

**NOMINATION OF CHRISTOPHER C. KREBS  
TO BE UNDER SECRETARY, NATIONAL  
PROTECTION AND PROGRAMS DIRECTORATE,  
U.S. DEPARTMENT OF HOMELAND SECURITY**

---

**HEARING**

BEFORE THE

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

SECOND SESSION

---

NOMINATION OF CHRISTOPHER C. KREBS TO BE UNDER SECRETARY,  
NATIONAL PROTECTION AND PROGRAMS DIRECTORATE,  
U.S. DEPARTMENT OF HOMELAND SECURITY

---

APRIL 25, 2018

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

32-455 PDF

WASHINGTON : 2019

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

RON JOHNSON, Wisconsin, *Chairman*

JOHN MCCAIN, Arizona

ROB PORTMAN, Ohio

RAND PAUL, Kentucky

JAMES LANKFORD, Oklahoma

MICHAEL B. ENZI, Wyoming

JOHN HOEVEN, North Dakota

STEVE DAINES, Montana

CLAIRE McCASKILL, Missouri

THOMAS R. CARPER, Delaware

HEIDI HEITKAMP, North Dakota

GARY C. PETERS, Michigan

MAGGIE HASSAN, New Hampshire

KAMALA D. HARRIS, California

DOUG JONES, Alabama

CHRISTOPHER R. HIXON, *Staff Director*

GABRIELLE D'ADAMO SINGER, *Chief Counsel*

DAVID N. BREWER, *Chief Investigative Counsel*

MICHELLE D. WOODS, *Senior Professional Staff Member*

MARGARET E. DAUM, *Minority Staff Director*

DONALD K. SHERMAN, *Minority Senior Counsel*

JULIE G. KLEIN, *Minority Professional Staff Member*

JOEL F. WALSH, *Minority Professional Staff Member*

LAURA W. KILBRIDE, *Chief Clerk*

BONNI E. DINERSTEIN, *Hearing Clerk*

# CONTENTS

Opening statements:	Page
Senator Johnson .....	1
Senator Heitkamp .....	2
Senator McCaskill .....	5
Senator Harris .....	9
Senator Peters .....	14
Senator Hassan .....	17
Senator Lankford .....	18
Prepared statements:	
Senator Johnson .....	27
Senator McCaskill .....	29

## WITNESSES

WEDNESDAY, APRIL 25, 2018

Christopher C. Krebs, to be Under Secretary, National Protection and Programs Directorate, U.S. Department of Homeland Security	
Testimony .....	3
Prepared statement .....	32
Biographical and financial information .....	34
Letter from the Office of Government Ethics .....	51
Responses to pre-hearing questions .....	54
Responses to post-hearing questions .....	104
Letters of Support .....	123



**NOMINATIONS OF CHRISTOPHER C. KREBS  
TO BE UNDER SECRETARY, NATIONAL  
PROTECTION AND PROGRAMS DIRECTORATE,  
U.S. DEPARTMENT OF HOMELAND SECURITY**

WEDNESDAY, APRIL 25, 2018

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

The Committee met, pursuant to notice, at 3:05 p.m., in room SD-342, Dirksen Senate Office Building, Hon. Ron Johnson, Chairman of the Committee, presiding.

Present: Senators Johnson, Lankford, McCaskill, Carper, Heitkamp, Peters, Hassan, Harris, and Daines.

**OPENING STATEMENT OF CHAIRMAN JOHNSON**

Chairman JOHNSON. This hearing will come to order.

Today we are holding this hearing to consider the nomination of Christopher C. Krebs to be the Under Secretary for the National Protection and Programs Directorate (NPPD), Department of Homeland Security (DHS). I think we are all hoping that that will soon be named the “Cybersecurity and Infrastructure Security Agency” (CISA). Maybe this will be the last time we ever hold a confirmation hearing for that Directorate’s confirmation.

I do not have a whole lot to say in terms of an opening statement. We had a really good hearing yesterday. Jeanette Manfra from the Office of Cybersecurity and Communications testified yesterday, and I think we really laid out the issues and asked a lot of good questions.

I would ask that my written statement, be entered into the record.<sup>1</sup>

I also want to enter into the record eight letters we have received in support<sup>2</sup> of Mr. Krebs signed by 58 different individuals, and it is a broad range of people from former DHS officials, Central Intelligence Agency (CIA), Federal Emergency Management Agency (FEMA), U.S. Customs and Border Protection (CBP), Department of Treasury, National Institute of Standards and Technology (NIST), the Department of Defense (DOD), National Security Agency (NSA), National Security Council (NSC). I think you get the drift.

<sup>1</sup> The prepared statement of Senator Johnson appears in the Appendix on page 27.

<sup>2</sup> The letters referenced by Senator Johnson appears in the Appendix on page 123.

There seems to be a fair amount of support for this nomination. It is obviously an enormously important position. What was underscored in yesterday's hearing are the threats we face are real; they are pervasive; they are growing. And as much as we have improved our defenses, folks on offense are not standing still either. So we still have that gap between offense and defense, and this is going to affect every part of our economy. It affects every nation in the world. In some respects, it can be an existential threat to this Nation.

