985 - present	Member
Royal Air Force Club, London UK	July 2004 – present	Member
Cambridge Security Institute; Cambridge University, UK	July 2019 - present	Member Academic Steering Committee for summer programs (supporting U.S. Naval Academy student participation in the summer program)

7. Political Activity

(A) Have you ever been a candidate for or been elected or appointed to a political office?

<u>Name of Office</u>	<u>Elected/Appointed/ Candidate Only</u>	<u>Year(s) Election Held or Appointment Made</u>	<u>Term of Service (if applicable)</u>
None			

(B) List any offices held in or services rendered to a political party or election committee during the last ten years that you have not listed elsewhere.

<u>Name of Party/Election Committee</u>	<u>Office/Services Rendered</u>	<u>Responsibilities</u>	<u>Dates of Service</u>
Biden-Harris Campaign	Member intelligence policy working group	Co-Chair development of intelligence priorities and actions for a prospective Biden administration	08/2020 – 11/2020

(C) Itemize all individual political contributions of \$200 or more that you have made in the past five years to any individual, campaign organization, political party, political action committee, or similar entity. Please list each individual contribution and not the total amount contributed to the person or entity during the year.

<u>Name of Recipient</u>	<u>Amount</u>	<u>Year of Contribution</u>
Biden – Harris 2020 Campaign	\$2800	2020
No others.		

8. Publications and Speeches

(A) List the titles, publishers and dates of books, articles, reports or other published materials that you have written, including articles published on the Internet. Please provide the Committee with copies of all listed publications. In lieu of hard copies, electronic copies can be provided via e-mail or other digital format.

To the best of my abilities, I have taken steps to recall and report all articles, reports and other published materials I have written for the specified period of time. If additional materials are identified, those materials will be reported promptly to the Committee.

<u>Title</u>	<u>Publisher</u>	<u>Date(s) of Publication</u>
"Illuminating a New Domain: The Role and Nature of Military Intelligence, Surveillance and Reconnaissance in Cyberspace"	Stanford Cyber Policy Program https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2836092	2016
"Cyberspace—Making Some Sense of It All"	Journal of Information Warfare Vol. 15, No. 2 (2016), pp. 17-26	2016
"The NSA's Smart Play to Install a Greater Margin of Safety"	CipherBrief https://www.thecipherbrief.com/the-nsas-smart-play-to-install-a-greater-margin-of-safety-2	7 May 2017
"U.S. Cyber Survival Depends on Greater Collaboration"	CipherBrief https://www.thecipherbrief.com/column/expert-view/u-s-cyber-survival-depends-on-greater-collaboration	21 June 2017
"The Global Commons is a Great Good"	CipherBrief https://www.thecipherbrief.com/global-commons-great-good	6 September 2017
"Hacking the Human Element of Code"	CipherBrief https://www.thecipherbrief.com/hacking-not-code-humans	8 October 2017
"Remembering Civil Liberties when Reforming Foreign Surveillance"	CipherBrief https://www.thecipherbrief.com/column/cyber-advisor/remembering-civil-liberties-reforming-foreign-surveillance	5 November 2017
Book Review by John C. Inglis on <i>The Darkening Web: The War for Cyberspace</i> , by Alexander Klimburg	Naval Institute Press	Spring 2018

“Cyber as Strategic Capability”, Executive Summary of a Study by the Defense Science Board, Chaired by Chris Inglis and James Gosler	Defense Science Board	March 2018
“Government cybersecurity commission calls for international cooperation, resilience and retaliation “ A Conversation with Chris Inglis	<u>The Conversation (Wordisk)</u> https://worddisk.com/reading-v2/article/104529/	12 May 2020
“Creating a more secure nation means public service hiring practices need an overhaul” Joe Heck and John C. "Chris" Inglis	The Hill https://thehill.com/blogs/congress-blog/politics/507954-creating-a-more-secure-nation-means-public-service-hiring	18 July 2020
“Improving Cyber-Oriented Education, One Cyber Clinic at a Time”, with Tatyana Bolton	Lawfare https://www.lawfareblog.com/improving-cyber-oriented-education-one-cyber-clinic-time	13 August 2020
“Shining a Light on Cyber”, an Interview with Chris Inglis	U.S. Air Force Strategic Studies Quarterly	Fall 2020
“Differentiating Kinetic and Cyber Weapons to Improve Integrated Combat” with Josiah Dykstra and Thomas S. Walcott	DoD Joint Force Quarterly, Issue 99, 4 th Quarter 2020	Fall 2020
Previewing Solarium recommendations John Carlin podcast with Chris Inglis	Podcast available on Facebook: https://www.facebook.com/CAFE/videos/755747568325364	11 September 2020
Interview on cyber strategy and policy with Chris Inglis, former Deputy Director NSA and Ciaran Martin, former	Cipher Brief https://www.youtube.com/watch?v=xjIEQNICpyA	13 April 2021

Director National Cyber Security Centre		
“Chinese Technology Platforms Operating in the United States - Assessing the National Security Threat” Joint Report of the National Security, Technology, and Law Working Group at the Hoover Institution at Stanford University and Tech, Law & Security Program at American University Washington College of Law Gary Corn, Jennifer Daskal, Jack Goldsmith, Chris Inglis, Paul Rosenzweig, Sam Sacks, Bruce Schneier, Alex Stamos and Vincent Stewart	Hoover Institution https://www.hoover.org/research/chinese-technology-platforms-operating-united-states	11 February 2021

(B) List any formal speeches you have delivered during the last five years and provide the Committee with copies of those speeches relevant to the position for which you have been nominated. Include any testimony to Congress or any other legislative or administrative body. These items can be provided electronically via e-mail or other digital format.

To the best of my abilities, I have taken steps to recall and report the formal speaking engagements I participated in for the specified period of time. On many occasions, I provided informal remarks, participated in panel discussions or otherwise spoke without written notes prepared in advance. If additional materials are identified, those materials will be reported promptly to the Committee.

<u>Title/Topic</u>	<u>Place/Audience</u>	<u>Date(s) of Speech</u>
Keynote: “The reality of cyber space, threats and what to do about it”	Accenture and Oracle Executive Event https://www.youtube.com/watch?v=elgm_Gc8SkQ	18 May 2016
“Cyber and encryption issues with a specific focus on the	Senate Committee on Armed Services	14 July 2016

challenges to law enforcement caused by encryption”		
“Cyber Enabled Information Operations”	Senate Committee on Armed Services	27 April 2017
Cybersecurity keynote – “Addressing Insider Threat”	7 th Annual Israeli International Security Conference University of Tel Aviv https://www.youtube.com/watch?v=atKR9E7WmI	6 July 2017
Speech to the Baltimore Council on Foreign Affairs “Security in the Age of Cyber and Great Power Competition”	Baltimore World Trade Center https://www.youtube.com/watch?v=01F8Qm93oIg	24 September 2019
“Recommendations of the Cyberspace Solarium Commission”	Subcommittee on Cybersecurity of the Senate Committee on Armed Services	4 August 2020

(C) List all speeches and testimony you have delivered in the past ten years, except for those the text of which you are providing to the Committee.

<u>Title</u>	<u>Place/Audience</u>	<u>Date(s) of Speech</u>
“Disclosure of National Security Agency Surveillance Programs”	House Select Intelligence Committee	18 June 2013
“The Administration’s Use of FISA Authorities”	House Judiciary Committee	17 July 2013
“Strengthening Privacy Rights and National Security: Oversight of FISA Surveillance Programs”	Senate Judiciary Committee	31 July 2013
“On the Very Idea of Secret Laws” – University of Pennsylvania Carey Law School, Keynote by John “Chris” Inglis	https://www.youtube.com/watch?v=gcGnyG74Obo	22 November 2013
60 Minutes Special on the Snowden Leaks, (transcript including remarks by Chris Inglis)	https://cryptome.org/2013/12/nsa-60mins/nsa-60mins.htm	December 2013

Brookings Institute Panel, "Did NSA Oversight Work Well?"	https://www.youtube.com/watch?v=h_ihYHQZ3Fo	6 June 2014
"On the Strategy of Combating Cyber Threats", Interview with Chris Inglis	https://www.bankinfosecurity.com/conversation-chris-inglis-strategy-a-8640	28 October 2015
Securionix interview with Chris Inglis on the State of Cybersecurity	https://www.youtube.com/watch?v=-PLtEapnTE4	January 2020 (posted 4 May 2010)
The Cyberspace Solarium Commission: "The International Impact" (Panel discussion including Chris Inglis)	https://carnegieendowment.org/2020/03/04/cyberspace-solarium-commission-international-impact-event-7293	4 March 2020
Previewing Solarium recommendations John Carlin podcast with Chris Inglis	Podcast available on Facebook: https://www.facebook.com/CAFE/videos/755747568325364	11 September 2020
60 Minutes special on Solarwinds	https://www.cbsnews.com/news/solarwinds-hack-russia-cyberattack-60-minutes-2021-02-14/	February 2021
Interview on cyber strategy and policy with Chris Inglis, former Deputy Director NSA and Ciaran Martin, former Director National Cyber Security Centre	Cipher Brief https://www.youtube.com/watch?v=xjIEQNlCpyA	13 April 2021

9. Criminal History

Since (and including) your 18th birthday, has any of the following happened?

- Have you been issued a summons, citation, or ticket to appear in court in a criminal proceeding against you? (Exclude citations involving traffic infractions where the fine was less than \$300 and did not include alcohol or drugs.) **No**
- Have you been arrested by any police officer, sheriff, marshal or any other type of law enforcement official? **No**
- Have you been charged, convicted, or sentenced of a crime in any court? **No**
- Have you been or are you currently on probation or parole? **No**

- Are you currently on trial or awaiting a trial on criminal charges? **No**
- To your knowledge, have you ever been the subject or target of a federal, state or local criminal investigation?
No

If the answer to any of the questions above is yes, please answer the questions below for each criminal event (citation, arrest, investigation, etc.). If the event was an investigation, where the question below asks for information about the offense, please offer information about the offense under investigation (if known).

This section not applicable

- A) Date of offense:
- a. Is this an estimate (Yes/No):
- B) Description of the specific nature of the offense:
- C) Did the offense involve any of the following?
- 1) Domestic violence or a crime of violence (such as battery or assault) against your child, dependent, cohabitant, spouse, former spouse, or someone with whom you share a child in common: **Yes / No**
 - 2) Firearms or explosives: **Yes / No**
 - 3) Alcohol or drugs: **Yes / No**
- D) Location where the offense occurred (city, county, state, zip code, country):
- E) Were you arrested, summoned, cited or did you receive a ticket to appear as a result of this offense by any police officer, sheriff, marshal or any other type of law enforcement official: **Yes / No**
- 1) Name of the law enforcement agency that arrested/cited/summoned you:
 - 2) Location of the law enforcement agency (city, county, state, zip code, country):
- F) As a result of this offense were you charged, convicted, currently awaiting trial, and/or ordered to appear in court in a criminal proceeding against you: **Yes / No**
- 1) If yes, provide the name of the court and the location of the court (city, county, state, zip code, country):
 - 2) If yes, provide all the charges brought against you for this offense, and the outcome of each charged offense (such as found guilty, found not-guilty, charge dropped or "nolle pros," etc). If you were found guilty of or pleaded guilty to a lesser offense, list separately both the original charge and the lesser offense:
 - 3) If no, provide explanation:
- G) Were you sentenced as a result of this offense: **Yes / No**
- H) Provide a description of the sentence:

- I) Were you sentenced to imprisonment for a term exceeding one year: **Yes / No**
- J) Were you incarcerated as a result of that sentence for not less than one year: **Yes / No**
- K) If the conviction resulted in imprisonment, provide the dates that you actually were incarcerated:
- L) If conviction resulted in probation or parole, provide the dates of probation or parole:
- M) Are you currently on trial, awaiting a trial, or awaiting sentencing on criminal charges for this offense: **Yes / No**
- N) Provide explanation:

10. Civil Litigation and Administrative or Legislative Proceedings

(A) Since (and including) your 18th birthday, have you been a party to any public record civil court action or administrative or legislative proceeding of any kind that resulted in (1) a finding of wrongdoing against you, or (2) a settlement agreement for you, or some other person or entity, to make a payment to settle allegations against you, or for you to take, or refrain from taking, some action. Do NOT include small claims proceedings.

<u>Date Claim/Suit Was Filed or Legislative Proceedings Began</u>	<u>Court Name</u>	<u>Name(s) of Principal Parties Involved in Action/Proceeding</u>	<u>Nature of Action/Proceeding</u>	<u>Results of Action/Proceeding</u>
None				

(B) In addition to those listed above, have you or any business of which you were an officer, director or owner ever been involved as a party of interest in any administrative agency proceeding or civil litigation? Please identify and provide details for any proceedings or civil litigation that involve actions taken or omitted by you, or alleged to have been taken or omitted by you, while serving in your official capacity.

<u>Date Claim/Suit Was Filed</u>	<u>Court Name</u>	<u>Name(s) of Principal Parties Involved in Action/Proceeding</u>	<u>Nature of Action/Proceeding</u>	<u>Results of Action/Proceeding</u>
None				

(C) For responses to the previous question, please identify and provide details for any proceedings or civil litigation that involve actions taken or omitted by you, or alleged to have been taken or omitted by you, while serving in your official capacity.

11. Breach of Professional Ethics

(A) Have you ever been disciplined 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? Exclude cases and proceedings already listed.

<u>Name of Agency/Association/ Committee/Group</u>	<u>Date Citation/Disciplinary Action/Complaint Issued/Initiated</u>	<u>Describe Citation/Disciplinary Action/Complaint</u>	<u>Results of Disciplinary Action/Complaint</u>
None			

(B) Have you ever been fired from a job, quit a job after being told you would be fired, left a job by mutual agreement following charges or allegations of misconduct, left a job by mutual agreement following notice of unsatisfactory performance, or received a written warning, been officially reprimanded, suspended, or disciplined for misconduct in the workplace, such as violation of a security policy?

12. Tax Compliance

(This information will not be published in the record of the hearing on your nomination, but it will be retained in the Committee's files and will be available for public inspection.)

REDACTED

REDACTED

13. Lobbying

In the past ten years, have you registered as a lobbyist? If so, please indicate the state, federal, or local bodies with which you have registered (e.g., House, Senate, California Secretary of State).

No.

14. Outside Positions

X See OGE Form 278. (If, for your nomination, you have completed an OGE Form 278 Executive Branch Personnel Public Financial Disclosure Report, you may check the box here to complete this section and then proceed to the next section.)

For the preceding ten calendar years and the current calendar year, report any positions held, whether compensated or not. Positions include but are not limited to those of an officer, director, trustee, general partner, proprietor, representative, employee, or consultant of any corporation, firm, partnership, or other business enterprise or any non-profit organization or educational institution. Exclude positions with religious, social, fraternal, or political entities and those solely of an honorary nature.

<u>Name of Organization</u>	<u>Address of Organization</u>	<u>Type of Organization</u> (corporation, firm, partnership, other business enterprise, other non-profit organization, educational institution)	<u>Position Held</u>	<u>Position Held From</u> (month/year)	<u>Position Held To</u> (month/year)
See OGE 278					

15. Agreements or Arrangements

X See OGE Form 278. (If, for your nomination, you have completed an OGE Form 278 Executive Branch Personnel Public Financial Disclosure Report, you may check the box here to complete this section and then proceed to the next section.)

As of the date of filing your OGE Form 278, report your agreements or arrangements for: (1) continuing participation in an employee benefit plan (e.g. pension, 401k, deferred compensation); (2) continuation of payment by a former employer (including severance payments); (3) leaves of absence; and (4) future employment.

Provide information regarding any agreements or arrangements you have concerning (1) future employment; (2) a leave of absence during your period of Government service; (3) continuation of payments by a former employer other than the United States Government; and (4) continuing participation in an employee welfare or benefit plan maintained by a former employer other than United States Government retirement benefits.

<u>Status and Terms of Any Agreement or Arrangement</u>	<u>Parties</u>	<u>Date</u> (month/year)
See OGE 278		

16. Additional Financial Data

All information requested under this heading must be provided for yourself, your spouse, and your dependents. (This information will not be published in the record of the hearing on your nomination, but it will be retained in the Committee's files and will be available for public inspection.)

REDACTED

REDACTED

SIGNATURE AND DATE

I hereby state that I have read the foregoing Statement on Biographical and Financial Information and that the information provided therein is, to the best of my knowledge, current, accurate, and complete.


John C. ("Chris") Inglis

This 28th day of April, 2021

REDACTED

UNITED STATES OFFICE OF
GOVERNMENT ETHICS

May 26, 2021

The Honorable Gary C. Peters
Chairman
Committee on Homeland Security
and Governmental Affairs
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

In accordance with the Ethics in Government Act of 1978, I enclose a copy of the financial disclosure report filed by John C. Inglis, who has been nominated by President Biden for the position of National Cyber Director, Office of the National Cyber Director.

We have reviewed the report and have obtained advice from the agency concerning any possible conflict in light of its functions and the nominee's proposed duties. Also enclosed is an ethics agreement outlining the actions that the nominee will undertake to avoid conflicts of interest. Unless a date for compliance is indicated in the ethics agreement, the nominee must fully comply within three months of confirmation with any action specified in the ethics agreement.

Based thereon, we believe that this nominee is in compliance with applicable laws and regulations governing conflicts of interest.