So the responsibilities of the Under Secretary are enormous, and we certainly want to thank you, Mr. Krebs, for your willingness to serve again. We want to thank your beautiful family, and we hope you introduce them in your opening comments. This is a full-time job, and you are going to be devoting a lot of time. You will be having a lot of time away from your beautiful family. So this is a whole family sacrifice, and we really do appreciate your willingness to allow Christopher to serve in this capacity.

So, with that, it is the tradition of this Committee to swear in witnesses, so if you will please stand and raise your right hand. 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?

Mr. KREBS. I do.

Chairman JOHNSON. Please be seated.

Senator Heitkamp, in the absence of Senator McCaskill, do you have a couple comments you would like to make?

#### **OPENING STATEMENT OF SENATOR HEITKAMP**

Senator HEITKAMP. This is a division that I think has been misnamed, and I would not say mismanaged but lacking focus. And I can only say from the hearing we had yesterday and reading your resume and the support, thank you for applying. Thank you for being willing to serve. This is an area where clearly people from this sector could command a lot of money in the private sector, and the willingness that you have exhibited to come to Washington and to be part of doing this for the entire country, it is a patriotic act, and I want to thank you.

We are really excited to hear your testimony, but I cannot speak for the rest of my colleagues on this Committee. I am excited to get you confirmed and get you to work so we can continue the discussion that we started yesterday.

Thank you, Mr. Chairman, and good luck.

Chairman JOHNSON. There is no doubt about it, we are very fortunate to have such a qualified candidate.

So, with that, Mr. Krebs, why do you not start your testimony?

**TESTIMONY OF CHRISTOPHER C. KREBS TO BE UNDER SECRETARY,<sup>1</sup> NATIONAL PROTECTION AND PROGRAMS DIRECTORATE, U.S. DEPARTMENT OF HOMELAND SECURITY**

Mr. KREBS. Chairman Johnson, Ranking Member McCaskill, and Members of the Committee, thank you for the opportunity to appear before you today as the President's nominee for Under Secretary of Homeland Security for the National Protection and Programs Directorate. I am honored to have been nominated for this position by President Trump, and I am grateful to have Secretary Nielsen's support.

More than anything else, I am especially grateful for the strong support of my family, and I would like to recognize those who have joined us today.

First, I would like to thank my parents, Van and Fran, for providing me the opportunities in life to succeed; my brothers who could not join us today, William and Davis, for keeping me honest, but also helping me develop my partnership-building skills; and my father-in-law, Dave, and mother-in-law, Patrice, for being there for me, my wife, and often as baby sitters for our children. Those kids are here today. We have Henry, Anna, Charlie—I think Jack had to step out.

Chairman JOHNSON. He is under wraps.

Mr. KREBS. Then the fifth is going to join us later this year. [Laughter.]

Chairman JOHNSON. Was that a new announcement?

Mr. KREBS. Yes.

Chairman JOHNSON. Congratulations.

Mr. KREBS. Thank you. They do keep me grounded——

Senator HEITKAMP. You missed your parents' response. [Laughter.]

Chairman JOHNSON. This is a Committee first, at least under my chairmanship, so thanks.

Mr. KREBS. Good start. They do keep me grounded, and I come to work every day to make the world a better, safer place for their future.

Last, but certainly not least, I would like to recognize my wife, Emily. Without her support, her patience, her strength, and her love, I would not be here today.

I would also like to give thanks to my friends, my coworkers old and new, and everyone else who has supported me on this journey. I am humbled to have their support. And those letters you mentioned, I am humbled to have the support of that community.

I am fortunate to have served at DHS in several capacities. Currently I serve as both the Assistant Secretary for Infrastructure Protection as well as the Senior Official Performing the Duties of the Under Secretary (SOPDUS) at NPPD, two names I would like to retire. I have dedicated my career to risk management and critical infrastructure protection in both government and the private sector. I am passionate about this mission, and if confirmed, it will be my honor to lead the Department's cyber and infrastructure security mission.

<sup>1</sup> The prepared statement of Mr. Krebs appears in the Appendix on page 32.

This context is important. In our nomination discussions, many of you asked what drew me to this job. The answer is simple: I view this position as the pinnacle of national risk management in cyber and physical infrastructure. We can do more to advance a national risk management agenda than any other single place in the U.S. Government. And since no single stakeholder has all the information necessary to detect or comprehensively manage systemic risk, NPPD's information-sharing and coordination role and ability to engage policy- and decisionmakers are essential to success in our shared homeland security mission.

Success in this mission cannot be possible without the tireless work of NPPD's incredibly talented workforce. While serving as the senior official, I have sought to place the employees first by creating a team-oriented culture, ensuring a diverse and inclusive environment, and helping good ideas rise to the top. If confirmed, I will continue to tirelessly represent the men and women of NPPD; increase the visibility of our mission and organization; and assertively engage leadership, industry, Congress, and our other stakeholders on their behalf.