Sincerely,

DAVID APOL

Digitally signed by DAVID
APOL
Date: 2021.05.26 11:46:06
-04'00'

David J. Apol
General Counsel

Enclosures REDACTED



21 May 2021

Ms. Dana Remus
Designated Agency Ethics Official
White House, West Wing
1600 Pennsylvania Avenue, NW
Washington, DC 20500

Dear Ms. Remus:

The purpose of this letter is to describe the steps that I will take to avoid any actual or apparent conflict of interest in the event that I am confirmed for the position of National Cyber Director, Office of the National Cyber Director. It is my responsibility to understand and comply with commitments outlined in this agreement.

SECTION 1 – GENERAL COMMITMENTS

As required by the criminal conflicts of interest law at 18 U.S.C. § 208(a), I will not participate personally and substantially in any particular matter in which I know that I have a financial interest directly and predictably affected by the matter, or in which I know that a person whose interests are imputed to me has a financial interest directly and predictably affected by the particular matter, unless I first obtain a written waiver, pursuant to 18 U.S.C. § 208(b)(1), or qualify for a regulatory exemption, pursuant to 18 U.S.C. § 208(b)(2). I understand that the interests of the following persons are imputed to me:

- Any spouse or minor child of mine;
- Any general partner of a partnership in which I am a limited or general partner;
- Any organization in which I serve as an officer, director, trustee, general partner, or employee; and
- Any person or organization with which I am negotiating or have an arrangement concerning prospective employment.

In the event that an actual or potential conflict of interest arises during my appointment, I will consult with an agency ethics official and take the measures necessary to resolve the conflict, such as recusal from the particular matter or divestiture of an asset.

If I have a managed account or otherwise use the services of an investment professional during my appointment, I will ensure that the account manager or investment professional obtains my prior approval on a case-by-case basis for the purchase of any assets other than cash, cash equivalents, investment funds that qualify for the regulatory exemption for diversified mutual funds and unit investment trusts at 5 C.F.R. § 2640.201(a), obligations of the United States, or municipal bonds.

I will receive a live ethics briefing from a member of the ethics office after my confirmation but not later than 15 days after my appointment pursuant to the ethics program regulation at 5 C.F.R. § 2638.305. Within 90 days of my confirmation, I will submit my

Certification of Ethics Agreement Compliance which documents my compliance with this ethics agreement.

I understand that as an appointee I will be required to sign the Ethics Pledge (Exec. Order No. 13989) and that I will be bound by it. Among other obligations, I will be required to recuse from particular matters involving specific parties involving my former employer or former clients for a period of two years after I am appointed, with the exception of federal, state and local government.

I will not modify this ethics agreement without your approval and the approval of the U.S. Office of Government Ethics pursuant to the ethics agreement requirements contained in the financial disclosure regulation at 5 C.F.R. § 2634.803(a)(4).

SECTION 2 – INGLIS A&C, LLC

I own Inglis A&C, LLC, a pass-through entity established to receive compensation for consulting activities and for services as a corporate director and advisor. During my appointment to the position of National Cyber Director, Inglis A&C, LLC, will remain dormant and will not advertise. I will not perform any services for the entity, except that I will comply with any requirements involving legal filings, taxes and fees that are necessary to maintain the entity while it is in an inactive status. All amounts owed to me by any clients, including those identified in sections 3 and 4 below, will be fixed before I assume the duties of the position of National Cyber Director, and I will not participate personally and substantially in any particular matter that to my knowledge has a direct and predictable effect on the ability or willingness of any of these clients to pay these amounts. During my appointment to the position of National Cyber Director, I will not participate personally and substantially in any particular matter that to my knowledge has a direct and predictable effect on the financial interests of Inglis A&C, LLC.

SECTION 3 – CLIENTS OF INGLIS A&C, LLC IN WHICH I HAVE EQUITY OR AN AGREEMENT FOR EQUITY

Upon my confirmation, I will resign my position with BlackPoint Cyber. I receive cash director fees and hold vested stock options. I do not hold any other equity in this entity. I will divest my vested stock options in BlackPoint Cyber as soon as practicable but not later than 90 days after my confirmation. If I divest the stock options by exercising them, I will divest the resulting stock as soon as practicable but not later than 90 days after my confirmation. I will not participate personally and substantially in any particular matter that to my knowledge has a direct and predictable effect on the financial interests of this entity until I have divested it, unless I first obtain a written waiver, pursuant to 18 U.S.C. § 208(b)(1), or qualify for a regulatory exemption, pursuant to 18 U.S.C. § 208(b)(2). I have verified that I will be able to carry out this divestiture within the timeframe described above. Pursuant to the impartiality regulation at 5 C.F.R.

2635.502, for a period of one year after my resignation, I also will not participate personally and substantially in any particular matter involving specific parties in which I know BlackPoint Cyber, is a party or represents a party, unless I am first authorized to participate, pursuant to 5 C.F.R. § 2635.502(d).

Upon my confirmation, I will resign my position with FedEx Corp. I receive cash director fees. I also hold common shares of stock and both vested and unvested stock options. I do not hold any other equity in this entity. I will forfeit any unvested stock options at resignation. I will divest my stock and vested stock options in FedEx Corp. as soon as practicable but not later than 90 days after my confirmation. If I divest the stock options by exercising them, I will divest the resulting stock as soon as practicable but not later than 90 days after my confirmation. I will not participate personally and substantially in any particular matter that to my knowledge has a direct and predictable effect on the financial interests of this entity until I have divested it, unless I first obtain a written waiver, pursuant to 18 U.S.C. § 208(b)(1), or qualify for a regulatory exemption, pursuant to 18 U.S.C. § 208(b)(2). I have verified that I will be able to carry out this divestiture within the timeframe described above. Pursuant to the impartiality regulation at 5 C.F.R. § 2635.502, for a period of one year after my resignation, I also will not participate personally and substantially in any particular matter involving specific parties in which I know FedEx Corp. is a party or represents a party, unless I am first authorized to participate, pursuant to 5 C.F.R. § 2635.502(d).

Upon my confirmation, I will resign my position with HawkEye 360. I do not receive cash compensation but hold both vested and unvested stock options. I do not hold any other equity in this entity. I will forfeit any unvested stock options at resignation. I will divest my vested stock options in HawkEye 360 as soon as practicable but not later than 90 days after my confirmation. If I divest the stock options by exercising them, I will divest the resulting stock as soon as practicable but not later than 90 days after my confirmation. I will not participate personally and substantially in any particular matter that to my knowledge has a direct and predictable effect on the financial interests of this entity until I have divested it, unless I first obtain a written waiver, pursuant to 18 U.S.C. § 208(b)(1), or qualify for a regulatory exemption, pursuant to 18 U.S.C. § 208(b)(2). I have verified that I will be able to carry out this divestiture within the timeframe described above. Pursuant to the impartiality regulation at 5 C.F.R. § 2635.502, for a period of one year after my resignation, I also will not participate personally and substantially in any particular matter involving specific parties in which I know HawkEye 360 is a party or represents a party, unless I am first authorized to participate, pursuant to 5 C.F.R. § 2635.502(d).

Upon my confirmation, I will resign my position with Huntington Bancshares. I receive cash director fees. I also hold common shares of stock and vested deferred stock units. I do not hold any other equity in this entity. My vested deferred stock units will be distributed to me in 5 annual installments, starting within 6 months my resignation. I have been advised that the duties of the position of National Cyber Director may involve particular matters affecting the financial interests of Huntington Bancshares. The Office of White House Counsel has determined that it is not necessary at this time for me to divest my interests in Huntington Bancshares because my recusal from particular matters in which these interests pose a conflict of interest will not substantially limit my ability to perform the essential duties of the position of National Cyber Director. Accordingly, for as long as I hold stock or deferred stock units in Huntington Bancshares, I will not participate personally and substantially in any particular matter that to my knowledge has a direct and predictable effect on the financial interests of Huntington

Bancshares, unless I first obtain a written waiver, pursuant to 18 U.S.C. § 208(b)(1), or qualify for a regulatory exemption, pursuant to 18 U.S.C. § 208(b)(2).

Upon my confirmation, I will resign my position with Securonix. I receive cash director fees and hold vested stock options. I do not hold any other equity in this entity. I will divest my vested stock options in Securonix as soon as practicable but not later than 90 days after my confirmation. If I divest the stock options by exercising them, I will divest the resulting stock as soon as practicable but not later than 90 days after my confirmation. I will not participate personally and substantially in any particular matter that to my knowledge has a direct and predictable effect on the financial interests of this entity until I have divested it, unless I first obtain a written waiver, pursuant to 18 U.S.C. § 208(b)(1), or qualify for a regulatory exemption, pursuant to 18 U.S.C. § 208(b)(2). I have verified that I will be able to carry out this divestiture within the timeframe described above. Pursuant to the impartiality regulation at 5 C.F.R. § 2635.502, for a period of one year after my resignation, I also will not participate personally and substantially in any particular matter involving specific parties in which I know Securonix is a party or represents a party, unless I am first authorized to participate, pursuant to 5 C.F.R. § 2635.502(d).

Upon my confirmation, I will resign my position with Vequity, Inc., dba Range Force. I do not receive cash compensation but hold both vested and unvested stock options. I do not hold any other equity in this entity. I will forfeit any unvested stock options at resignation. I will divest my vested stock options in Vequity, Inc., as soon as practicable but not later than 90 days after my confirmation. I intend to accomplish this divestiture by directing Vequity, Inc., to transfer the unexercised options to Paladin Capital Group, which will pay me the fair value of these unexercised options, less the exercise price. I will not participate personally and substantially in any particular matter that to my knowledge has a direct and predictable effect on the financial interests of Vequity, Inc. until I have received payment from Paladin Capital Group, unless I first obtain a written waiver, pursuant to 18 U.S.C. § 208(b)(1), or qualify for a regulatory exemption, pursuant to 18 U.S.C. § 208(b)(2). I have verified that I will be able to carry out this divestiture within the timeframe described above. Pursuant to the impartiality regulation at 5 C.F.R. § 2635.502, for a period of one year after my resignation, I also will not participate personally and substantially in any particular matter involving specific parties in which I know Vequity, Inc., is a party or represents a party, unless I am first authorized to participate, pursuant to 5 C.F.R. § 2635.502(d).

SECTION 4 – CLIENTS OF INGLIS A&C, LLC IN WHICH I DO NOT HAVE EQUITY OR AN AGREEMENT FOR EQUITY

Upon confirmation, I will resign from my positions with the following entities, if I have not already done so:

- Avance IT Solutions, LLC
- Elbit Systems of America (subsidiary of Elbit Systems, Ltd.)
- ManTech International
- Penn State Advanced Research Laboratory

I previously resigned my position with WestExec Advisors, LLC, in April 2021 and my position with Trinity Cyber, LLC, in May 2021. I do not hold any equity or agreement for equity in any of these entities. Pursuant to the impartiality regulation at 5 C.F.R. § 2635.502, for a period of one year after my resignation from each of these entities, I will not participate personally and substantially in any particular matter involving specific parties in which I know that entity is a party or represents a party, unless I am first authorized to participate, pursuant to 5 C.F.R. § 2635.502(d). In addition, pursuant to the impartiality regulation at 5 C.F.R. § 2635.502, I will not participate personally and substantially in any particular matter involving specific parties in which I know a former client of mine through WestExec Advisors, LLC, is a party or represents a party for a period of one year after I last provided service to that client, unless I am first authorized to participate, pursuant to 5 C.F.R. § 2635.502(d).

SECTION 5 – PALADIN CAPITAL GROUP

Upon confirmation, I will resign from my position with Paladin Capital Group. I receive cash salary, hold equity interests in Paladin Cyber Investors, LP, and Paladin Cyber Investors II, LP, and have carried interest in Paladin Cyber Investors, LP, Paladin Cyber Investors II, LP, and Paladin Investors III, LP. I do not hold any equity in Paladin Capital Group itself or other any Paladin fund. As soon as practicable but not later than 90 days after my confirmation, I will divest my equity and carried interests in the above-referenced Paladin funds back to Paladin Capital Group for prices fixed as of the date of my resignation. Until I receive payment for these interests, I will not participate personally and substantially in any particular matter that to my knowledge has a direct and predictable effect on the ability or willingness of Paladin Capital Group to make the payment, unless I first obtain a written waiver, pursuant to 18 U.S.C. § 208(b)(1). I have verified that I will be able to carry out the divestitures within the timeframe described above. Pursuant to the impartiality regulation at 5 C.F.R. § 2635.502, for a period of one year after my resignation, I will not participate personally and substantially in any particular matter involving specific parties in which I know that Paladin Capital Group is a party or represents a party, unless I am first authorized to participate, pursuant to 5 C.F.R. § 2635.502(d).

SECTION 6 – OTHER POSITIONS AND DIVESTITURES

Upon confirmation, I will resign from my position with the National Cryptologic Museum Foundation. Pursuant to the impartiality regulation at 5 C.F.R. § 2635.502, for a period of one year after my resignation from this entity, I will not participate personally and substantially in any particular matter involving specific parties in which I know the National Cryptologic Museum Foundation is a party or represents a party, unless I am first authorized to participate, pursuant to 5 C.F.R. § 2635.502(d).

As soon as practicable but not later than 90 days after my confirmation, I will divest my interests in the following entities:

- AT&T Inc.
- Duke Energy
- Enbridge
- Frontier Communications

- Phillips Morris
- Under Armour
- USAA Precious Metals and Minerals Fund
- Vanguard Energy Fund
- Verizon Communications
- Walmart
- Apple

With regard to each of these entities, I will not participate personally and substantially in any particular matter that to my knowledge has a direct and predictable effect on the financial interests of the entity until I have divested it, unless I first obtain a written waiver, pursuant to 18 U.S.C. § 208(b)(1), or qualify for a regulatory exemption, pursuant to 18 U.S.C. § 208(b)(2). I have verified that I will be able to carry out the divestitures within the timeframe described above.

SECTION 7 – CERTIFICATES OF DIVESTITURE AND AGREEMENT NOT TO REPURCHASE

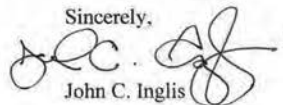
I understand that I may be eligible to request a Certificate of Divestiture for qualifying assets and that a Certificate of Divestiture is effective only if obtained prior to divestiture. Regardless of whether I receive a Certificate of Divestiture, I will ensure that all divestitures discussed in this agreement occur within the agreed upon timeframes and that all proceeds are invested in non-conflicting assets. I understand that I must timely submit my request for a Certificate of Divestiture to allow for adequate time for OGE to process the Certificate of Divestiture, and in order to divest assets within the agreed upon timeframe.

I (including my spouse and dependent children if applicable) will not repurchase any asset I was required to divest without consulting with my agency ethics official and the U.S. Office of Government Ethics.

SECTION 8 – PUBLIC POSTING

I have been advised that this ethics agreement and the Certification of Ethics Agreement Compliance will be posted publicly, consistent with the public information law at 5 U.S.C. § 552, on the website of the U.S. Office of Government Ethics with ethics agreements of other Presidential nominees who file public financial disclosure reports.

Sincerely,



John C. Inglis

**U.S. Senate Committee on Homeland Security and Governmental Affairs
Pre-hearing Questionnaire
For the Nomination of John "Chris" Inglis
to be National Cyber Director**

I. Nomination Process and Conflicts of Interest

1. Did the President or anyone else give you specific reasons why the President nominated you to be the National Cyber Director (NCD), and if so, what were they?

Yes. I have spoken with the National Security Advisors for the President and the Vice President, as well as the Deputy Assistant to the President for National Security Affairs for Cyber and Emerging Technology. All have consistently relayed the President's commitment to significantly improving the coherence, performance, and contributions of the federal cyber enterprise to the security of the Nation and his expectation that I can and, if confirmed, will make a significant contribution to this effort.

2. Were any conditions, expressed or implied, attached to your nomination? If so, please explain.

No.

3. Have you made any commitments with respect to the policies and principles you will attempt to implement as National Cyber Director? If so, what are they, and to whom were the commitments made?

No.

4. Are you aware of any business relationship, dealing, or financial transaction that could result in a possible conflict of interest for you or the appearance of a conflict of interest? If so, please explain what procedures you will use to recuse yourself or otherwise address the conflict. And if you will recuse yourself, explain how you will ensure your responsibilities are not affected by your recusal.

In connection with the nomination process, I have consulted with the ethics office of the White House to identify any potential conflicts of interest. Any potential conflicts were resolved in accordance with the terms of an ethics agreement that I signed and transmitted to the White House Designated Agency Ethics Official, and which was subsequently provided to this Committee. I am not aware of any other potential conflicts of interest.

If there is a reason for me to recuse myself from any matter before the Office of the National Cyber Director, I will follow the guidance of the White House Designated Agency Ethics Official within the Executive Office of the President and, consistent with that guidance, defer the matter to the appropriate official.

5. Please provide the name of any individual, law firm, consulting firm, lobbying firm, public relations firm, or other entity you have formally retained, contracted, or consulted with regarding this nomination, including any amounts paid in fees or otherwise.

I did not retain or contract with any individual, law firm, consulting firm, lobbying firm, public relations firm, or other entity regarding this nomination.

II. Background of the Nominee

6. What specific background, experience, and attributes qualify you to be the National Cyber Director?

My experience in cyber spans more than thirty-five years, dating back to my initial entry into service at the National Security Agency in January 1986. As detailed in the following bullets, I have held hands-on technical roles as a computer scientist and security analyst; talent development roles as an educator and organizational leader; strategy and policy roles for government, allied and private sector operations; and a variety of leadership and command roles in both the government and the private sector.

A. Experience in Cyber Strategy, Doctrine and Policy:

- *Served as the National Security Agency (NSA) Deputy Director, Chief Operating Officer, and its senior civilian - responsible for overall NSA strategy, policy and operational implementation - from 2006-2014*
- *Participant and contributor to National Security Council (NSC) Deputies Committee (inter-agency) deliberations, 2006-2014*
- *Member Department of Defense Science Board. To include DoD studies in 2017, on Cyber Deterrence; and 2018 Cyber as a Strategic Capability (co-chair) which underpinned the transformation of DoD Cyber Strategy in 2018*
- *Commissioner on the U.S. Cyberspace Solarium Commission, 2019-present, which crafted a comprehensive strategy for U.S. Cyber Strategy*
- *Member U.S. Strategic Command Strategic Advisory Group and Chair of its intelligence panel (with responsibilities for cyber), 2014-2019*

B. Experience as a Strategic Leader:

- *Member Senior Executive Service at NSA from 1997-2014 with leadership assignments in 24/7 time-sensitive operations (1996-1997), global analysis and production (2001-2003), encryption policy (1995-1996), and overall NSA operations and strategy as its Deputy Director (2006-2014)*
- *Senate confirmed U.S. Air Force Brigadier General*
 - *30 + year active and reserve career (1976 – 2006)*
 - *Commanded at squadron, group and joint force headquarters levels*
 - *Command pilot with 25+ years flight experience (T37, T38, C141, C130 B/E/J)*

- Commanded lead unit for introduction of the C-130J to active USAF service (1996-2000)
- Drove the conversion of Maryland Guard traditional communication squadrons to cyber operations units in 2000 – 2001, now a model for total force cyber force development

C. Experience as a cyber educator and leadership in developing cyber talent

- Served as the inaugural U. S. Naval Academy Robert and Mary M. Looker Distinguished Visiting Professor for Cyber Studies, 2014 – present.
 - Helped lead and implement a 4-year curriculum and major in cyber studies that is now the third most popular major of the 26 offered at the Naval Academy – a feat achieved in the first five years of the program.
- Chief of Staff for the 2014-2017 national U.S. effort to define and gain formal approval of a nationally accredited baccalaureate curriculum in Cyber Science (now accredited by the Accreditation Board for Engineering and Technology)
- Member, Cyber Panel of the Aspen Security Institute. Significant contributor to Aspen Institute's 2018 *Principles for Growing and Sustaining the Nation's Cybersecurity Workforce*, a roadmap for cyber education
- Trustee and Board Member of the National Intelligence University, 2015-2020

D. Experience in International Policy and Liaison:

- Engaged senior intelligence leaders of over 30 nations during service as NSA's lead for global intelligence production (2001-2003) and as its Chief Operating Officer (2006-2014)
 - Led U.S. delegations on signals intelligence (SIGINT), information assurance and cyber cooperation to India, Japan, UAE, Afghanistan, Pakistan, Taiwan, Republic of Korea, Germany, UK, France, Israel, Canada, Australia, New Zealand, Singapore, Norway, Sweden, Italy, and Spain
- Special U.S. Liaison to London from 2003-2006 – responsible for all NSA personnel (exceeding 2,000) and operations in and with the UK
- Member U.S. National Academy of Sciences Track 1.5 discussions on cyber policy and strategy with the PRC and Russia, 2015 – present

E. Experience in Cyber Operations:

- NSA Deputy Director and Chief Operating Officer from 2006-2014
- NSA Director for (all) global intelligence production from 2001-2003
- Board member and chair of the technology committees for FedEx and Huntington Bank

F. Experience in Cyber Innovation:

- Member Strategic Advisory Board, and cyber lead, of Penn State University Advanced Research Laboratory, 2014-present

- *Managing Director Paladin Capital, which is the global leader in early stage investments in cyber companies*
- *Director and/or strategic advisor on several cyber startups: Trinity, Securonix, Blackpoint, RangeForce*

G. *Selected Writings:*

- “Cyberspace—Making Some Sense of It All”, *Journal of Information Warfare Vol. 15, No. 2 (2016)*, sole author, pp. 17-26, Peregrine Technical Solutions
- “Illuminating a New Domain: The Role and Nature of Military Intelligence, Surveillance and Reconnaissance in Cyberspace”, sole author, *Stanford Cyber Policy Program*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2836092, 2016
- “Differentiating Kinetic and Cyber Weapons to Improve Integrated Combat”, with Josiah Dykstra and Thomas S. Walcott, *Joint Force Quarterly*, Issue 99, 4th Quarter 2020, pp116-124, 2020
- “Improving Cyber-Oriented Education, One Cyber Clinic at a Time”, with Tatyana Bolton, *Lawfare*, August 13, 2020, <https://www.lawfareblog.com/improving-cyber-oriented-education-one-cyber-clinic-time>
- “Chinese Technology Platforms Operating In The United States”, with multiple authors, 11 February 2021, Hoover Institution, <https://www.hoover.org/research/chinese-technology-platforms-operating-united-states>

H. *Education:*

- *U.S. Air Force Academy, 1976, B.S., Engineering Mechanics*
- *Columbia University (Guggenheim Fellow), 1977, M.S., Mechanical Engineering*
- *Johns Hopkins University, 1984, M.S., Computer Science*
- *George Washington University, 1990, Applied Scientist (Professional Degree), Computer Science*
- *Kellogg Business School in-residence Executive Development Program, 1994*
- *Air War College, USAF Air University, 1996*

I. *Significant Awards:*

- *Clements award as the U.S. Naval Academy's Outstanding Military Faculty member (1984)*
- *Three Presidential Rank Awards (2000, 2004, 2009)*
- *U.S. Air Force Distinguished Service Medal (2006)*
- *Boy Scouts of America Distinguished Eagle Scout Award (2009)*
- *Director of National Intelligence Distinguished Service Medal (2014)*
- *The President's National Security Medal (2014)*
- *U.S. Air Force Academy Distinguished Graduate Award (2019)*

7. How will your experience at the National Security Agency inform your approach to leading the Office of the National Cyber Director (ONCD)? How will the role of NCD differ from your prior roles in the Intelligence Community?

My time at NSA provided significant experience in understanding the security of digital systems and networks, experience that is directly applicable to systems being used across the federal government and private sector. This experience also taught me the importance of considering and addressing technological, human and doctrinal factors in designing and implementing the security of complex systems. NSA also provided valuable experience in leading large complex organizations, working within the executive branch interagency process, and coordinating with allies.

My prospective service as a National Cyber Director would be significantly different than the roles I held within the Intelligence Community in several key ways.

As the National Cyber Director I would:

- *Work closely with the private sector, state, local and tribal organizations to understand, support and collaborate with their cyber security initiatives;*
- *Conduct the majority of my work in unclassified or sensitive but unclassified venues to ensure the NCD is accessible to and supportive of federal civil and non-government cyber needs;*
- *Finally, I would have a significant engagement role with the Congress to ensure the NCD keeps Congress informed of the state of the cybersecurity posture of the United States, the effectiveness of current national cyber policy and strategy, and the status of implementation of such policy and strategy.*

8. Please describe:

- a. Your leadership and management style.

I strive to practice servant leadership, using the power inherent in a leadership role to inspire, enable and empower the work of the people serving in the organization.

I am accountable for the present success of the organization, the welfare of its people, and the future health of both. Believing that culture is the most powerful force an organization can bring to bear, I spend significant time building a culture that fosters respect, initiative and innovation to ensure that every individual sees him/herself as a critical resource and applies themselves accordingly. Finally, I believe that leaders are accountable for the performance of their organizations by ensuring three things: (1) every person in the organization has a clear and shared view of the organization's purpose and expected results; (2) every person knows what he or she does to support corporate goals; and (3) every person is accountable to take actions necessary to discern and adjust to change in the operating environment of the organization ("Acting like owners vice employees.")

b. Your experience managing personnel.

I have led people in organizations ranging in size from ten to tens of thousands for over forty years. My education at the U.S. Air Force Academy provided a foundation in leadership and management that I have worked to improve through self-study, formal education, and hands-on experience. My specific leadership and management experience includes:

- *Service as a senior executive at NSA for 17 years (1997-2014) with responsibility across that time to lead: (a) a 24/7 operations team responsible for NSA time sensitive operations (1997); (b) a more than 10,000 person work force responsible for all NSA intelligence production (2001-2003); U.S. activities in the United Kingdom as the U.S. Special Liaison London (2003-2006); and (c) as NSA's chief operating officer and senior civilian as NSA deputy director (2006-2014)*
- *I also led various organizations in the U.S. Air Force and Air National Guard as an active and reserve officer from 1976-2006. I commanded a C-130 tactical airlift squadron, a C-130 operations and maintenance group, and a joint force headquarters (comprised of Army and Air Force personnel) supporting both federal and State missions (Maryland National Guard).*
- *In all of these, I was responsible for hiring, developing, counseling, rewarding and/or holding employees accountable for their performance.*

c. What is the largest number of people who have worked under your supervision?

As the NSA Deputy Director for Analysis and Production (2001-2003), I was responsible for more than 12,000 NSA analysts. As NSA's Deputy Director and senior civilian (2006-2014), I was responsible for more than several hundred NSA senior leaders (members of the senior executive service) and more than 20,000 NSA civilians.

9. What experience do you have standing up new organizations or programs?

In 1996-2000, I led the Maryland Air National Guard's transition from C-130 E model to C-130J model aircraft (as the overall project lead and commander of the gaining squadron and then group.) Maryland served as the lead unit for the introduction of the C-130J to tactical service within the U.S. Air Force. The C-130J had a significantly different set of capabilities and crew complement than the C-130E, which necessitated the development of procedures and the transition of displaced navigators and flight engineers, a task made all the more challenging by Maryland's role as the lead tactical operations unit to receive and deploy the C-130J. The Distinguished Service Medal I received on retirement from the Air Force was largely based on this work.

In 2001, I led the standup of NSA's Directorate of Analysis and Production, a globally distributed organization that combined 12 different production lines (each focused on a specific geopolitical or issue-based intelligence topic) and the technology and systems staffs needed to support their work. Comprised of more than 12,000 people, these organizations had previously been hosted in three separate analysis and technology organizations.

From 2014 – 2021, I served as the inaugural Distinguished Visiting Professor of Cyber Studies and member of the initial cadre of the Naval Academy's Cyber Center and its associated Cyber Science Department. As Chief of Staff of a national effort to define and achieve accreditation of curriculum standards for a Cyber Science major, I helped the Naval Academy stand up its cyber education program, achieve accreditation of the cyber science major, and grow its cyber majors program to its current status as one of the top five majors (in numbers of students) and one of only eleven accredited majors in its offering of 26 overall majors at the baccalaureate level.

10. What would you consider your greatest successes as a leader?

Service as NSA's Deputy Director through the period of 2006-2014, a time when NSA significantly improved the scope, quality and timeliness of its combat support and developed cybersecurity tradecraft that provides an important contribution to the Nation's overall cybersecurity effort.

11. What would you consider your greatest failure as a leader? What lessons did you take away from that experience?

The Edward Snowden allegations of 2013 identified a significant trust deficit between the agency, the American people and many of their elected representatives. As the then-Chief Operating Officer for NSA, I accept some responsibility for the failure of NSA to ensure that its missions, major initiatives, and oversight processes were fully communicated and understood by the people NSA is charged to serve. The lesson for me was the importance for government leaders to continuously assess and, as necessary, update government initiatives to ensure they make the difference they must in support of the security and defense of civil liberties for U.S. citizens.

12. Please give examples of times in your career when you disagreed with your superiors and advocated your position. Describe circumstances in which you were successful and in which you were unsuccessful.

When the federal government determined in 2013 that it would furlough employees across the executive branch in a show of solidarity with certain Departments that faced personnel funding shortfalls, I argued that NSA should find and pay its fair share to assist the DoD in covering its personnel accounts but that NSA should not, in the absence of compelling cause, furlough the very people that it described at every turn as "its most valued and valuable resource". After significant pushback from the DoD comptroller and the program manager for the Information Systems Security Program (ISSP), my

recommendation was subsequently supported and implemented by the Directors of NSA and National Intelligence.

When the Maryland Air National Guard was being considered for conversion from its legacy C-130E's to a newer platform in the 1995 timeframe, I argued strongly as the unit's modernization project officer to Congressional and active duty Air Force leadership that the unit be considered for C-130H equipment that would retain the Navigator and Flight Engineer positions, and against the newer C-130J version which was being touted as a major technology upgrade that would remove and replace navigators and flight engineers from the platform. I argued that the challenges of implementing a new weapons system in the reserve component alone (the active duty Air Force did not then plan to procure any C-130J's) would introduce significant risks to the conversion owing to the Air National Guard's lack of doctrinal capacity to consider and revise Air Force wide tactics and procedures as well as personnel challenges regarding how to accommodate displaced crew members. I was unsuccessful in making the case for C-130H's and the unit became the first tactical airlift unit in the combined active and reserve Air Force to transition to the C-130J. The transition was ultimately successful but took considerably longer and experienced far greater costs than originally imagined. I subsequently served as the unit's conversion project officer while commanding at the squadron and group level, and the resulting conversion paved the way for successful introduction of the C-130J to the larger Air Force as the mainstay of the tactical airlift fleet.

13. Do you seek out dissenting views and encourage constructive critical dialogue with subordinates? Please provide examples of times in your career when you have done so.

Yes, seeking, reconciling and taking influence from dissenting views is an essential best practice. Throughout my career, I have actively sought out, taken influence from and strongly supported the right of people to express candid views on matters relevant to the shared work of the organization.

14. Please list and describe examples of when you made politically difficult choices that you thought were in the best interest of the country or your organization.

See answer to question 12, above.

15. Please describe how you build credibility and trust among staff as a leader.

I prioritize establishing, communicating, and modeling the behaviors expected of employees (integrity, proactive service, accountability, and respect for others key among them). I actively seek out employee perspectives, visit their workspaces to observe and learn about their work first-hand, and provide feedback on their inputs and work. I provide clear guidance on priorities while remaining open to feedback. And finally, I believe that a core tenet of building trust is to communicate, communicate, communicate.

16. During your career, has your conduct as a government employee ever been subject to an investigation or audit by the Office of Special Counsel, Department of Justice, agency Equal Opportunity office or investigator, agency Inspector General, or any other similar federal, state, or local investigative entity? If so, please describe the nature of the allegations/conduct and the outcome(s) of the investigation(s) or audit(s).

Yes. While serving as Commander of the 135th Airlift Group (Maryland Air National Guard) in 2000, I was directed by my Commander to investigate a report of sexual harassment by a member of my unit. I did so and found that there was a sufficient basis to warrant referral to the unit inspector general. As a result, I was accused by the accused member of prejudicial and discriminatory behavior. The accusation was investigated by the Air National Guard inspector general, and I was found innocent of all accusations.

III. Role of the National Cyber Director

17. Please describe your view of the core mission of the Office of the National Cyber Director and what you would consider to be your primary role and responsibilities if confirmed.

The core mission of the Office of the National Cyber Director is defined in statute as the principal advisor to the President on cybersecurity policy and strategy and to lead coordination of implementing that policy and strategy. Foremost among my priorities is to expeditiously stand-up the Office of the National Cyber Director. This includes administrative tasks such as finding space and hiring staff to more substantive, legal tasks, such as ensuring roles and responsibilities of the NCD are reflected in executive branch policy, processes, and procedures.

A primary responsibility will be to get Federal system's digital infrastructure in order, which will include the expeditious implementation of the Executive Order 14028 (Improving the Nation's Cybersecurity) and harmonizing and updating Federal incident response procedures to reflect NCD and private sector roles.

I plan to focus on ensuring federal cybersecurity roles across agencies and departments are crisply defined, deconflicted and complementary. This will mean ensuring the NCD supports and connects CISA, FBI, Secret Service, and the distributed cybersecurity centers across all federal agencies and departments to the larger federal strategy and attendant initiatives.

The office should prioritize coordinating implementation of policy and strategy related to public-private collaboration on cyber security of critical systems and functions vital to the national security of the U.S. This will include ensuring implementation of the Integrated Cyber Center provision of NDAA FY21, Continuity of the Economy and related exercises are conducted as required by law, and improving the cybersecurity posture for private sector, state, local and tribal entities.

Finally, I plan to ensure the office works on significantly improving cyber education and talent development programs, in collaboration with federal, state, local and private sector stakeholders.

18. Please describe your understanding of the authorities of the Office of the National Cyber Director and how those authorities facilitate the core mission of the office.