NPPD's responsibilities have grown substantially since its inception, driven by a dramatic shift in the threat environment few could have anticipated 10 years ago. Today we face the challenge of managing risk in both the physical and digital worlds. This risk comes from Mother Nature; a diverse group of threat actors including nation-states like Russia, China, Iran, and North Korea; as well as cyber criminals, terrorist groups, and others. We must do everything we can to mitigate these threats and enhance the resilience of our infrastructure.

I see three primary strategic goals for NPPD. First, we must defend civilian networks and secure Federal facilities. Second, we must help manage systemic risk to national critical functions. And, third, we must raise the security baseline by providing stakeholders with the tools and resources they need to secure infrastructure. We must foster voluntary, incentive-driven partnerships with a wide range of stakeholders. If confirmed, I will draw on my private sector experience and understanding of government's unique value to ensure our approach is customer-centric and requirements-driven.

Operationally, one of my top priorities at NPPD has been enhancing the resilience of our Nation's election systems. In the face of unprecedented Russian interference in our 2016 election, NPPD has worked closely with State and local election officials across the country to ensure each American's vote counts and is counted correctly. If confirmed, I will continue to make this my top priority.

I will also work closely with Congress to facilitate oversight of NPPD's activities and advance shared legislative priorities, including restructuring NPPD, enhancing election system security, reauthorizing the Chemical Facility Anti-Terrorism Standards (CFATS) program, hardening infrastructure against threats like electromagnetic pulse (EMP) and others.

I want to thank this Committee for including legislation transforming NPPD into the Cybersecurity and Infrastructure Security Agency in the recent DHS authorization bill. I look forward to working with this Committee to pass that critical legislation.



Thank you again for the opportunity to appear before you today, and I look forward to answering your questions.

Chairman JOHNSON. Thank you, Mr. Krebs.

As we ad libbed the opening here, I forgot to introduce you, so I will do that now before I ask our three questions.

Mr. Christopher Krebs is currently serving as the Assistant Secretary for the Office of Infrastructure Protection for the National Protection and Programs Directorate in the Department of Homeland Security and is concurrently filling the role as the Senior Official Performing the Duties of the Under Secretary of the NPPD. That is as long a title as I have ever read.

Prior to joining DHS, Mr. Krebs was the director of cybersecurity policy for Microsoft, leading their work on cybersecurity and technology issues. Mr. Krebs previously served in DHS as a Senior Adviser to the Assistant Secretary for Infrastructure Protection, where he helped establish a number of national and international risk management programs.

Again, I could not be more pleased we have a person of such caliber and experience willing to serve our Nation in this capacity.

There are three questions the Committee asks of every nominee for the record.

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?

Mr. KREBS. No, Mr. Chairman.

Chairman JOHNSON. 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?

Mr. KREBS. No, sir.

Chairman JOHNSON. And, finally, 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?

Mr. KREBS. I do. And if I may caveat the first answer on the conflicts of interest, I have consulted with Ethics Counsel, and I will recuse myself for the next 11 months from any particular matters involving Microsoft or the National Cybersecurity Alliance.

Chairman JOHNSON. OK. That is noted for the record.

I will defer my questions out of respect for other Members' time here, so, Senator McCaskill?

#### **OPENING STATEMENT OF SENATOR MCCASKILL<sup>1</sup>**

Senator MCCASKILL. Thank you. I want to apologize to you, Mr. Krebs, for not being here at the beginning. I was on the floor trying to get a UC for a Taxpayer's Right to Know data availability online bill with Senator Lankford. We were trying to get it passed, and so I was running a little late, so I missed the announcement about your family and that you have four children and one on the way?

Mr. KREBS. Yes, ma'am.

<sup>1</sup> The prepared statement of Senator McCaskill appears in the Appendix on page 29.

Senator McCASKILL. My husband and I have seven children, and we have 11 grandchildren, and I just want you to know the more babies, the better. [Laughter.]

It is the motto around my house. We just had two new babies a month and a half ago, two new grandsons, and they are the light of my life.

I want to ask you—first of all, I am thrilled that you have agreed to serve. I have reviewed your background, and I think you are—and I will tell you that staff that interviewed you came back and said, “He is the real deal. He really knows what he is talking about.” We need you in this job, I believe, and I think it is very important that you are given the resources and the authority you need to move the needle in this important area.

The first question I ask every witness is very important because I am a big oversight freak and I love to do oversight, and I always want to make sure that oversight can continue, regardless of the parties that are in charge. So I want to ask you these three questions:

Do you agree to provide information and documents when requested by Members of Congress, regardless of party?

Mr. KREBS. Yes, ma’am, I do.

Senator McCASKILL. Do you believe that the NPPD management should comply with requests for documents and information from Members of Congress, regardless of party?

Mr. KREBS. Yes, ma’am, I do.

Senator McCASKILL. And what role do you think Congress should play in assisting NPPD management in rooting out waste, fraud, and abuse?

Mr. KREBS. In your oversight role, I believe you can assist us in understanding where we could be more efficient, give us the appropriate authorities to ensure that we are responsible stewards of the taxpayers’ dollars.

Senator McCASKILL. Let me ask you about the 17 States that have requested risk assessments. I asked Assistant Secretary Manfra, and I think I got an answer that was a little confusing. I asked if any States were waiting right now for an assessment that they have not been able to get. She said nobody in the election community is waiting for an assessment.

My question was not about a backlog, but I was instead trying to determine if all the States that have requested risk assessments have actually received the service and that the request has been completed. Do you have the data on that?

Mr. KREBS. So, ma’am, we have 17 States and 8 local jurisdictions that have requested vulnerability assessments. There are a number that are in the scheduling phase, and the reason that they have not necessarily been completed to today is that there is a certain degree of preparation that is required for a risk and vulnerability assessment (RVA). That sometimes can include some preparation oftentimes, rather, preparation on the State or the local jurisdiction side. In some cases, what we have seen is that they do have some upgrades, patches, things like that that they need to get in order. There are also some basic legal agreements that we have to get in place that we understand, so they understand the scope

of the risk and vulnerability assessment. And on that note, there is some scoping of the RVA that has to happen.

I will say this, though: If any State or local jurisdiction asks for an RVA in advance of the 2018 midterm elections, they will get it when they need it or they want it. There is no backlog. The wait list is due to preparation. So you have my commitment on that and that we are prioritizing these RVAs, and they will get done at the request of the——

Senator MCCASKILL. So you are telling me the wait is on their end and not on your end?

Mr. KREBS. I would say that there is just a standard preparation that has to take place, and I would not say it is on anybody's end necessarily. It is just getting ready for a vulnerability assessment.

Senator MCCASKILL. How many of those 17 have actually been completed?

Mr. KREBS. My understanding, at this point we are up to about nine, I believe, and I would have to come back to you on that one. But as I understand it, the majority of them will be completed by if not the end of May, soon thereafter.

Senator MCCASKILL. OK. Obviously, it is the end of April.

Mr. KREBS. Yes, ma'am.

Senator MCCASKILL. The election is quickly approaching, and I think it is really important if those States—and I really admire the States that have stepped forward and said voluntarily—and, by the way, whatever you find, what they do with it is voluntary. There is nothing here about the heavy hand of the Federal Government reaching into the States and telling them what to do. I am really proud of those States that have stepped forward and asked for the help, and I do not want in any way to ever indicate that that shows that they somehow are lacking. I think just the opposite. I think they are showing a high degree of professionalism and responsibility by asking for all the help they can get, especially when we are willing to provide it to them at no cost. So I want to compliment them.

I asked also yesterday—or I guess it was the day before yesterday—Assistant Secretary Manfra how many people in DHS work full-time on election security. She was going to get back to me on that. Could you give me that answer?

Mr. KREBS. So the high-side number of full-time—and it changes day to day based on when a special election is, when we have an RVA, things like that. It is the 10 to 15 range. Again, it flexes a little bit.

We do have a number of part-time, meaning we have full-time equivalence Federal employees at DHS, that in some part of their day are focused on State and local election activities, including our risk and vulnerability assessment teams. They may be going from a State to do election assistance to a Federal high-value-asset assessment, depending on the week. So it is going to vary.

The \$26.2 million that Congress provided us in the fiscal year (FY) 2018 omnibus is going to allow us, rather, to build out our capacity in terms of what we can do not just for State election systems, but more broadly the State and local community as well. As we have seen I think with Mecklenburg County, with Colorado, with Atlanta, there is a real need for technical support and other

assistance at the State and local level, and so as we are engaging on the election front, we are also expanding and looking a little bit more broadly at the information technology (IT) systems across States.

Senator MCCASKILL. I do not think 10 to 15 full-time on election security is anywhere near adequate, and I want you to know that I personally will try to do everything I can to help get more there. I am sure you agree with me that 10 to 15 people to cover election security in this entire country with all the various election systems that exist is woefully inadequate. But I do think we can also be looking at—I know that all of this is being provided free. It seems to me we ought to noodle on whether or not we could do some kind of agreement where we would help with some kind of matching funds from the State and local governments, because many of them are hiring from the private sector at a high cost, and we could partner with them and do more with maybe not quite as much Federal money being spent. And I would like to explore that also.

Thank you, Mr. Chairman.

Chairman JOHNSON. Just to augment that a little bit, they obviously have cybersecurity individuals in the States as well, so that is not just 10 or 15. You have a force multiplier in terms of the State election officials, correct?

Mr. KREBS. Yes, sir, that is right. If I may, historically when we have talked about this over the last year, we have taken this bottom-up approach of here is how DHS can help do X, Y, or Z.

I think what we need to do—and I believe the conversation is turning that way—is take a more top-down approach in terms of here is the shared responsibility of election security. DHS is in support of State and local officials. State and local officials have been managing risk to their enterprise and their environments for years. It goes back well before elections. They are the best there is at managing what happens on election day when there is a power outage or there is a tornado or there is a hurricane. They do this quite well. And IT security has increasingly been one of the things they have looked at.