As per the authorizing legislation (National Defense Authorization Act of 2021), the National Cyber Director will:

(A) Serve as the principal advisor to the President on cybersecurity policy and strategy relating to the coordination of—

- (i) information security and data protection;*
- (ii) programs and policies intended to improve the cybersecurity posture of the United States;*
- (iii) efforts to understand and deter malicious cyber activity;*
- (iv) efforts to increase the security of information and communications technology and services and to promote national supply chain risk management and vendor security;*
- (v) diplomatic and other efforts to develop norms and international consensus around responsible state behavior in cyber space;*
- (vi) awareness and adoption of emerging technology that may enhance, augment, or degrade the cybersecurity posture of the United States; and*
- (vii) such other cybersecurity matters as the President considers appropriate;*

(B) Offer advice and consultation to the National Security Council and its staff, the Homeland Security Council and its staff, and relevant Federal departments and agencies, for their consideration, relating to the development and coordination of national cyber policy and strategy, including the National Cyber Strategy;

(C) Lead the coordination of implementation of national cyber policy and strategy, including the National Cyber Strategy;

(D) Lead coordination of the development and ensuring implementation by the Federal Government of integrated incident response to cyberattacks and cyber campaigns of significant consequence;

(E) Preparing the response by the Federal Government to cyberattacks and cyber campaigns of significant consequence across Federal departments and agencies with responsibilities pertaining to cybersecurity and with the relevant private sector entities;

(F) Coordinate and consult with private sector leaders on cybersecurity and emerging technology issues in support of, and in coordination with, the Director of the Cybersecurity and Infrastructure Security Agency, the Director of National Intelligence, and the heads of other Federal departments and agencies, as appropriate; and

(G) Annually report to Congress on cyber security threats and issues facing the United States, including any new or emerging technologies that may affect national security, economic prosperity, or enforcing the rule of law.

19. Today there are more than 20 agencies across the federal government with roles and responsibilities associated with U.S. cyber capabilities.

- a. What role do you believe the Office of National Cyber Director should play in relation to these other agencies?

Congress assigned responsibility to the NCD to:

- *"Lead the coordination of implementation of national cyber policy and strategy, including the National Cyber Strategy."*
- *"Lead coordination of the development and ensuring implementation by the Federal Government of integrated incident response to cyberattacks and cyber campaigns of significant consequence"*
- *"Prepare the response by the Federal Government to cyberattacks and cyber campaigns of significant consequence across Federal departments and agencies with responsibilities pertaining to cybersecurity and with the relevant private sector entities"*

Each of these NCD responsibilities acknowledges the essential need for context, coherence and direction to create unity of purpose and effort among the various federal agencies and departments exercising cyber responsibilities. Cyber is a team sport, requiring leaders to build and leverage operational collaboration and complementary relationships as the essential foundation of an efficient, effective and well defended cyber ecosystem. If confirmed, I will work to build and sustain unity of purpose and effort from strategy through operational execution while respecting each agency's statutory authority and role.

- b. What challenges do you anticipate the office will face as it establishes relationships with other agencies? If confirmed, how do you plan to overcome those challenges?

Change in the status quo will be perceived by some as an encroachment on their extant authority, by some as optional, and by still others as unnecessary. The NCD must demonstrate the compelling case for change and an unwavering determination to drive needed change. I've led change with new organizations a number of times in my career. This is a dynamic that is familiar to me and I intend to bring my considerable experience in assuaging anxiety of vested interests when presented with the new role of the NCD.

20. Please describe your understanding of the respective roles and responsibilities of the Office of the National Cyber Director compared to the Director of the Cybersecurity and Infrastructure Security Agency (CISA) within the Department of Homeland Security (DHS).

The NCD is accountable for leading the coordination and implementation of national cyber policy and strategy, the development and implementation by the Federal Government of integrated incident response to cyberattacks and cyber campaigns of significant consequence, and coordinating and consulting with private sector leaders on cybersecurity and emerging technology issues in support of and in coordination with the Director of CISA.

The Director of CISA is the overall lead for the implementation of operations of federal civilian cybersecurity, defense of critical infrastructure, and operational collaboration with the private sector. The National Cyber Director will champion and support the Director of CISA in their operational leadership, to help ensure that policies, programs, and plans are fully executed in good faith by all Federal stakeholders.

In sum, the NCD focuses on ensuring the sufficiency and implementation of cyber strategy while the Director CISA focuses on operations that implement federal cyber strategy and its collaboration with the private sector on related matters. Using a sports analogy, the NCD will serve in the role of a "coach" while the Director of CISA will operationalize cybersecurity strategy as an on-the-field "quarterback."

21. Please describe your understanding of the respective roles and responsibilities of the Office of the National Cyber Director compared to the Deputy National Security Advisor for Cyber and Emerging Threats.

The NCD is accountable for leading the coordination and implementation of national cyber policy and strategy, the development and implementation by the Federal Government of integrated incident response to cyberattacks and cyber campaigns of significant consequence, and coordinating and consulting with private sector leaders on cybersecurity and emerging technology issues.

Consistent with the direction of the President, the functions of the National Security Council are to—

- (1) advise the President with respect to the integration of domestic, foreign, and military policies relating to the national security so as to enable the Armed Forces and the other departments and agencies of the United States Government to cooperate more effectively in matters involving the national security;*
- (2) assess and appraise the objectives, commitments, and risks of the United States in relation to the actual and potential military power of the United States, and make recommendations thereon to the President;*
- (3) make recommendations to the President concerning policies on matters of common interest to the departments and agencies of the United States Government concerned with the national security*

In that vein, the Deputy National Security Advisor for Cyber and Emerging Technology (DNSACET) manages the development of cyber policy and strategy for the National Security Council. In the execution of these responsibilities, the DNSACET should

coordinate closely with the NCD, who is a regular attendee of relevant Principal Committee meetings of the NSC and a participant in its attendant policy processes.

In sum, these roles are complementary and, by definition, will need to maintain close coordination in the execution of their respective portfolios. While the NCD establishes the overall, long-term vision for a national cyber strategy, the DNSACET will be a vital partner in achieving consensus and developing implementing policies and procedures.

22. Please describe your understanding of the respective roles and responsibilities of the Office of the National Cyber Director compared to the Office of Management and Budget including the Federal Chief Information Officer and Federal Chief Information Security Officer.

In accordance with the provisions of the Federal Information Security Modernization Act (FISMA) of 2014, the Office of Management and Budget (OMB) shall oversee agency information security policies and practices, and ensure that the Cybersecurity and Infrastructure Security Agency carries out its authorities and functions authorized by FISMA.

With these statutory provisions in mind, the Federal Chief Information Officer (CIO) and Chief Information Security Officer (CISO) collectively oversee federal technology spending, federal information technology (IT) and cybersecurity policy, and conduct strategic planning for federal information technology and cybersecurity infrastructure and investments. As they are under the Office of Management and Budget, the Federal CIO and CISO play a primary role in reviewing and overseeing department and agency budgets and programs related to federal IT and cybersecurity.

The NCD is charged with developing and implementing a national cyber strategy, which, by definition, is inclusive of federal cybersecurity. In this role, if confirmed, I would expect to coordinate closely with the CIO and CISO in developing a long-term strategy for Federal cybersecurity and overseeing its implementation. Additionally, the NCD is authorized to review the annual budget proposals for federal agencies to advise on whether such proposals are consistent with the national cyber policy and strategy, which would require close coordination with the CIO and CISO. Whereas the federal CIO and CISO's focus is solely on federal IT and cybersecurity, the NCD is intended to take a broader view and can therefore identify and drive synergies and opportunities between federal enterprise cybersecurity efforts and the broader, national mission to secure the cyber ecosystem.

23. Please describe your understanding of the role and responsibilities of the Office of the National Cyber Director with respect to private sector entities. If confirmed, what steps would you take to establish and maintain relationships with the private sector?

As authorized, the NCD will "...coordinate and consult with private sector leaders on cybersecurity and emerging technology issues in support of, and in coordination with, the Director of the Cybersecurity and Infrastructure Security Agency, the Director of

National Intelligence, and the heads of other Federal departments and agencies, as appropriate."

The law correctly recognizes that the private sector is a critical partner in both cyber policy and operations. If confirmed, I would immediately establish relationships to key private sector stakeholders using existing constructs created to facilitate public-private engagement on cyber matters (NSTAC, NLAC, ISACs and the Enduring Security Framework key among them). I also would expect to routinely coordinate with and support the Cybersecurity and Infrastructure Security Agency and Sector Risk Management Agency-led sector coordinating councils under the Critical Infrastructure Partnership Advisory Council (CIPAC). These, and other constructs, will be critical to informing the NCD of expectations, aspirations, and ideas regarding how best to significantly and expeditiously improve two-way communication on strategic expectations, existing and forthcoming policy, government programs, threats and risks, and supporting lines of effort.

IV. Policy Questions

Management, Workforce

24. What do you consider to be the principal challenges in the area of human capital management while standing up the Office of National Cyber Director?

The Office of the National Cyber Director will be created from 'scratch', so a key challenge will be determining hiring authorities and establishing associated administrative resources. I will give a high premium in ensuring diversity of both views and experience is fully reflected in the makeup of the office.

25. What measurements would you use to determine whether the ONCD is successful?

- *Standup and full empowerment of the office of the National Cyber Director, reflected in budget procedures, strategy processes, policy, and executive orders.*
- *Clarity in the defined cyber responsibilities and resulting operational coherence of Federal departments and agencies, with updated procedures and executive orders.*
- *Integration of the private sector in U.S. government cyber planning and operations, through common situational awareness, response planning, and analytical collaboration.*
- *Reduction in overall number and scope of cyber incidents that constitute a common hazard to federal, state, local, tribal, and territorial governments and the private sector.*
- *Reduction in the average 'time in target' of cyber intrusions, meaning quicker detection and faster response to incidents when they occur in the private sector and government(s) (federal, state, local, territorial and tribal).*
- *Significant reduction in cybersecurity workforce gaps in federal departments and agencies.*

- Improvements in nation-wide cyber education and talent development (working with federal, state, local and private sector)
- Greater joint, multi-agency efforts in cyber operations, response, and planning.

26. How will you address the challenge of recruiting, hiring, training, and retaining the necessary personnel with critical cybersecurity expertise?

Please note that my answer to this question addresses the staffing of the Office of the National Cyber Director. My answer to question 28 addresses the broader question of staffing the federal cyber workforce and supporting national workforce development.

With respect to staffing the Office of the National Cyber Director, I will take personal responsibility for recruiting and hiring key staff while taking care to bring aboard personnel and administrative specialists with experience in creating and staffing Executive Office of the President (EOP) entities. Establishing a clear vision, positive workplace culture, empowered employees, and a sense of mission will be one of the clearest ways to make the Office of the National Cyber Director an attractive place to work – both in recruiting new employees and in retaining existing ones.

27. If confirmed, how will you ensure the Office of the National Cyber Director is positioned to succeed beyond your tenure as NCD? What steps will you take to prepare the office for future presidential transitions?

The office must establish lines of effort that reflect enduring needs rather than the shorter horizons of a present administration. Succession planning must be given high priority for all positions, especially senior leadership. Ultimately, however, success in delivering on the statutory responsibilities of the NCD will be the best guarantor of its continuance. As with any Senate-confirmed position, Congress is both an accountability mechanism and strategic partner. The NCD is obligated, and will, report on that progress to the Congress on a regular basis.

28. What do you view is the role of the NCD in developing the government-wide cyber workforce?

Improving and expanding the availability of quality cyber talent for the Federal Government and the private sector is a central concern in cybersecurity and, consequently, must be addressed by any National Cyber Strategy. The National Cyber Director, responsible for both developing and overseeing implementation of such a strategy, clearly plays a clear role in identifying problems and achieving workable solutions vis-à-vis workforce. If confirmed, I commit to working with this committee and stakeholders across the private and public sectors, and academia, to explore and support all reasonable means of addressing the talent gap to ensure the Nation has the cyber talent needed to build, operate and defend the digital infrastructure that underpins virtually every facet of our personal and professional lives.

Federal cyber workforce development efforts are inextricably linked to the development

of a robust national cyber workforce. Accordingly, if confirmed I will work to stimulate growth throughout the national cyber workforce ecosystem and establish reliable, concrete methods to draw on cyber talent outside the federal government. Any solution to the current deficit in cyber talent must give time, effort and resource to all facets of the problem.

- *We need to improve awareness and opportunity that motivate greater numbers of people to enter cyber career tracks (example, awareness or education programs for every student at the earliest possible moment in their matriculation).*
- *We need to re-evaluate the skills that are actually required to fill cyber and information technology jobs (In many, if not most, cases a Bachelor of Science is not required and we should adjust the requirements accordingly.)*
- *Consistent with this approach, we need to examine and employ all mechanisms that can prepare people for cyber related jobs – internships, cooperative education, certification, and, of course, educational paths through two and four year colleges.*
- *Once ‘on the job’ we need to ensure that our cyber workers have and enjoy viable career paths that motivate them to remain on the job, so we will need to improve feedback and career tracks to ensure mentoring, development opportunities and rewards actively incentivize and sustain the workforce we need.*
- *Finally, we should give attention to developing greater digital literacy in every cyber user – equivalent to learning how to safely cross a street or drive a car – since they are the people who are most often on the “front lines” of the cyber ecosystem.*

To address the federal workforce cyber talent gap, I would, if confirmed, begin by establishing structures to improve interagency coordination on federal cyber workforce development efforts and conduct a review of coding structures and organizational systems for Federal cyber jobs. This review would seek to determine whether structural changes are needed in job classifications. In tandem, I will also initiate the development of a strategy for cyber workforce development. Looking to a longer time horizon, I will work to expand existing entry points to federal cyber service while also developing new pathways that allow federal hiring to recruit talent overlooked by existing vehicles.

29. How would you assess the current organizational structure around cybersecurity governance within the federal government? What, if anything, do you think should change?

As a private citizen, I do not have extensive insight into the federal government's structure around cybersecurity governance. However, my initial observation is that it remains distributed and federated both across the Federal government and within departments and agencies, despite some progress towards a more centralized governance model. Tools such as FISMA, FITARA, Binding Operational Directives, the Federal Acquisition Security Council (FASC), the Technology Modernization Fund (TMF), and the Chief Information Officer (CIO) Council are each important levers to centralize governance, but my perception is that significant gaps remain. If confirmed, a core

priority for the NCD will be to conduct an assessment of barriers to centralized governance and accountability and develop a strategy to address them expeditiously.

30. Do you believe there currently is adequate accountability for federal cybersecurity? If not, how would you ensure there is, if confirmed?

Accountability is critical in ensuring that Federal investments in information technology and cybersecurity are yielding optimal outcomes. The Federal Information Security Modernization Act (FISMA) is an important tool that provides baseline responsibilities and accountability for department and agency heads, the Office of Management and Budget, the Cybersecurity and Infrastructure Security Agency, and the National Institute of Standards and Technology, among others. To that end, FISMA establishes a clear assignment of accountability in its provision that provides that the head of each agency is accountable for their cybersecurity:

*“(a)In General.—The head of each agency shall be responsible for—
(A) providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—
(i) information collected or maintained by or on behalf of the agency; and
(ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.”*

While FISMA has established a good foundation, if confirmed, I would work to expand its remit from a compliance-based model to a risk-based model focused on empirical evidence, reduced attack surface, and demonstrable security outcomes. As mentioned previously, if confirmed, a core priority will be conducting an assessment of Federal cybersecurity and defining a long-term strategy to improve security outcomes. Increasing accountability, transparency, and oversight will be a core focus area of that review.

National Cybersecurity Priorities

31. What do you view to be the most significant current and potential cybersecurity threats facing our nation?

Rogue nation states and criminal actors who conduct indiscriminate and impactful cyber operations top the growing lists of cyber hazards that the U.S. and its allies must interdict and bring to heel. The list of cyber events of significant impact includes, but is not limited to, Wannacry (2017), notPetya (2017), intellectual property theft, interference in democratic processes, ransomware (including Colonial pipeline), and supply chain attacks (Solarwinds and Hafnium).

The conditions which fuel the escalation of these events are common across all of them: insufficient resilience in digital infrastructure (technology, people and doctrine regarding

roles and responsibilities); the absence of timely consequences for malign actors in cyberspace; and the lack of enduring and meaningful collaboration between the victims of these depredations. The result is that adversaries operate far too often with impunity, picking off their victims one at a time by exploiting seams in cyber defenses that offer them manifold opportunities to find and exploit weakness. We must make ourselves a harder target, align actions taken in cyberspace (good and bad) with consequences, and force transgressors to have to beat the combined efforts of all defenders in order to beat any one of them. Resilience, action and collaboration will make a transformative difference.

32. In your view, what are the highest priorities for enhancing national cybersecurity? Why?

The highest priorities must be: (a) to apply a mindset of basic cyber resilience to the cyber ecosystem (e.g., across the technology, people and doctrine that comprise cyberspace); (b) Clearly define and operationalize who's responsible for what with a bias for collaboration vice division-of-effort (private-public collaboration in the defense of systems and functions that cut across private-public sector boundaries will be an important enabler here); and (c) align actions to consequences in cyberspace (there should be incentives and rewards for good behavior, as well as a timely imposition of costs for actions that violate accepted norms and laws).

33. What do you consider to be the principal challenges facing the government when it comes to national cybersecurity policy and strategy? What experience from your past positions best equips you to advise on these challenges?

Moving from stove-piped efforts where organizations protect their perceived equities by focusing on executing their missions in silos to collaboration is a principal challenge to transforming cyber defense but must be built on the foundational priority of building basic resilience robustness into our digital infrastructure. Convincing agency and department leaders that there is no viable substitute for these efforts has long been a challenge but the growing non-partisan support of cybersecurity as an essential and fundamental activity is a promising sign. We must deliver on it.

In my previous positions in the National Security Agency, I had to deal with similar stove-piping and siloed efforts across the agency. Indeed, much of my work was focused on breaking down unhelpful or unconstructive barriers between different lines of work, and on establishing synergies, common processes and procedures.

34. If confirmed, how would you work with other agencies with responsibilities for cybersecurity to implement these priorities?