So when I talk about the 10 to 15-plus that we have from the Department of Homeland Security, that is obviously in support of thousands of security specialists across the country. And it is, as you point out, not just State and local officials. Some of those that are not taking our services, they do so because they have their own capabilities, whether it is in-house or contracted resources. But your point is take about the matching funds.

Senator MCCASKILL. Let me just make this point. I know what State employees are paid in the State of Missouri. I know what the market bears for good IT help right now. I do not mean to denigrate any of the State employees in my great State, but we have cut and cut and cut and cut local and State governments, and when you do that, you actually eat at the muscle of our ability to track the best talent to do the kind of really high-level work we are talking about here. So there may be people on the payroll in a lot of States. I am not sure that all of them have the expertise that we can help them with from your Department.

Thank you, Mr. Chairman.

Chairman JOHNSON. But as is true in the private sector, you do use private sector security analysts as well to aid. But, anyway, I know Senator Harris has a unique situation. I think this has been cleared that you are going to ask questions next. Is that——

Senator HEITKAMP. That is fine.

Chairman JOHNSON. OK. Senator Harris.

#### OPENING STATEMENT OF SENATOR HARRIS

Senator HARRIS. Senator Heitkamp, I thank you for your gracious leadership and friendship.

Senator McCASKILL. You are saying you owe her one? I just want to make sure we got that.

Senator HARRIS. I knew she was not going to let it go this easy. I am ranking in another hearing.

Senator HEITKAMP. I have a celestial log book I keep. [Laughter.]

Senator HARRIS. I look forward to the day I can pay you back.

Congratulations on all of the changes that are happening in your life in the midst of one of the great crises of our country, which is securing our elections. And I appreciate the last time you were before us and the answers to the questions I presented. And I also know that you followed up and actually did some reprioritization around the election cycle, so I appreciate that.

I have a few questions for you about security clearances for State elections officials. My understanding is that 30 State elections officials, which are representing 30 States, have received a security clearance or an interim security clearance as of today. Fifteen State officials have requested a clearance but have not yet received one, and five State officials have not yet applied.

Do you have a proposed timeline when all of these 30 State officials will receive a permanent clearance?

Mr. KREBS. So, ma'am, on those five that have not yet applied, in some situations they have actually declined to have a clearance. Instead, we are working with other officials in their States, for whatever reason.

On the 15 that are going through the process right now of the adjudication of their SF-86, their clearance documents, they are rolling in on a day-to-day basis. That process is managed by the DHS Office of Intelligence Analysis (OIA).

I will say this: I do not have specifics because every single case is different. Every single official has experienced some life event that requires a little bit extra investigation or adjudication. What came to my attention I was unaware of, Secretaries of States are sued a lot just as a matter of the course of business. Every single legal action has to be recorded. I think we talked about that before.

So what we are doing is we are putting a lot of pressure on the Intelligence Analysis Office to move those along, but I will say this: I know, I have confidence that if right now I needed to get a piece of intelligence in front of a State election official, I could do that in a matter of hours. If I needed to pull together a meeting tomorrow to share classified information, we could do that. That is the progress we have made in the last year.

I do not want to pin everything on issuing security clearances. It is the outcome we are trying to achieve, and that is, making sure

that we can get classified information in their hands when it is needed.

Senator HARRIS. I appreciate your point, but the concern I have is that, short of a permanent security clearance, then there is a process by which you would go day to day, right? They have to go day to day in terms of when they are going to receive or if they have the authority to receive classified information. There is nothing that would give them a certain permanence in terms of having it every day consistently without reapplying. Is that correct?

Mr. KREBS. It is not a reapplying. If confirmed, I personally would have the authority to give 1-day read-ins.

Senator HARRIS. Right.

Mr. KREBS. And it is not, submit information, it has to be adjudicated there are known entities.

Senator HARRIS. But do you have to authorize that each day to give a 1-day clearance?

Mr. KREBS. Yes, ma'am, but to be frank, if they had their permanent clearances and I needed to get information to them, I would have to do a judgment on need to know, anyway. So it is a little bit of extra paperwork, but, again, I have confidence that if I need to get a piece of information, we could make that happen.

Senator HARRIS. Can you followup with this Committee and give us a timeline on when those 30 State officials will receive their permanent clearance, taking into account all the variables?

Mr. KREBS. Yes, ma'am, the additional 15, we will absolutely follow up.

Senator HARRIS. Yes, the 15.

Mr. KREBS. Yes, ma'am.

Senator HARRIS. And then I am sure you are aware, but I asked my team to give me a list of the upcoming elections, and so I am not going to ask you to tell me the status of each election officials from these States. But I am sure you are aware May 8th is Ohio. I hope they have theirs. May 15th, Idaho, Nebraska, Oregon, and Pennsylvania; May 22nd, Arkansas and Georgia; June 5th, Alabama, California; Iowa, New Mexico, South Dakota, June 12th; another series of States, June 26th. So this is all imminent.

Mr. KREBS. Yes, ma'am, and we are taking a risk-based approach, so we are looking at what is imminent and then working with the intelligence analysis folks to see what we can do to increase the sense of urgency around that.

Senator HARRIS. Can you tell me which States are the five States who do not want security clearances?

Mr. KREBS. So two things on that.

First is that, generally speaking, we do not discuss security clearance matters in public as a matter of operational security. They can then become targets for collection from foreign intelligence agents. So that is the first piece.

The second is from an individual State, who is doing what, who is taking what action, we are in a position where we are not disclosing the individual pieces of information. Our approach here is nonpartisan, apolitical.

Senator HARRIS. I hope so.

Mr. KREBS. We are absolutely——

Senator HARRIS. Because this is absolutely a nonpartisan issue. So there is no rule that prohibits you from telling this Committee, even in a classified setting, which States——

Mr. KREBS. So in a different setting, we can discuss more specifics, but from a——

Senator HARRIS. Mr. Chairman, I would urge that we get that information and, in particular, inform our colleagues who represent those five States and make sure they are aware of the seriousness of this issue.

Chairman JOHNSON. I have no problem with that.

Senator HARRIS. OK. That would be great.

And then on election data breach notification, another important service—we have discussed this before—that DHS provides is what I refer to as “hazmat teams” that will go out to the State and help an election agency, if it has been hacked, to get back up and running, to be resilient after an attack.

In an interview, the Illinois State Board of Elections executive director said that—and this is, I think, the Ranking Member’s point, too—“They have a good IT department,” when they faced a threat from a sophisticated foreign actor. But they said their resources are like bows and arrows against the lightning. So we are talking about, obviously, an attack on a State election system. Would you agree that even though it attacks a State, it really is a threat to national security?

Mr. KREBS. Yes, ma’am. I think Secretary Nielsen has been consistent about that as well. Election security is a national security issue.

Senator HARRIS. And so do you believe that if a State election agency is hacked while administering a Federal election, the State election agency should be required to notify the Department of Homeland Security?

Mr. KREBS. Ma’am, I think it depends on the definition of “hack.” As I think Assistant Secretary Manfra discussed yesterday, there is a difference between scanning and targeting. Scanning happens in some cases thousands of times a day.

Senator HARRIS. So, in your opinion, who should we leave the definition up to? Because it seems to me we should have some clear indication of what would require a State to report to DHS that they have been hacked. And I appreciate the point that has been discussed often, which is it is perhaps a vague term. But whose responsibility is it then to clarify what qualifies as a reportable hacking?

Mr. KREBS. So I think that is a conversation that is happening right now in the Secure Elections Act. I think the recent conversations you had with the Secretaries of State, that is the exact sort of forum in which we can start hashing out what the threshold is for a notification. I do not believe a scan, frankly, would require notification, but a penetration of a date of registration, I think there is some incentive or some indication that——

Senator HARRIS. So my time is up, but what I would like to do for follow-up is get from you your suggestions about what should be defined as a “hack” which would require a State to report that to DHS.

Mr. KREBS. Yes, ma’am.

Senator HARRIS. OK, thank you. And if you could do that within the next 3 weeks, that would be great.

Thank you.

Chairman JOHNSON. Thank you, Senator Harris.

Just a quick comment. The complexity of data breach notification is something I have learned a fair amount over the last 5 or 6 years. Senator Heitkamp.

Senator HEITKAMP. Thank you, Mr. Chairman and Ranking Member, and thank you, Mr. Krebs, for agreeing to serve our country, as I said in my opening comments.

I just want to throw out an idea that I think would be helpful, and it goes to the kind of general theme of what I want to talk about here, and that is, there needs to be a Center of Excellence for cybersecurity. You know where I am going, right? So we do financial audits in State government. We do performance audits. Claire was, I think, the State auditor, probably did a number of performance audits. I think it is only responsible, especially when we are talking about Federal elections, to do performance audits of the security of State systems.

Now, we are in a crisis because we are up against a couple months where, as Senator Harris pointed out, these elections are coming now, and many of these elections will be decided in the primary. And that is true particularly in States like California where you have a jungle primary. And so it is on us, and we cannot look our constituents in the eye and say, "Yes, everything is cool. We have it under control." We need to have a Center of Excellence for cybersecurity on all things that affect our national defense and our national security. And I really believe that your agency is the place where that should be. I think Senator Carper may agree with me on this. We fought pretty hard to try and claw back some jurisdiction on cyber. It has been centered in Intel, as it should. They should be concerned about it. But we need a broader government-wide, nationwide plan for what we are going to do in cyber so we are not stepping on each other, we are not taking missteps that are incredibly costly. You know how costly all of this is. But we cannot ignore the small stuff, and this is what I am getting at. This is something we talked about yesterday, which is that resiliency of the foundation. Right now I would tell you it is fairly porous. I think that when people put their passwords as "password" or "11111" or they do not do the kinds of things that are recommended in common-sense ways to try and protect the resiliency of either their devices or their programs or managing their data.