If confirmed I will immediately reach out to relevant department and agency heads, many of whom I've worked with before, to establish a close working relationship and open lines of communication. Effective policy and strategy requires trust, communication, and consensus among all stakeholders built around a cohesive, compelling, and unifying vision. If confirmed, I would work closely with my partners in other departments and

agencies to craft this vision, gain their buy-in, and hold them accountable to commitments they've made in achieving it.

Additionally, the enabling legislation for the NCD empowers the position with key authorities and responsibilities in implementing policy and strategy, these include:

- Identifying and monitoring the impact and outcomes of national cybersecurity policies;
- Reviewing the effectiveness, including costs, of Federal departments and agencies' ongoing and planned efforts to implement national cyber policy;
- Ensuring interoperability and integration, including real-time information sharing, across the Federal cyber centers; and
- Providing recommendation on changes to information security, budgets, personnel, or other resources needed to achieve identified policy and strategy outcomes.

35. If confirmed, how would you work with the private sector to implement these priorities?

If confirmed, I would utilize existing constructs created to facilitate public-private engagement on cybersecurity, such as the NIAC, NSTAC, and ISACs, among others. I do not expect that I would conduct this engagement alone, but in coordination with departments and agencies who manage these fora or who have central equities related to the issues at hand. The Critical Infrastructure Partnership Advisory Council (CIPAC), led by the Cybersecurity and Infrastructure Security Agency, is, through its sector coordinating councils, the most mature forum for public-private engagement. If confirmed, I would coordinate with the Director of CISA in utilizing these councils to advance the policy and strategic priorities set forth by the U.S. government.

36. What elements do you believe should be in a federal cybersecurity strategy?

A federal cybersecurity strategy should address challenges and opportunities inherent in the technologies, services, structures, processes, and workforce that constitute the federal civilian information technology enterprise. This should include measures that:

- *Improve transparency, oversight, and accountability for department and agency heads and Federal CIOs for the security of their enterprise;*
- *Take advantage of shared services and infrastructure within departments and agencies and across the Federal government for cost reduction, greater situational awareness, and better security outcomes;*
- *Improve situational awareness of the Federal enterprise within and across agencies, to include reducing barriers to information-sharing between Federal cyber centers, security operations centers, and other segments of Federal networks (such as the intelligence community and the Department of Defense);*
- *Standardize incident response and notification procedures across departments and agencies for a more cohesive and consistent approach;*
- *Address the talent gap felt by many departments and agencies in their cybersecurity programs, to include increasing availability of talent, centralizing*

services reduce security burden, and consolidating education and training programs between departments and agencies;

- *Partner with the private sector to both leverage its strengths and to deliver federal support when and where appropriate to the shared challenge of building, sustaining and defending digital infrastructure critical to the Nation.*

37. Do you believe the lines between offensive and defensive cyber roles are appropriately drawn? If not, what changes would you recommend ?

As a private citizen, I have insufficient insight into the current relationship between offensive and defensive cyber roles to fully answer this question. I believe they must complement each other and commit, if confirmed, to working with this committee to assess and influence the doctrine needed to guide their authorization, resourcing and integration.

38. Do you believe the lines between military and civilian cyber responsibilities are appropriately drawn? If not, what would you recommend to change?

As a private citizen, I have insufficient insight into the current relationship between offensive and defensive cyber roles to fully answer this question. With that limitation in mind, I assess that current roles and responsibilities between DoD and civilian cyber agencies have been sufficiently studied, implemented and adjusted over time to achieve a reasonable degree of complementary effect, optimizing the strength of each while taking care to apply their respective authorities consistent with the imperatives to defend civil liberties while achieving domestic and national security. If confirmed, I commit to working with Congress to assess and influence the doctrine needed to guide their authorization, resourcing and integration.

International Partners and Adversaries

39. What do you see as the role of ONCD in negotiating and maintaining partnerships with other countries on cybersecurity? Do you see this as duplicative of other existing agency responsibilities?

The NCD will play an important role in forging cybersecurity relationships with allies but that work must always be performed in the larger context of geo-political objectives and the various instruments of power that can be brought to bear in realizing them. To that end, the National Security Council will retain the overall lead for national security and in defining and allocating roles that allies and various instruments of power will maintain. The Secretary of State will retain overall lead for diplomacy and the formulation and conduct of alliances. If confirmed I will support their work and participate in international collaboration as called upon and consistent with the direction and policies they and the President set forth.

I do not see the role of the National Cyber Director as duplicative of other agencies vis-à-vis international cooperation, but rather complementary and supportive of their efforts.

Cyber and emerging technologies are increasingly central to all nations' national security and economic security. The National Cyber Director will play a critical role in providing a comprehensive and cohesive viewpoint across all U.S. government department and agency equities and missions, one that can act as an effective counterpart with similar positions in ally and partner governments.

40. What opportunities do you see for increased cooperation to combat international cybersecurity threats?

See answers to question 39, above and question 41, below.

41. Nation-state actors are increasingly using domestic networks to conduct foreign espionage campaigns. What is NCD's role in mitigating the exploitation of our country's infrastructure and how will your role help thwart this persistent activity?

The law creating the NCD provides that the NCD will "...coordinate and consult with private sector leaders on cybersecurity and emerging technology issues in support of, and in coordination with, the Director of the Cybersecurity and Infrastructure Security Agency, the Director of National Intelligence, and the heads of other Federal departments and agencies, as appropriate"

The legislation creating the NCD also holds that the NCD shall:

Lead coordination of the development and ensuring implementation by the Federal Government of integrated incident response to cyberattacks and cyber campaigns of significant consequence, including—

- (i) ensuring and facilitating coordination among relevant Federal departments and agencies in the development of integrated operational plans, processes, and playbooks, including for incident response, that feature—*
 - (I) clear lines of authority and lines of effort across the Federal Government;*
 - (II) authorities that have been delegated to an appropriate level to facilitate effective operational responses across the Federal Government; and*
 - (III) support for the integration of defensive cyber plans and capabilities with offensive cyber plans and capabilities in a manner consistent with improving the cybersecurity posture of the United States;*
- (ii) ensuring the exercising of defensive operational plans, processes, and playbooks for incident response;*
- (iii) ensuring the updating of defensive operational plans, processes, and playbooks for incident response as needed to keep them updated; and*
- (iv) reviewing and ensuring that defensive operational plans, processes, and playbooks improve coordination with relevant private sector entities, as appropriate;*

A key line of effort in this work will be to develop integration and collaboration that provides a collective and shared picture of threat activity taking place across the boundaries that define domestic and foreign jurisdictions (which govern which

organization can see and act on observed threats). While it is premature for me to state what the solution may be, it is unlikely to be one that simply subordinates the interests and/or authorities of one party to another. The more likely solution will be found in information sharing that reveals threats that cut across jurisdictions while protecting personal, proprietary and/or classified information that would otherwise result in violations of privacy or confidentiality.

42. What do you believe is important to include in a deterrence strategy in cyberspace?

My service on the U.S. Cyberspace Solarium Commission significantly informs my answer here. The U.S. must combine several facets of deterrence in order to achieve the desired effect of changing the decision calculus of both transgressors and defenders in cyberspace. Foundational components of that deterrence strategy should include:

- *Defense and resilience: We must make ourselves a harder target, reduce systemic vulnerability in our ecosystem that affords our adversaries ample opportunity for exploitation, increase detection and sharing of threat information to mitigate and respond to incidents quickly, and institute robust planning to quickly recover and restore functionality if an incident does occur.*
- *Align actions with consequences: There should be benefits to behaving responsibly in cyberspace and costs imposed for violating legally defined norms and behaviors. Timely imposition of costs on transgressors will be particularly important. We must align actions taken in cyberspace with consequences, hold adversaries accountable for unacceptable behavior, and attribute and impose consequences when that behavior violates international norms or U.S. national security interests. The tools we employ to impose costs should leverage all capabilities: the ability to directly disrupt and counter using cyber methods as well as legal, diplomatic, and financial remedies.*
- *Finally, we must get the roles and responsibilities of individuals, private sector organization and governments (at all levels) sorted out so that they complement one another, so that the resulting collaboration puts adversaries in a position that they have to beat all of the defenders in cyberspace in order to beat any one of them.*

43. What is your stance on public attribution of nation-state actors when they have compromised our federal and national networks?

The United States government should continue to identify, and as necessary publicly call-out, malicious actors that compromise Federal or critical infrastructure networks contrary to U.S. national security interests and international norms. Attribution is a foundational and necessary tool, constituting an important element of efficiently focusing limited resources on identified threats, mitigating malicious cyber campaigns, and, perhaps most importantly, in ensuring malign actors bear appropriate costs for their transgressions. Public attribution, whereby the U.S. government publicly 'calls out' a

bad actor, should precede, by necessity, most means of cost imposition meant to deter future behavior. Attribution should proceed under rigorous evidentiary standards commensurate with the severity of measures the United States elects to impose on an adversary. When and where possible, the United States should seek to coordinate with allies and partners to achieve reliable attribution, publicly call out malign behavior, and, when warranted, impose consequences on malign actors for any behavior contrary to international norms and collective national security interests.

44. Attribution in cyberspace is difficult to prove. In your view, what level of proof is necessary before attributing a cyber-attack?

When discussing attribution, we need to make a distinction between detection, identification, and a more formal, government-led attribution process, which includes making attribution public as evidence and circumstances warrant. If an adversary has compromised a system, detection is sufficient for an owner or operator to neutralize it within their system. If an adversary is conducting operations that constitute existential harm to life, health and safety, then attribution needs only identify the literal source of the activity to justify interdicting and stopping it.

Actions beyond those taken above require a more formal and rigorous attribution process. This requires reasonable analysis based on the preponderance of evidence relevant to the attacker and the circumstances of the attack. These include matching malware, infrastructure, tactics, techniques, and procedures with known threat actor groups; identifying intent and motivation of the attack to determine who benefits; and utilizing both public and classified means to determine affiliation with or support of state or non-state groups. For more public attribution, which should be a precondition for imposition of serious consequences such as sanctions or indictments, the bar should be set intentionally high and should proceed with a rigorous evidentiary standard intrinsic to the 'high-confidence' assessment required.

Given the difficulties occasioned by inadequate attribution, work to improve the prospects of firmer and more timely attribution should be a high priority for both research and operational collaboration.

Information Sharing

45. How do you define success for cybersecurity information sharing across the public and private sectors?

Public-private information sharing is a complex suite of operations that requires routine communication between all parties and a robust effort on the U.S. government's part to be a central consolidator, enricher, and disseminator of indicators, context, and risk information. Its usefulness is not limited to any one discipline of security, but equally critical for prevention, mitigation, response, and recovery. Foundational metrics of success for information sharing should include a reduction in the number of successful cyber intrusions over time, reduction in time-to-detection of intrusions for private entities

and federal agencies, and a reduction in down-time and impact when an intrusion is successful. Ultimately, while information shared should aim to prevent attacks, it is equally important that we are able to leverage detection and identification of a cyber intrusion from one entity to rapidly inoculate or enable detection in others. This is vital in mitigating and limiting the scope of adversary cyber campaigns

From a U.S. government program management perspective, success will mean an overall increase in the number of public and private entities participating in information sharing programs, increase in the quantity and utility of information shared by all parties, the interoperability and automation of sharing programs with existing detection and security mechanisms, and the usefulness (or perceived 'value proposition') of these programs in participating entities' security enterprise. We must keep in mind that information sharing is not an end in itself, but rather an enabler and, at times a precondition, for public-private operational collaboration. In this regard, the U.S. government must take care to ensure that it maintains a value proposition sufficient to provide clear advantages to those who would participate and contribute meaningfully.

We also must ensure that we avail ourselves of information shared to take lessons and insights that can be applied to a better understanding of risk and best practices for the future. This will require that time and attention is given to the collection of cyber statistics that can serve as the benchmark. While study of any one incident alone can provide some meaningful information, drawing inferences and identifying causal factors for a cyber campaign or across a series of similar cyber incidents can provide insight to guide security investment, prevention and response action. It is critical that in any information sharing enterprise, the U.S. government conducts after action analysis and actively seeks to better understand what works and what doesn't in cybersecurity.

Improvements in the resilience of digital infrastructure and the development of substantive and vigorous information sharing can serve as an important leading indicator of success but our focus must remain on the primary measures, not illusory ones.

46. What do you believe is the federal government's responsibility to share cybersecurity information with the private sector? Do you believe the government is meeting its responsibility to share information with the private sector?

The Federal government has an affirmative obligation to share information with the private sector, particularly in instances where there is a known or suspected threat to the entity in question. At a minimum, the U.S. government has a duty to inform a private sector entity in any instance where there is clear evidence the entity has been compromised by a malicious cyber actor. This obligation must be balanced with the reasonable need to preserve sources and methods within the intelligence community, as compromising such sources may deprive the government from the very tools they need to detect and identify threats to private sector entities.

As a private citizen it is difficult for me to assess whether the U.S. government is fully meeting its responsibilities to share information with the private sector. My perception, however, is that there are considerable legal, procedural, and organizational barriers to more effective public-private information sharing, a dynamic exacerbated by lack of single, comprehensive mechanism for situational awareness of cyber threats across Federal departments and agencies.

47. Do you believe there is adequate reporting of cyber incidents to the government by non-federal entities? If not, what would you change?

As private citizen it is difficult for me to assist the current status and sufficiency of incident reporting. My views on incident reporting are as follows.

Incident reporting serves a number of highly beneficial purposes. It affords the reporting entity and the government an opportunity to collaboratively assist the affected entity. More importantly, it contributes to a more comprehensive understanding of risk, allowing the government and affected stakeholders to gain insight into evolving tradecraft, intent, and capability of adversaries – information which can thereafter be shared with other entities who may be similarly targeted. This sharing, aggregation and analysis is foundational to the goal of understanding and addressing adversary behaviors that cut across network and jurisdictional boundaries.

It is increasingly clear that voluntary incident reporting and the sharing of identified trends is currently insufficient to gain a system-wide level of awareness, to inform appropriate response options, and/or to hold organizations accountable for clearly deficient security practices.

If confirmed, I commit to working with this committee and stakeholders across the private and public sectors to assess the sufficiency of information sharing and to recommend measures that will increase beneficial sharing while ensuring the continued defense of privacy and legally protected information.

48. Please describe your plans, if confirmed, for improving cybersecurity threat information sharing, including ensuring that the information is timely and actionable for recipients to integrate into their cybersecurity defensive capabilities.

If confirmed, I would focus on broader, deeper and more timely operational collaboration between the public and private sector, with an emphasis on ensuring there is a two-way flow of information of value, while protecting privacy and proprietary or classified information.

49. Please describe your views on the appropriate role of private sector entities in working with the federal government to improve our nation's cybersecurity.

Given that the private sector develops, owns, and operates the significant majority of digital infrastructure underpinning critical functions within the United States, they are a

critical partner in developing security solutions across the range of technology, education, and cyber defense. Actual operations to defend infrastructure should be governed by rules that ensure defenders have explicit legal permissions to surveil a given network and/or to take actions to interdict and contest adversary action. The imposition of cost(s) through cyber action, legal remedies, diplomacy, financial sanctions and regulation remains the province of governments at federal, state and local levels. Collaboration between private and public organizations is needed to ensure the combined authorities, capabilities, and energies of both sectors are fully applied to the shared task of cyber defense.

As to public-private collaboration more generally, all companies are different and the nature of their participation in the protection of the country's critical assets varies depending on a number of factors, including their sector, size, criticality, and relative sophistication or maturity. At a minimum, private sector critical infrastructure entities should engage with the DHS-led Critical Infrastructure Partnership Advisory Council (CIPAC) which is the primary forum through which they can contribute to risk decisions and communicate their enterprise or sector-specific needs. As to deeper private sector engagement, the appropriate role and contours of a private sector company's engagement often depends on what they are able to contribute to the broader national effort. For instance, for larger, more critical companies, who tend to have more sophisticated security operations and can act as mature partners in public-private collaboration, they should be expected to play a greater role in cyber response planning and information sharing. Smaller companies, who generally have less sophisticated security measures, should contribute to an understanding of risk, but should also routinely engage to give the U.S. government an understanding of their intelligence gaps and security needs so that they can be addressed in future program offerings and public policy.

Incident Prevention, Detection, Response, and Recovery

50. What is your assessment of the federal government's current capabilities to prevent incidents? If confirmed, how will you work to improve them?

It is, of course, difficult to account for incidents that may have been prevented through existing government efforts vs. ones that have manifested through increases in adversary activity. What's clear is that the U.S. government can do more to reduce vulnerability in the technology and processes in the cyber ecosystem, such as through identification and communication of best practices, rapid information sharing, and establishment of security standards for enterprise networks and common technologies in use that can meaningfully advance the security of these systems and reduce opportunities of exploitation.

If confirmed in the position of NCD, I will give high priority to prevention as the preferred strategy for bringing greater confidence to our dependencies on digital infrastructure.

51. What is your assessment of the federal government's current capabilities to detect incidents? If confirmed how will you work to improve them?

As a private citizen, I do not have detailed knowledge of the federal government's current capabilities to detect incidents. My perception, however, is that the U.S. government is severely limited in its ability to detect and identify threats affecting entities in the domestic United States, to include SLTT and private sector critical infrastructure. It is imperative that the U.S., in collaboration with the private sector, achieves a level of shared situational awareness sufficient to quickly interdict or prevent threats before or as they occur – while respecting privacy and civil liberties. This shared situational awareness is a necessary precondition for public-private collaboration and should be a core priority. If confirmed, I will conduct an assessment of these challenges and devise a strategy to address them while ensuring the defense of civil liberties.