And so there is a whole lot of force multipliers that we can rely on, whether it is nonprofit, consumer-oriented groups, whether it is the State groups that do consumer protection and consumer awareness and education, it is true probably in a lot of areas in life, but many people just want that magic bullet. You are going to create that impenetrable, hardened shield, and we have to tell them, look, we can have the best military, we can have the best law enforcement in the world, but if we do not lock our doors, we are less secure.

So can you walk with me how you see your role in that piece of it, not the top-down but the bottom-up kind of resiliency of users? And that is pretty much all of us now in America.



Mr. KREBS. Yes, ma'am, absolutely. Thank you for the question. I mentioned it in my opening statement, but when NPPD was originally organized as a successor to Preparedness back in the 2007 timeframe. It was a collection of programs, and the name, in fact, reflects that, National Protection and Programs Directorate. It was a hodgepodge. The threat, the cybersecurity threat at the time was obviously nowhere near what it is today. The budgets alone show that. The National Cybersecurity Division was a small collection of folks that had an issue they were trying to get their arms around.

Where we are now with the threat environment, with the authorities that are provided by Congress, by the appropriations that we have been provided, I think it is clear that now—and this is the reason we need the Cybersecurity and Infrastructure Security Agency—DHS NPPD is the primary—it is the leader for national risk management for cyber and critical infrastructure protection. It has statutory authorities to be the lead critical infrastructure protection coordinator. There are sector-specific agencies that have the sector excellence, the expertise, whether it is Treasury, the Department of Energy (DOE), HHS, but it all comes together at the top. So when you talk about a top-down—and I understand where we are going with the bottom-up, but on the top-down, there needs to be one person, one organization, rather, that can stitch it all together.

Senator HEITKAMP. I just want you to know we expect you to throw some sharp elbows. There has been a lot of turf on this, and there cannot be. We need a Center of Excellence, and that is your job, in my opinion, is to create a Center of Excellence to be that entity that evaluates products out there, that can be, in fact, protective and shield, to develop products that can better educate the public on how to protect themselves, and then have the ability to integrate those not just with those cyber threats, but understand that that will put pressure on physical threats and be at the table when we are evaluating all threats and bring that expertise. That is why we are excited that you have applied for this job, but that is my expectation of what you are going to do with this job.

Mr. KREBS. Yes, ma'am, we have a common adversary; we have a common enemy. I have no patience for infighting across the family. We should be working toward the same common purpose, but what we need is a centralization function, and that is us as the—

Senator HEITKAMP. Right, but the problem that you have is that now that everybody has gotten panicked about cyber, this is the new bright, shiny object over here. That is where there is going to be some money. We might get some personnel. You know how the bureaucracy reacts to that opportunity. And it will go places that will be dispersed in ways that we do not have the best and the brightest centralized in a Center of Excellence. And that is what I want. That is what I want you to be. That is what I want your agency to be. I have been nothing but impressed by you and the people who have come before this Committee, and I think we have a real opportunity here to work with universities, we have a real opportunity to work with other State agencies. You have 4½ or a quarter—I am not sure what it all is, where it is.

Mr. KREBS. Four plus one.

Senator HEITKAMP. Showing the shock on your parents' faces, it might be just a quarter. Four and a quarter kids. This is going to be hard work, and I am so grateful. I want to say this—because I am running out of time—to your family because we are putting a lot on your husband, and we are putting a lot on your son and your son-in-law. But the work that he is going to do is just as important as anyone who puts on a uniform and carries a gun. He is on the front line of serious threats to this country, and you should be so extraordinarily proud of him and that you raised a fine human being, and for your kids, they will know that you are working to make the world a better place for them.

Thank you, and I look forward to ongoing discussions.

Mr. KREBS. Yes, ma'am. Thank you.

Chairman JOHNSON. Senator Heitkamp, before you potentially leave here, I appreciate you bringing up the subject of turf wars. I raised that issue yesterday. There is a reason we did not get the name change in the omnibus. There was objection to that. So we need to be honest about this. The reality of the situation is that there is conflict here. I have been trying to facilitate and I will make the offer again today. By the way, I talked to Chairman Burr about this on the floor of the House waiting for President Macron to speak about getting the Secretary, yourself when confirmed, getting other Members of Congress together, Intelligence Committee and DHS, and let us work this out. That is what we need to do. This threat is too significant to allow turf wars to get in the way of as efficient an operation as possible in terms of dealing with a very complex and serious problem.

Senator HEITKAMP. I do not think there is any doubt about it, and I think that when we have dispersed jurisdictions, we have no accountability. So with this power, if we get this done, comes accountability, and I think accountability and understanding if something happens it is on you instead of pointing the finger over at DOD, instead of pointing the finger over at the intel community, I think that is critical for accountability and oversight.

Chairman JOHNSON. So it is time to stop burying our heads in the sand in terms of the turf wars that are occurring right now. We have to get by those, and we have to come to an agreement on this. So from my standpoint, this is a top priority. We have to get this decided, agreed upon, and move past it. Senator Peters.