52. What is your assessment of the federal government's current strategies to respond to cyberattacks when they occur? If confirmed, how will you work to improve those strategies?

While, as a private citizen, I do not have detailed insights into the federal government's capabilities or strategies to respond to cyberattacks and other cyber incidents, my perception is that the capabilities are multi-faceted, distributed across many agencies and departments, uneven in capabilities, and, at times, inconsistent in approach. While the Federal government's cyber effort has improved much over the last ten years, it remains limited by capacity and the lack of a long-standing and well-practiced framework that creates unity of purpose and effort. If confirmed, I will assess and identify gaps between current policy and department and agency execution in detection and notification of incidents and their response procedures. I will make recommendations regarding the authority and capacity of each cyber capability and work to ensure that strategy and operational coordination is implemented to create a more cohesive and effective response.

53. What is your assessment of the federal government's current capabilities to respond to cyberattacks? If confirmed, how will you work to improve these capabilities?

While, as a private citizen, I do not have detailed insights into the federal government's capabilities or strategies to respond to cyberattacks and other cyber incidents, my perception is that the capabilities are multi-faceted, distributed across many agencies and departments, uneven in capabilities, and, at times, inconsistent in approach. While the Federal government's cyber effort has improved much over the last ten years, it remains limited by capacity and the lack of a long-standing and well-practiced framework that creates unity of purpose and effort. If confirmed, I will assess and identify gaps between current policy and department and agency execution in detection and notification of incidents and their response procedures. I will make recommendations regarding the authority and capacity of each cyber capability and work to ensure that strategy and operational coordination is implemented to create a more cohesive and effective response.

54. What do you view as the federal government's role in supporting non-federal entities (e.g. private sector, state/local government agencies) that are responding to or recovering from a cyberattack?

The federal government has an affirmative obligation to bring its unique authorities and capabilities to bear in defense of non-federal entities. The U.S. government should, as with other significant incidents regardless of cause (cyber, physical, natural), maintain some capability to assist both SLTT and private entities in responding to and recovering from an incident. The U.S. government, however, should be wary of 'moral hazard' and this assistance should not be a substitute for basic private sector and SLTT security responsibilities and duty of care.

V. Accountability

Whistleblower Protections

55. Protecting whistleblowers and their confidentiality is of the utmost importance to this Committee.

- a. Please describe any previous experience with handling whistleblower complaints. What steps did you take to ensure those individuals did not face retaliation and that their claims were thoroughly investigated?

As the former Deputy Director of the National Security Agency, I complied with all whistleblower protection laws, regulations, rules, and guidance.

- b. If confirmed, what steps will you take to ensure that whistleblower complaints are handled appropriately at the Office of the National Cyber Director?

I firmly believe in whistleblower protections. If confirmed, I will follow all laws and procedures to ensure whistleblowers are protected, and I will direct my staff to do the same.

- c. If confirmed, what steps will you take to ensure that whistleblowers at the Office of the National Cyber Director do not face retaliation, that whistleblower identifiers are protected, and that complaints of retaliation are handled appropriately?

If confirmed, I will ensure that whistleblowers do not face retaliation and are protected. I will follow all laws and procedures to ensure whistleblower claims are properly investigated, and direct my staff to ensure they appropriately protect whistleblowers consistent with the law.

Cooperation with Inspectors General

56. Inspectors General (IGs) face unique obstacles as they do their work, including budget challenges and disputes with agency heads over access to information. How do you view ONCD's relationship with various Offices of Inspectors General (OIGs)?

The Inspectors General are independent, objective offices. They have a critical role in identifying waste, fraud, and abuse as well as conducting audits and investigations into programs. The recommendations of the IGs are provided to the Departments and Congress. If confirmed, I will work with them to ensure they have information needed to carry out their missions.

57. Under what circumstances, if any, do you believe ONCD would not be required to provide any OIG with timely access to agency records?

If confirmed, I will work to ensure that the OIGs have access to the information they need to perform their vital function, consistent with the law.

58. If confirmed, do you commit to fully cooperate in a timely manner with any audits, investigations, and other reviews and related requests for information from IGs?

Yes.

Cooperation with GAO

59. If confirmed, do you commit without reservation to ensuring GAO receives timely, comprehensive responses to requests for information, including for records, meetings, and information?

If confirmed, I will work to ensure that GAO has access to the information it needs to perform its vital function, consistent with the law.

60. If confirmed, do you commit to fully cooperate in a timely manner with any audits, investigations, and other reviews and related requests for information from GAO?

If confirmed, I will work to ensure that GAO has access to the information it needs to perform its vital function, consistent with the law.

61. If confirmed, what steps will you take to ensure ONCD and its employees cooperate fully and promptly with GAO requests?

If confirmed, I will work to ensure that GAO has access to the information it needs to perform its vital function, consistent with the law.

VI. Relations with Congress

62. Do you agree without reservation to comply with any request or summons to appear and testify before any duly constituted committee of Congress if you are confirmed?

If confirmed, I will work to ensure that duly constituted Congressional committees have access to the information they need to perform their vital functions, consistent with the law.

63. Do you agree without reservation to make any subordinate official or employee available to appear and testify before, or provide information to, any duly constituted committee of Congress if you are confirmed?

If confirmed, I will work to ensure that duly constituted Congressional committees have access to the information they need to perform their vital functions, consistent with the law.

64. Do you agree without reservation to comply fully, completely, and promptly to any request for documents, communications, or any other agency material or information from any duly constituted committee of the Congress if you are confirmed?

If confirmed, I will work to ensure that duly constituted Congressional committees have access to the information they need to perform their vital functions, consistent with the law.

65. If confirmed, how will you make certain that you will respond in a timely manner to Member requests for information?

If confirmed, I will work closely with Members and their staff. Congress should receive timely responses and I will communicate that clearly to my staff if I am confirmed.

66. If confirmed, will you direct your staff to adopt a presumption of openness where practical, including identifying documents that can and should be proactively released to the public, without requiring a Freedom of Information Act request?

If confirmed, I will commit to making public information about the work of ONCD to the extent possible, consistent with the law.

67. If confirmed, will you keep this Committee apprised of new information if it materially impacts the accuracy of information your agency's officials have provided us?

Yes.

VII. Assistance

68. Are these answers completely your own? If not, who has provided you with assistance?

Yes. These answers are my own. I relied on my experience, publicly available information, and have received input from staff in the Administration, who provided comments which I was free to accept or reject.

69. Have you consulted with the Executive Office of the President, or any other interested parties? If so, please indicate which entities.

These answers are my own. In preparation for my confirmation process, I consulted with staff through high-level, pre-confirmation briefings from the Executive Office of the President, the Departments of Homeland Security, Justice, Defense, and Office of the Director of National Intelligence. These consultations were generally used to inform my answers at a very high level.

I, John "Chris" Inglis, hereby state that I have read the foregoing Pre-Hearing Questionnaire and that the information provided therein is, to the best of my knowledge, current, accurate, and complete.


(Signature)

This 4th day of June, 2021

**Senator Rand Paul
Post-Hearing Questions for the Record
Submitted to Chris Inglis**

**Nominations of Robin Carnahan to be Administrator, General Services Administration;
Jen Easterly to be Director, Cybersecurity and Infrastructure Security Agency, DHS; and
Chris Inglis to be National Cyber Director
Thursday, June 10, 2021**

1. As former deputy director and chief operating officer of the National Security Agency (NSA), you possess an intimate knowledge of the vast surveillance capabilities possessed by the federal government.

Question: Do you believe that the warrantless bulk data collection activities conducted by the NSA during your tenure as deputy director and chief operating officer were constitutional?

I believe the laws that provide for intelligence collection are powerful tools to protect the United States against national security threats. However, the government must use these authorities consistent with statutory safeguards, and internal policies, procedures and oversight mechanisms in order to protect privacy and civil liberties and to keep the trust and confidence of the American people. During my tenure as Deputy Director of the National Security Agency, these authorities were reviewed by federal judges, inspectors general, Congress, and executed in accordance with the laws, controls, and reporting procedures in place at the time. I take very seriously the government's obligations to be scrupulously accurate in presentations to the FISA Court and to ensure that these authorities are exercised accordance with constitutional due process and consistent with American values.

As a general matter, I believe it is critical we work closely with Congress to ensure our national security programs appropriately balance security with civil rights and civil liberties. The strength of our Constitution is in the rights and protections of liberties it affords to individuals.

Question: If confirmed, in what ways do you intend to deploy your knowledge of the NSA's surveillance capabilities in your role as National Cyber Director?

If confirmed, my fundamental and unwavering responsibility would be to ensure that actions undertaken by the NCD and its staff are consistent with the Constitution and protect U.S. national interests. The law authorizing the Office of the National Cyber Director includes a rule of construction that nothing within the authorities of the Director or any person acting under the authority of the Director may be construed to interfere with or to direct an intelligence activity, resource, or operation; or to modify the classification of intelligence information. I would therefore take the role of an intelligence customer and would take explicit steps to understand and comply with the laws, policies and controls in place.

2. As National Cyber Director, any intelligence that crosses your desk will inevitably have been collected under any one of several different authorities which are purposefully kept distinct – most notably with respect to the collection, dissemination, and retention of military, foreign, and domestic intelligence.

Question: How will you ensure that the dissemination of intelligence products by and/or through the National Cyber Director's office will be appropriately limited based on the authorities under which the intelligence was originally gathered? In other words, how do you intend to guard against the potential for the National Cyber Director's office to erode the distinctions Congress has drawn between military, foreign and domestic intelligence gathering activities?

If confirmed, my fundamental and unwavering responsibility would be to ensure that actions undertaken by the NCD and its staff comply with the Constitution and the laws of the United States, and advance U.S. national interests. The law authorizing the Office of the National Cyber Director includes a rule of construction that nothing within the authorities of the Director or any person acting under the authority of the Director may be construed to interfere with or to direct an intelligence activity, resource, or operation; or to modify the classification of intelligence information. . I would bring my former intelligence experience to bear in ensuring the office of the NCD fully complies with laws and policies of the Intelligence Community and to protect civil liberties consistent with American values.

Question: How do you intend to guard against any other misuse, abuse, or manipulation of intelligence by the National Cyber Director's office or any other element of the federal intelligence community?

If confirmed, I would explicitly direct in written policy and verbal guidance that such abuse will not be tolerated and will be investigated and referred to the Department of Justice for prosecution to the fullest extent of the law. I would also ensure that reporting mechanisms are in place to encourage and protect reporting of any such abuse.

3. On January 5, 2018, U.S. Customs and Border Protection (CBP) in the Department of Homeland Security (DHS) released updated guidance¹ on their standard operating procedures for searching electronic devices under the so-called border search exception to the Fourth Amendment. However, CBP's most recent interpretation of the border search exception still requires every American who wishes to travel abroad to surrender any and all expectation of privacy in their digital devices.

Question: Do you think that CBP's updated device search policy is appropriate? Why or why not? *Since I am not a lawyer, I have not studied the legal question. I believe that the Department of Homeland Security's guidance and practices must be consistent with the*

¹ <https://www.cbp.gov/newsroom/national-media-release/cbp-releases-updated-border-search-electronic-device-directive-and>

Constitution in order to protect privacy and civil liberties and to keep the trust and confidence of the American people.

If confirmed as the National Cyber Director, my authorities would not include collection of information under this or similar programs. However, I would use my office to help ensure the full application of legal review and compliance with applicable law in the establishment and execution of any and all capabilities intended to enhance cyber security.

If confirmed, I would work closely with Congress to ensure our national security programs and policies appropriately balance security with civil rights and civil liberties. The strength of our Constitution is in the rights and protections of liberties it affords to individuals.

Question: Do you think this policy violates the Fourth Amendment? Why or why not?

Since I am not a lawyer, I have not studied the legal question. My understanding of the Fourth Amendment is that it prohibits unreasonable search and seizure (to include communications) and, in such cases, requires probable cause that is specific to the person and the circumstance. As a general matter, I believe it is critical to work closely with Congress to ensure our national security programs appropriately balance security with civil rights and civil liberties. The strength of our Constitution is in the rights and protections of liberties it affords to individuals.

Question: Do you agree with the premise advanced by the Eleventh Circuit in *United States v. Touset*² that a smartphone is a physical container indistinguishable from a suitcase?

Since I am not a lawyer, I have not studied the legal question. As a general matter, I believe it is critical we work closely with Congress to ensure our national security programs appropriately balance security with civil rights and civil liberties. The strength of our Constitution is in the rights and protections of liberties it affords to individuals.

Question: Do you think most Americans would accept the premise that searching the contents of a device containing every photo, email, contact, calendar item, appointment, text message, and direct message they have, as well as every Google search, browser visit, navigation search, and note they ever made, along with a detailed history of everywhere they've been—is no different from searching the contents of their toiletry bag or suitcase?

² <https://law.justia.com/cases/federal/appellate-courts/ca11/17-11561/17-11561-2018-05-23.html>

I believe that most Americans would support reasonable searches and seizures that are consistent with the Fourth Amendment of the U.S. Constitution. An example of this would be the searches conducted by TSA for prospective flight travelers.

Question: Do you think that most Americans are aware that forensic searches of their cell phones could yield some 900 pages of information (as was the case in *United States v. Kolsuz*³)? And that to produce this report, their phone may be confiscated by government agents for an entire month, based on nothing more than reasonable suspicion (vs. probable cause)?

Since I am not a lawyer, I have not studied the legal question and I am not familiar with this case. As a general matter, I believe it is critical we work closely with Congress to ensure our national security programs appropriately balance security with civil rights and civil liberties. The strength of our Constitution is in the rights and protections of liberties it affords to individuals.

4. Travelers rely on cell phones to navigate foreign cities, communicate in foreign languages, pay for goods and services, and to keep their families safe while abroad. Federal courts have acknowledged as much; in *U.S. v. Cotterman*, the Ninth Circuit wrote⁴ that it is “impractical, if not impossible, for individuals to make meaningful decisions regarding what digital content to expose to the scrutiny that accompanies international travel”. In *U.S. v. Kolsuz*, the Fourth Circuit wrote⁵ that “it is neither realistic nor reasonable to expect the average traveler to leave his digital devices at home when traveling.”

Question: Given the impracticality of traveling without a cell phone, is abandoning Fourth Amendment protections a *de facto* requirement for international travel under existing DHS border device search policies?

As I mentioned in my answer above, I am not familiar with DHS border search laws and policies, and I do not anticipate exercising oversight over this issue in my role if I am confirmed as the National Cyber Director.

Since I am not a lawyer, I have not studied the legal question. However, I do believe that CBP should consult closely with its attorneys and the Department of Justice, as appropriate, to ensure its programs are implemented consistent with the Constitution and the law.

As a general matter, I believe it is critical we work closely with Congress to ensure our national security programs appropriately balance security with civil rights and civil liberties. The strength of our Constitution is in the rights and protections of liberties it affords to individuals.

³ <https://www.ca4.uscourts.gov/opinions/164687.P.pdf>

⁴ <http://cdn.ca9.uscourts.gov/datastore/opinions/2013/03/08/09-10139.pdf>

⁵ <https://www.ca4.uscourts.gov/opinions/164687.P.pdf>

5. I remain concerned about reported instances of American citizens being detained at points of entry when traveling back into the United States—in particular, the reported instances of Americans being asked by DHS officials to turn over their phones or other digital devices for search, including:
- In 2017, a National Aeronautics and Space Administration (NASA) engineer and U.S. citizen was reportedly pulled into inspection when returning from a vacation in Chile. The individual subjected to inspection recounted how CBP demanded the “PIN” to his phone and handed him a form that explained how CBP had the right to copy the contents of his phone. He recalled that the form indicated that participation in the search was “mandatory” and it threatened “detention and/or seizure” of the device if he did not comply.⁶ He was reportedly released after providing the PIN to his phone—a work phone that was itself property of NASA.⁷
 - Two U.S. citizens were stopped on a return from Canada and held for two hours after their phones were taken by CBP officers. They alleged that they were stopped again on another return trip from Canada three days later in which they were again told to turn over their phones. They also alleged that CBP officers physically took one of the phones in order to search it.⁸
 - An NBC News investigation reported that they examined 25 different cases of U.S. citizens being told to turn over their phones, unlock them, or provide passwords to CBP officers.⁹
 - A U.S. citizen was reportedly stopped from boarding a flight in Los Angeles, handcuffed, and released after “a Homeland Security agent looked through his phone for about 15 minutes.”¹⁰
 - In 2015, a U.S. citizen journalist alleged that, while traveling back to Texas from Brazil, he was detained while officials “went through all his contacts, emails and WhatsApp messages on his phone.”¹¹

Question: If DHS agents lack a warrant, do you believe that it is appropriate that an American citizen, a green card holder, or any other valid visa holder to be delayed or denied entry into the United States if the individual refuses to provide his device’s password, unlock his device, or otherwise provide access to the information on his device? If yes, under what authority, and how does an individual’s citizenship or visa status affect your answer?

⁶ <https://www.theatlantic.com/technology/archive/2017/02/a-nasa-engineer-is-required-to-unlock-his-phone-at-the-border/516489/>

⁷ <http://www.cnn.com/2017/02/13/us/citizen-nasa-engineer-detained-at-border-trnd/>

⁸ <http://www.nbcnews.com/news/us-news/american-citizens-u-s-border-agents-can-search-your-cellphone-n732746>

⁹ *ibid*

¹⁰ <https://www.nytimes.com/2017/02/14/business/border-enforcement-airport-phones.html>

¹¹ https://www.buzzfeed.com/tasneemnashrulla/this-american-journalist-said-he-was-detained-at-miami-airpo?utm_term=.clMvKx0EB#.goOwWgBpZ

As I noted in my answer above, I am not familiar with DHS border search laws and policies, and I do not anticipate the issue coming before the Office of the National Cyber Director.

Since I am not a lawyer, I have not studied the legal question. However, I do believe that CBP should consult closely with its attorneys and the Department of Justice, as appropriate, to ensure its programs are implemented consistent with the Constitution and the law.

As a general matter, I believe it is critical we work closely with Congress to ensure our national security programs appropriately balance security with civil rights and civil liberties. The strength of our Constitution is in the rights and protections of liberties it affords to individuals.

Question: If you believe that DHS has the authority to delay entry in any of these instances, what is the maximum amount of time you believe that the government can delay entry for an American citizen, a green card holder, or any other valid visa holder?

As I noted in my answer above, I am not familiar with DHS border search laws and policies, and I do not anticipate the issue coming before the Office of the National Cyber Director.

As a general matter, I believe it is critical we work closely with Congress to ensure our national security and border security programs appropriately balance security with civil rights and civil liberties. The strength of our Constitution is in the rights and protections of liberties it affords to individuals.

Question: Do you believe that the sharing of information gathered at the border from electronic devices with other federal, state, and local law enforcement is appropriate? What limitations do you believe should exist on sharing information gathered under the border search exception to the Fourth Amendment with other federal, state, and local law enforcement entities?

As I noted in my answer above, I am not familiar with DHS border search laws and policies, and I do not anticipate the issue coming before the Office of the National Cyber Director.

Since I am not a lawyer, I have not studied the legal question. However, I do believe that CBP should consult closely with its attorneys and the Department of Justice, as appropriate, to ensure its programs are implemented consistent with the Constitution and the law.

As a general matter, I believe it is critical we work closely with Congress to ensure our national security programs appropriately balance security with civil rights and civil liberties. The strength of our Constitution is in the rights and protections of liberties it affords to individuals.

6. At the U.S.-Mexico and U.S.-Canada border, DHS personnel have used the so-called border search exception to conduct searches of Americans within 100 miles of a border, without a warrant or even probable cause. These searches are premised on individuals transiting to or from the United States, yet many millions of Americans live and work in these zones and are not transiting into or out of the country.¹² The result is that Americans in large swaths of the country have diminished constitutional rights.

Question: Should the regulations on which this practice is based be updated to more narrowly define this practice?

As I noted in my answer above, I am not familiar with DHS border search laws and policies, and I do not anticipate the issue coming before the Office of the National Cyber Director.

Since I am not a lawyer, I have not studied the legal question. However, I do believe that CBP should consult closely with its attorneys and the Department of Justice, as appropriate, to ensure its programs are implemented consistent with the Constitution and the law.

As a general matter, I believe it is critical we work closely with Congress to ensure our national security programs appropriately balance security with civil rights and civil liberties. The strength of our Constitution is in the rights and protections of liberties it affords to individuals.

Question: Do you believe any geographic limitation exists to where and how DHS personnel may deploy suspicionless checkpoints within the United States?

As I noted in my answer above, I am not familiar with DHS border search laws and policies, and I do not anticipate the issue coming before the Office of the National Cyber Director.

Since I am not a lawyer, I have not studied the legal question. However, I do believe that CBP should consult closely with its attorneys and the Department of Justice, as appropriate, to ensure its programs are implemented consistent with the Constitution and the law.

As a general matter, I believe it is critical we work closely with Congress to ensure our national security programs appropriately balance security with civil rights and civil

¹² <https://www.aclu.org/other/constitution-100-mile-border-zone>

liberties. The strength of our Constitution is in the rights and protections of liberties it affords to individuals.

Question: Do you support the capture of all vehicle information by DHS, including license plates, for vehicles that travel through a DHS checkpoint—including those that have done nothing wrong and are simply driving from Point A to Point B as part of their daily business? If so, what limitations on this practice—including storage of vehicle information—might you support?

As I noted in my answer above, I am not familiar with DHS border search laws and policies, and I do not anticipate the issue coming before the Office of the National Cyber Director.

Since I am not a lawyer, I have not studied the legal question. However, I do believe that CBP should consult closely with its attorneys and the Department of Justice, as appropriate, to ensure its programs are implemented consistent with the Constitution and the law.

As a general matter, I believe it is critical we work closely with Congress to ensure our national security programs appropriately balance security with civil rights and civil liberties. The strength of our Constitution is in the rights and protections of liberties it affords to individuals.

7. On December 21, 2018, the Federal Acquisition Supply Chain Security Act of 2018 was enacted as Title II of P.L. 115-390.¹³ Under the Federal Acquisition Supply Chain Security Act, the Secretary of Homeland Security, the Secretary of Defense, and the Director of National Intelligence are authorized to exclude from procurement or remove from existing systems any information technology or telecommunications equipment that are determined to pose some level of risk to the security of government data.

Question: Would you agree that a potential procurement source that is otherwise qualified to contract with the government should not be excluded from consideration based solely or substantially on the fact of foreign ownership? In other words, do you agree that a company owned by a foreign interest does not *ipso facto* pose a national security threat to the U.S. government supply chain?

While I am not a lawyer, I understand that the law does not authorize the issuance of an exclusion or removal order based solely on the fact of foreign ownership of a potential procurement source that is otherwise qualified to enter into procurement contracts with the federal government.

8. In testimony before the Senate Homeland Security and Government Affairs Committee in October 2018, Federal Bureau of Investigation (FBI) Director Christopher Wray discussed what the FBI describes as the “Going Dark” problem.¹⁴ In short, the FBI does

¹³ <https://www.congress.gov/bills/115th-congress/house-bill/7327>

¹⁴ <https://www.hsgac.senate.gov/imo/media/doc/Testimony-Wray-2018-10-10.pdf>

not want service providers like Google and Apple to offer confidential services because they may hinder efforts by law enforcement to collect and/or analyze private communications. The FBI has suggested that Congress should consider legislation forcing companies to build or enable “backdoor” access to such services; however, backdoors inherently degrade the security of these systems.

On May 15, 2018, Director of the National Counterintelligence and Security Center (NCSC) William Evanina testified¹⁵ that government officials and Members of Congress should avoid potentially “backdoored” services in favor of truly confidential “end-to-end” encrypted services.

Question: Do you support deliberately weakening end-to-end encrypted communications services? If so, how? And if so, for what purposes?

I believe that the overwhelming priority for the U.S. government should be to ensure strong encryption is developed and deployed to ensure the safety and security of U.S. person communications. Access to content under any scheme should be restricted to the Constitutional protections and applicable laws.

Question: Have you at any time ever advocated for deliberately weakening end-to-end encryption as a part of your work at the National Security Agency or the U.S. military?

While I never personally advocated for the deliberate weakening of end-to-end encryption during my service, there were occasions where an organization I served in would consider how to weaken systems used by foreign adversaries for national security purposes. The details of those specific cases are, of necessity, classified and not accessible to me, but were all, to the best of my knowledge, conducted within the scope of the government’s limited authorities with appropriate oversight and legal reviews.

I believe that the overwhelming priority for the U.S. government should be to ensure strong encryption is developed and deployed to ensure the safety and security of U.S. person communications. Any national security activities must be conducted within the scope of the government’s limited authorities with appropriate oversight and legal reviews consistent with the Constitution and law.

Question: Do flaws impacting the confidentiality of popular encryption tools represent a national security threat?

I believe that flaws in any component designed to protect the confidentiality of sensitive information could represent a national security threat.

Question: Do you agree with former NCSC Director Evanina’s assertion that Members of Congress should use services with true end-to-end confidentiality?

¹⁵ <https://www.intelligence.senate.gov/hearings/open-hearing-nomination-william-r-evanina-be-director-national-counterintelligence-and>

I do.

Question: Would you recommend that the U.S. armed forces and government agencies use services with true end-to-end confidentiality?

I would.

Question: Would you recommend that the general public use services with true end-to-end confidentiality?

I would.

Question: If your answers to the previous two questions (“Would you recommend that the U.S. armed forces and government agencies use services with true end-to-end confidentiality?” and “Would you recommend that the general public use services with true end-to-end confidentiality?”) differ – why do they differ?

N/A

Question: Would you recommend that providers work to ensure that cell phones, messaging applications, and other services Americans rely on be “secure by default”?

I would.

9. **Question:** If confirmed, what will you do to insure that any and all intelligence gathered or disseminated by the federal intelligence community will be handled with utmost concern regarding people’s privacy and other rights by all entities that may receive or encounter such information?

The law authorizing the Office of the National Cyber Director includes a rule of construction that nothing within the authorities of the Director or any person acting under the authority of the Director may be construed to interfere with or to direct an intelligence activity, resource, or operation; or to modify the classification of intelligence information. If confirmed, I would ensure compliance with applicable laws and policies pertaining to the use and dissemination of intelligence handled by the Office of the NCD. Moreover, I believe that the intelligence community should be guided by strong privacy and civil liberties protections.

Question: With regard to Fusion Centers, what will you do to ensure the appropriate use of and consistent privacy protections for information shared by them among their partner entities?

The law authorizing the Office of the National Cyber Director includes a rule of construction that nothing within the authorities of the Director or any person acting under the authority of the Director may be construed to interfere with or to direct an intelligence activity, resource, or operation; or to modify the classification of intelligence

information. Notwithstanding, I believe that the Fusion Centers operated by State and local governments should follow appropriate privacy protections. If consulted, I would support efforts by the Department of Homeland Security to provide guidance, training, and resources to Fusion Centers to improve privacy protections.

10. **Question:** If confirmed, what will you do to ensure employees can and will disclose violations of law, rule, or regulation, and instances of fraud, waste, abuse and mismanagement to any or all appropriate sources, including Congress?

I firmly believe in whistleblower protections. If confirmed, I will ensure that whistleblowers do not face retaliation and are protected. I will follow all laws and procedures to ensure whistleblower claims are properly investigated, and direct my staff to ensure they appropriately protect whistleblowers consistent with the law. Moreover, if confirmed, I would welcome the opportunity to work with your staff and the Government Accountability Office to ensure that the Office of the National Cyber Director is being a good steward of American tax dollars.

11. **Question:** As your nomination moves forward, will you commit to providing a written response to any further questions related to your nomination prior to your confirmation vote?

I do.



The Honorable Gary Peters
Chairman, Senate Committee on Homeland
Security and Governmental Affairs
340 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Robert Portman
Ranking Member, Senate Committee on
Homeland Security and Governmental Affairs
340 Dirksen Senate Office Building
Washington, DC 20510

May 27, 2021

RE: Upcoming Confirmation Hearing for Chris Inglis as National Cyber Director

Dear Chairman Peters and Ranking Member Portman,

On behalf of the Analysis and Resilience Center for Systemic Risk (ARC), I am writing to express our support for Chris Inglis as the National Cyber Director. ARC members are owners and operators of infrastructure formally designated by the Department of Homeland Security under Section 9 of Executive Order 13636 as systems where a cybersecurity incident could have catastrophic effects on economic and national security.

These "Section 9" firms founded the ARC as a non-profit, cross-sector organization to work with each other and with the U.S. Government to mitigate systemic risk to designated infrastructure. The ARC partners with many agencies across the U.S. Government and the Intelligence Community and we look forward to working with Chris Inglis as the nation's first National Cyber Director.

Mr. Inglis' long experience at the National Security Administration, his personal credibility as a nuanced thinker on intelligence matters, and his openness to the possibilities of deeper public-private collaboration make him the ideal choice to serve as National Cyber Director. As a member of the Cyberspace Solarium Commission, Mr. Inglis brings firsthand knowledge of the bipartisan, public-private intent of adding the National Cyber Director as a principal adviser to the President on cybersecurity policy and strategy. The ARC is confident that he will quickly integrate this new position and its associated staff into the government's cybersecurity capability with demonstrable results for the security of critical assets in the private sector.

Today's cyber threat environment requires a leader who can collaborate across the myriad law enforcement, intelligence, and military agency authorities, to bring whole-of-nation capability to bear on cyber threats. We urge the Senate Homeland Security and Governmental Affairs Committee to support Chris Inglis' nomination by recommending him for Senate Confirmation.

Sincerely,

A handwritten signature in black ink, appearing to read "Scott DePasquale", with a stylized flourish extending to the right.

Scott DePasquale, President and CEO
The Analysis and Resilience Center for Systemic Risk

CHAMBER OF COMMERCE
OF THE
UNITED STATES OF AMERICA

CHRISTOPHER D. ROBERTI
SENIOR VICE PRESIDENT,
CYBER, INTELLIGENCE, AND
SECURITY POLICY

1615 H STREET, NW
WASHINGTON, DC 20062
(202) 463-5449
CROBERTI@USCHAMBER.COM

June 8, 2021

The Honorable Gary Peters
Chair
Committee on Homeland Security and
Governmental Affairs
United States Senate
Washington, DC 20510

The Honorable Rob Portman
Ranking Member
Committee on Homeland Security and
Governmental Affairs
United States Senate
Washington, DC 20510

Dear Chairman Peters and Ranking Member Portman:

The U.S. Chamber of Commerce strongly supports the nomination of John C. ("Chris") Inglis to be the first National Cyber Director. Mr. Inglis is the right choice at this critical time for America's cybersecurity.

Mr. Inglis has extensive experience in government. In his 28-year career at the National Security Agency (NSA), he served as Deputy Director and Chief Operating Officer, the NSA's highest civilian position. While at NSA, he developed significant interagency experience and deep relationships with senior U.S. government leaders, Members of Congress, the U.S. business community, and essential foreign partners and allies.

Following his retirement from NSA, Chris remained dedicated to improving America's cybersecurity. He is the inaugural Distinguished Visiting Professor for Cyber Studies at the U.S. Naval Academy, and he has a unique understanding of the cybersecurity challenges that American businesses face. He understands and appreciates the necessary collaboration between government and the private sector to enhance America's national and economic security and create an environment of collective defense.

Mr. Inglis also played a pivotal role as Commissioner on the bipartisan U.S. Cyberspace Solarium Commission. In this role, he engaged with various stakeholders, including the business community, to ensure robust dialogue throughout the process. The fiscal year 2021 National Defense Authorization Act includes many of the Commission's recommendations and could be considered the most comprehensive U.S. cyber legislation to date. This body of work will be vital as the Office of the National Cyber Director executes its mandate to update the U.S. national cyber strategy.

Mr. Inglis has a distinguished record of service and demonstrates exceptional operational, strategic, policy, and political skills that would serve him well as the first National Cyber Director.

Sincerely,



Christopher D. Roberti

cc: Members of the Senate Committee on Homeland Security and Governmental Affairs
Members of the Senate Armed Services Committee



June 8, 2021

To: Senator Gary Peters (MI), Chairman of the U.S. Senate Committee on Homeland Security and Governmental Affairs

Senator Rob Portman (OH), Ranking Member of the U.S. Senate Committee on Homeland Security and Governmental Affairs

Subject: Support of John "Chris" Inglis's Nomination for National Cyber Director and Jen Easterly's Nomination for Director of the Cybersecurity and Infrastructure Security Agency

As Chair of the Financial Services Sector Coordinating Council (FSSCC)*, I want to offer my strong support for the nomination of John "Chris" Inglis to be the first National Cyber Director. The position of National Cyber Director (NCD) created by Congress under the National Defense Authorization Act for Fiscal Year 2021 is very important to the FSSCC and the entire financial services industry, as the NCD will advise the President, National Security Council, Homeland Security Council and relevant federal departments/agencies on national cybersecurity policy and strategy, coordinate the implementation of national cybersecurity policy and strategy, and coordinate and consult with the private sector on cybersecurity issues.

Mr. Inglis's background in national security, computer science and the financial services industry (one of the 16 critical infrastructure sectors) makes him uniquely qualified to serve as NCD. As Deputy Director and senior civilian leader at the National Security Agency, Mr. Inglis was responsible for guiding and directing the NSA's strategies, operations and policy, providing him with operational experience that is easily transferable to the NCD's task of implementing the necessary policies and strategies to improve our nation's cybersecurity. Mr. Inglis began his career at the NSA as a computer scientist within the National Computer Security Center through which he gained a solid technical background essential for understanding the complex cybersecurity challenges that the NCD will be charged with addressing. Mr. Inglis has gained valuable knowledge of the cybersecurity threats specific to the financial services sector as a Director on the Board of Huntington Bank and in his current role as Managing Director of the Paladin Capital Group. He also has extensive leadership experience important to the role of NCD from his thirty years of military service, including serving as Brigadier General in the Air National Guard.

As Chair of the FSSCC, I also support the mission of the Cybersecurity and Infrastructure Security Agency (CISA) and the nomination of Jen Easterly for the role of CISA Director. The FSSCC, as well as the entire financial services sector, has a significant interest in the valuable work of CISA from a security, resiliency and critical infrastructure perspective.

Ms. Easterly's combination of national security and financial services industry experience will be extremely useful in understanding how CISA can further develop public sector/private industry collaboration. Her experience helping to create the United States Cyber Command will be important to advancing CISA's mission within the federal government and amongst important allies in law enforcement and the intelligence community, uniquely positioning her to be effective in the role of CISA Director. Her international background (including tours of duty in Haiti, the Balkans, Iraq, and Afghanistan with U.S. Army intelligence and cybersecurity) and membership in the Aspen Global Leadership Network provide her

Public



with a global and strategic view on the complex global challenges confronting the financial industry. Ms. Easterly is currently a Managing Director of Morgan Stanley and Global Head of the Firm's Cybersecurity Fusion Center, providing her with an understanding of current threats being faced by the financial services industry and our nation, which is invaluable for the CISA Director role.

Ms. Easterly's cybersecurity expertise gained in both the public and private sectors and her substantial leadership experience make her an excellent candidate to lead CISA.

As both Mr. Inglis and Ms. Easterly are active participants in the financial services sector, I am confident that their appointment to serve in the roles of NCD and CISA Director, respectively, will be of great benefit to the security of our nation. Specifically, the leadership experience of both Mr. Inglis and Ms. Easterly will be extremely valuable in the implementation of the President's recent Executive Order on Improving the Nation's Cybersecurity.

Thank you for your consideration of this support of Chris Inglis's nomination to be National Cyber Director and Jen Easterly's nomination to be Director of CISA.

Sincerely,

A handwritten signature in black ink, appearing to read 'Ron Green', is written over a light blue horizontal line.

Ron Green, Chair
Financial Services Sector Coordinating Council (FSSCC)

** The Financial Services Sector Coordinating Council is operated by the nation's financial services companies and industry associations to coordinate policy that enhances the security and resiliency of the United States financial system. The FSSCC proactively promotes an all-hazards approach to drive preparedness through its collaboration with the U.S. Government for the benefit of consumers, the financial services sector, and the national economy. The Department of Homeland Security recognizes the FSSCC as a member of the Critical Infrastructure Partnership Advisory Council on behalf of the banking and finance sector.*



Mission Needs* (1 of 6)



*Draft list as supplied by ME&T 28-March 2019

UNCLASSIFIED//FOUO

CISA Response to HSGAC April 5, 2021 Letter
Not for Further Dissemination or Public Release

4

CISA_000397

GARY C. PETERS, MICHIGAN, CHAIRMAN
 THOMAS R. CARPER, DELAWARE
 MAGGIE HASSAN, NEW HAMPSHIRE
 KYRSTEN SINEMA, ARIZONA
 JACKY FROEN, NEVADA
 ALEC PADILLA, CALIFORNIA
 JON OSOFF, GEORGIA
 ROB PORTMAN, OHIO
 RON JOHNSON, WISCONSIN
 RANDI PAUL, KENTUCKY
 JAMES LANKFORD, OKLAHOMA
 MITT ROONEY, UTAH
 ROX SCOTT, FLORIDA
 JOSH HAWLEY, MISSOURI

DAVID M. WEINBERG, STAFF DIRECTOR
 PAMELA THIESSEN, MINORITY STAFF DIRECTOR
 LAURA W. KUBRIDE, CHIEF CLERK

United States Senate
 COMMITTEE ON
 HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
 WASHINGTON, DC 20510-6250

April 5, 2021

Mr. Brandon Wales
 Acting Director, Cybersecurity & Infrastructure Security Agency
 Department of Homeland Security
 Washington, D.C. 20528

Dear Mr. Wales:

Thank you for your recent testimony before the Committee on Homeland Security and Governmental Affairs as part of the Committee's investigation into the SolarWinds Orion hack, Microsoft Exchange server hacks, and other recent cyberattacks. A recent report has raised the troubling possibility that the Department of Homeland Security (DHS or the Department) did not fully report the extent of the SolarWinds breach to Congress.¹

As our hearing highlighted, there is no easy solution to advanced persistent cyber threats. Time and again this Committee has discussed the challenges of defending against sophisticated, well-resourced, and patient cyber adversaries.² Nevertheless, the fact remains that despite significant investments in cyber defenses, the federal government did not initially detect this cyberattack. We appreciate your testimony on this issue, along with that of your colleagues, raising important questions about our national and federal cybersecurity strategy.

A layered and holistic federal cybersecurity strategy is key to a comprehensive federal cyber deterrence and defense capability. An effective federal cybersecurity strategy will need to reevaluate core assumptions and consider new solutions and approaches to cybersecurity. For example, it may be appropriate to assume some level of compromise within networks and implement a zero-trust network architecture, improve protection at end points complemented by heuristic and behavior-based detection capabilities, and regularly deploy hunt teams to seek out malicious actors. Mitigating vulnerabilities and reducing legacy information technology that serve as open doors to malicious hackers is also important. So will be deterrence efforts that create real-world consequences for cyber-attacks against the United States—investigation,

¹ Alan Suderman, ASSOCIATED PRESS, *AP sources: SolarWinds hack got emails of top DHS officials* (March 29, 2021), available at <https://apnews.com/article/rob-portman-hacking-email-russia-8bcd4a4cb3be1f8f98244766bae70395>.

² E.g., *Under Attack: Cybersecurity & the OPM Data Breach: Hearing Before the S. Comm. on Homeland Security & Governmental Affairs*, S. Hrg. 114-449 (June 25, 2015) (Statement of Dr. Andy Ozment, Ass't Secretary for Cybersecurity & Communications, Dep't of Homeland Security); SEN. TOM COBURN, RANKING MEMBER, S. COMM. ON HOMELAND SECURITY & GOVERNMENTAL AFFAIRS, A REVIEW OF THE DEPARTMENT OF HOMELAND SECURITY'S MISSIONS AND PERFORMANCE 97 (Dec. 2015) (quoting Suzanne E. Spaulding, former Under Secretary of National Protection & Programs, Dep't of Homeland Security, "The promise of an impervious cybersecurity shield protecting vast amounts of information from a determined and sophisticated adversary is at best a distant dream, and at worst a dangerous myth.").

Mr. Brandon Wales
 April 5, 2021
 Page 2

attribution, prosecution, and sanctions. At the national level, our cybersecurity strategy will require careful consideration of the appropriate role of the federal government, companies, and citizens in cyber defense, especially when it comes to nation-state actors with near unlimited resources and time.

Our hearing also revealed key limitations of the EINSTEIN intrusion detection and intrusion prevention system. EINSTEIN is a signature-based intrusion detection and prevention system that sits on the perimeter of civilian federal agencies' computer networks.³ As you alluded to in your testimony, network perimeters are increasingly irrelevant with modern information technology infrastructure that emphasizes end-to-end encryption and reliance on cloud service providers outside of an organization's network; these technologies represent an inherent limitation of perimeter-based intrusion detection systems like EINSTEIN.⁴ Additionally, signature-based intrusion detection and intrusion prevention systems are largely limited to detecting previously seen threats—they are ineffective at identifying or blocking sophisticated and novel attacks like the SolarWinds hack. As this Committee warned nearly five years ago, "Current reliance on decades old signature-based detection technology limits the effectiveness of EINSTEIN against advanced persistent threats."⁵

The authorization for DHS to operate EINSTEIN lapses on December 18, 2022 and we look forward to working with you to determine whether and how to reauthorize the program to address these limitations and, more broadly, how to defend better against advanced persistent cyber threats. To assist us in this investigation and these policy considerations, please provide unredacted copies of the following documents no later than 5:00 p.m. on April 20, 2021:

1. Documents sufficient to show the specific information systems compromised at federal agencies shared with CISA in regards to the SolarWinds and MS Exchange cyberattacks or that may have been captured by EINSTEIN in the past six months, including the names of the individuals whose accounts or systems were compromised or targeted if at the SES, ES, or equivalent level; and the agencies and programs with which those individuals and systems were associated, to the greatest level of detail possible.
2. The Department's current cybersecurity strategy and implementation plan⁶ and intrusion assessment plan.⁷

³ S. Rept. 114-378.

⁴ E.g., NAT'L INST. OF STANDARDS & TECHNOLOGY, NAT'L CYBERSECURITY CENTER OF EXCELLENCE, ZERO TRUST ARCHITECTURE, <https://www.nccoe.nist.gov/projects/building-blocks/zero-trust-architecture> ("The proliferation of cloud computing, mobile device use, and the Internet of Things has dissolved traditional network boundaries. Hardened network perimeters alone are no longer effective for providing enterprise security in a world of increasingly sophisticated threats.").

⁵ S. Rept. 114-378.

⁶ Homeland Security Act of 2002 § 2211(a), (d).

⁷ Homeland Security Act of 2002 § 2210(b)(1).

Mr. Brandon Wales
 April 5, 2021
 Page 3

3. Documents sufficient to show the current and planned technical capabilities of EINSTEIN 1 (E1); EINSTEIN 2 (E2); EINSTEIN 3 Accelerated (E3A); and Enhanced Cybersecurity Services, including any improvements, new technologies, modification of existing technologies, advanced protective technologies, or detection technologies beyond signature based detection planned, acquired, tested, evaluated, piloted, or deployed on the EINSTEIN platform.⁸
4. All reports, evaluations, studies, or reviews related to EINSTEIN classified indicators, including the assessment CISA performed in 2020 on the efficacy of utilizing classified indicators and any update since the publication of that study.
5. All classified indicators in use on E3A as of the date of this letter as well as any contextual information DHS has regarding those indicators.
6. Documents sufficient to show the current and planned technical capabilities of the Continuous Diagnostics and Mitigation (CDM) program including advanced network security tools to improve visibility of network activity and to detect and to mitigate intrusions and anomalous activity,⁹ and the current plan to ensure that each agency utilizes advanced networks security tools as part of the CDM program.¹⁰
7. The performance work statement for each CDM integrator including for each: documents sufficient to show whether the contract is fixed price or cost based and incentives and awards.
8. Operations and spending plans for the National Cybersecurity Protection System and for the CDM program to the greatest level of detail possible for the each of the past five fiscal years.

The Committee is authorized by Rule XXV of the Standing Rules of the Senate and S. Res. 70 “to investigate the efficiency and economy of operations of all branches of the Government . . .” and is the primary Committee of jurisdiction in the United States Senate for federal cybersecurity.

Many of the documents requested should be readily available to the Department. As such, please begin production of documents as soon as possible and do not delay productions for the purpose of including a cover letter. We request a letter only at the conclusion of the production to certify completeness. Classified information should be provided under separate cover via the Office of Senate Security. Additionally, we request CISA provide briefings to discuss its cybersecurity programs and the documents provided, after providing those documents.

⁸ Homeland Security Act of 2002 §§ 2312(b)(4)–(5), 2313(b)(2).


⁹ Federal Cybersecurity Enhancement Act of 2015 § 224(a).


¹⁰ Federal Cybersecurity Enhancement Act of 2015 § 224(b).

Mr. Brandon Wales
April 5, 2021
Page 4

Thank you for your prompt attention and cooperation in this matter. These documents and information will help us in considering potential reauthorization language for the National Cybersecurity Protection System. If you have any questions about this request, please contact Christopher Mulkins at (202) 228-1346 for Chairman Peters and Liam McKenna at (202) 228-0079 for Ranking Member Portman.

Sincerely,



Gary C. Peters
Chairman

Rob Portman
Ranking Member

GARY C. PETERS, MICHIGAN, CHAIRMAN
 THOMAS R. CARPER, DELAWARE
 MAGGIE HASSAN, NEW HAMPSHIRE
 KYRSTEN SINEMA, ARIZONA
 JACKY ROSEN, NEVADA
 ALEX PADILLA, CALIFORNIA
 JON OSOFF, GEORGIA
 ROB PORTMAN, OHIO
 RON JOHNSON, WISCONSIN
 RANDI PAUL, KENTUCKY
 JAMES LANKFORD, OKLAHOMA
 MITT ROONEY, UTAH
 RICK SCOTT, FLORIDA
 JOE HAWLEY, MISSOURI

DAVID M. WEINBERG, STAFF DIRECTOR
 PAMELA THRESEN, MINORITY STAFF DIRECTOR
 LAURA W. KILBRIDE, CHIEF CLERK

United States Senate
 COMMITTEE ON
 HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
 WASHINGTON, DC 20510-6250

April 5, 2021

Mr. Christopher DeRusha
 Federal Chief Information Security Officer
 Office of Management & Budget
 Washington, D.C. 20500

Dear Mr. DeRusha:

Thank you for your recent testimony before the Committee on Homeland Security and Governmental Affairs as part of the Committee's investigation into the SolarWinds Orion hack, Microsoft Exchange server hacks, and other recent cyberattacks. A recent report has raised the troubling possibility that some federal agencies did not fully report the extent of the SolarWinds breach to Congress.¹

As our hearing highlighted, there is no easy solution to advanced persistent cyber threats. Time and again this Committee has discussed the challenges of defending against sophisticated, well-resourced, and patient cyber adversaries.² Nevertheless, the fact remains that despite significant investments in cyber defenses, the federal government did not initially detect this cyberattack. We appreciate your testimony on this issue, along with that of your colleagues, raising important questions about our national and federal cybersecurity strategy.

A layered and holistic federal cybersecurity strategy is key to a comprehensive federal cyber deterrence and defense capability. An effective federal cybersecurity strategy will need to reevaluate core assumptions and consider new solutions and approaches to cybersecurity. For example, it may be appropriate to assume some level of compromise within networks and implement a zero-trust network architecture, improve protection at end points complemented by heuristic and behavior-based detection capabilities, and regularly deploy hunt teams to seek out malicious actors. Mitigating vulnerabilities and reducing legacy information technology that serve as open doors to malicious hackers is also important. So will be deterrence efforts that create real-world consequences for cyber-attacks against the United States—investigation,

¹ Alan Suderman, ASSOCIATED PRESS, *AP sources: SolarWinds hack got emails of top DHS officials* (March 29, 2021), available at <https://apnews.com/article/rob-portman-hacking-email-russia-8bcd4a4cb3be1f8f98244766bae70395>.

² E.g., *Under Attack: Cybersecurity & the OPM Data Breach: Hearing Before the S. Comm. on Homeland Security & Governmental Affairs*, S. Hrg. 114-449 (June 25, 2015) (Statement of Dr. Andy Ozment, Ass't Secretary for Cybersecurity & Communications, Dep't of Homeland Security); SEN. TOM COBURN, RANKING MEMBER, S. COMM. ON HOMELAND SECURITY & GOVERNMENTAL AFFAIRS, *A REVIEW OF THE DEPARTMENT OF HOMELAND SECURITY'S MISSIONS AND PERFORMANCE* 97 (Dec. 2015) (quoting Suzanne E. Spaulding, former Under Secretary of National Protection & Programs, Dep't of Homeland Security, "The promise of an impervious cybersecurity shield protecting vast amounts of information from a determined and sophisticated adversary is at best a distant dream, and at worst a dangerous myth").

Mr. Christopher DeRusha
 April 5 2021
 Page 2

attribution, prosecution, and sanctions. At the national level, our cybersecurity strategy will require careful consideration of the appropriate role of the federal government, companies, and citizens in cyber defense, especially when it comes to nation-state actors with near unlimited resources and time.

Also important to our federal cybersecurity strategy is defined structures for inter-agency coordination on incident response. At our hearing, we discussed the numerous entities with potentially overlapping responsibilities related to federal cybersecurity. It is important that there be a single point of accountability for leading response efforts to prevent confusion and duplication. We are concerned this level of accountability is currently lacking.

We look forward to working with the Administration on needed improvements to the Federal Information Security Modernization Act of 2014, and other legislative improvements to defend better against advanced persistent cyber threats. To assist us in this investigation and these policy considerations, please provide unredacted copies of the following documents no later than 5:00 p.m., April 20, 2021:

1. The current federal cybersecurity strategy and any associated implementation plan(s) and a description of any plan to update the strategy or plan(s).
2. A list of roles and responsibilities for federal cybersecurity including an assessment of how these defined roles prevent duplicative efforts and facilitated the federal government's response to the SolarWinds attack.
3. Documents sufficient to show the specific information systems compromised or targeted at federal agencies in the SolarWinds Orion attack and Microsoft Exchange attacks; the names of the individuals whose accounts or systems were compromised or targeted if at the SES, ES, or equivalent level; and the agencies, programs, and teams with which those individuals and systems were associated, to the greatest level of detail possible.
4. Documents sufficient to show current and planned metrics used to measure security in accordance with section 3554 of title 44, United States Code.
5. Cyberscope data received for each department or agency for FY 2020.

The Committee is authorized by Rule XXV of the Standing Rules of the Senate and S. Res. 70 to investigate "the efficiency and economy of all branches of the Government . . ." and is the primary Committee of jurisdiction in the United States Senate for federal cybersecurity.


Many of the documents requested should be readily available to the Department. As such, please begin production of documents immediately and do not delay productions for the purpose of including a cover letter. We request a letter only at the conclusion of the production to certify completeness. Classified information should be provided under separate cover via the Office of Senate Security. Additionally, we request your office provide a briefing to discuss the documents provided, after providing those documents.

Mr. Christopher DeRusha
April 5 2021
Page 3

Thank you for your prompt attention and cooperation in this matter. These documents and information will help the Committee in considering potential legislation to improve federal cybersecurity, including reforms to the Federal Information Security Modernization Act of 2014. If you have any questions about this request, please contact Christopher Mulkins at (202) 228-1346 for Chairman Peters and Liam McKenna at (202) 228-0079 for Ranking Member Portman.

Sincerely,



Gary C. Peters
Chairman

Rob Portman
Ranking Member