#### **OPENING STATEMENT OF SENATOR PETERS**

Senator PETERS. Thank you, Mr. Chairman. Mr. Krebs, again, thank you for your willingness to serve. Senator Heitkamp is right. This is an incredibly important position, and we are going to be looking for your leadership every day dealing with what is perhaps our No. 1 national security threat, which are these cyber attacks.

I want to pick up on the theme that we have heard over and over again about turf wars and how we have these silos in the Federal Government. We often talk and this Committee talks about some of these big challenges and we have to have a whole-of-government approach. Yet the "whole of government" is in all these discrete areas, do not talk to each other like they should, and are not efficient, and we are not really focused on the overall mission, which is to protect the American people.

It is not obviously the first time we have had these issues, and the Department of Defense particularly has had these issues for many years, from the Navy, the Air Force, and the Army. They are very proud parts of the service, but for many years they never really talked to each other. It is pretty hard to conduct a war when the Navy is not talking to the Army and they are not working together. And in order to resolve that, jointness has been a big part of military doctrine for many years, where they work in a joint fashion. There are joint duty officers that actually will work in different branches to learn about other branches and can be able to help coordinate that.

But, unfortunately, we do not have that in the civilian side so I am going to ask you about some legislation I am working on that will hopefully allow us to have that kind of joint duty officer, similar to what we would have in the Department of Defense. I am working with Senator Hoeven on a bill that we hope will be up at some point, Mr. Chairman. It is the Federal Cybersecurity Joint Duty Program Act, which would establish a civilian personnel rotation program designed specifically for cyber professionals that would enable them to gain experience across the Federal enterprise. So authorizing a joint duty program would provide both clarity and guidance for human capital officers across the government and help them develop, I believe, a stronger cyber workforce if they have had a chance to work in different departments. They are going to bring lessons learned in this department to another department. They are going to likely learn a whole lot in that department. And then when you are trying to coordinate all these, you are going to have a team of people who have actually worked across these different agencies.

Yesterday in the previous hearing, Assistant Secretary Manfra thought it was a good idea that we should move forward, but I would like to have your thoughts. Would such a program that would provide these kinds of rotational opportunities be beneficial to employees? Is this something you think we need to be looking at?

Mr. KREBS. Yes, sir, I think it bears a lot of merit. I think the ability to standardize and centralize cybersecurity across civilian agencies is something that will only help us. In fact, we are looking at ways to do that now with the Continuous Diagnostics and Mitigation (CDM) program. We are doing some training for existing IT security professionals so they know how to use the tools we are deploying through the CDM program.

But this is a great example of if you put somebody in a different environment and allow them to understand what the operational environment looks like, they are going to come back more well rounded, better off, and able to contribute to the bigger mission.

I would also offer that, in addition to internal government inter-agency rotations, we need to continue looking at government programs exchanges with the private sector, so DHS has the exemplar program that sends government officials out into the private sector, as well as the loan executive program that brings them in. So in some cases, we have them sitting in our National Cybersecurity and Communications Integration Center. That is another example of we can put our folks out into an environment. They understand

what private sector requirements are, and they come back in and they help fine-tune the mission.

So I am looking forward to having a continued conversation on your bill in particular, though.

Senator PETERS. Well, one thing that I see this doing, too—and I would like your thoughts on it—is that it makes an already interesting job even more interesting at a time when we want to retain these professionals in Federal service. To be able to have that wide range of experience I would think would aid with retention. Do you agree?

Mr. KREBS. Yes, sir. I think if I can hang along with a name that tells folks what my organization is, the Cybersecurity Agency, if I can in a recruiting manner tell them, hey, you can go hunt for the Russians, you can go hunt for the Chinese across various departments and agencies, that is a pretty attractive recruiting pitch.

Senator PETERS. And how would the Federal cyber workforce be strengthened if employees at other agencies were afforded the chance to serve in a rotational capacity at NPPD?

Mr. KREBS. Well, for one, they would understand how we approach incident response assessment, so when they do a rotation within NPPD, they go back to their agency, and, again, we have a standardized approach to cybersecurity and information security professionals across the Federal Government. To the extent that we can continue to standardize and streamline our approach across the Federal Government, that is going to make us better off.

Senator PETERS. Great. Well, I appreciate that. I look forward to working with you, if confirmed. And I think the other idea that you raise, which would have to be the next step, is people who can move out of the Federal Government into the private sector and back, as you know, with civil service rules that can be a lot more complicated, but one that I think is absolutely critical. We see folks who are outstanding individuals in the cyber space now who are willing to serve, for example, in the National Guard in our new cyber units that we are setting up there. They do not do it for the money. They do it because of the mission. They do it because they are patriotic Americans, but we have the opportunity to get highly skilled folks in the private sector working on national defense issues. I think there are opportunities to do that as well. Do you agree?

Mr. KREBS. Yes, sir, and I think what you are highlighting is that there are a number of tools in the cybersecurity professional toolkit. DHS is not the only one that is having some workforce challenges. The NSA is having workforce challenges. We have already talked about the State and local government official workforce challenges. The private sector has workforce challenges.

So what we need to be looking at is, in addition to filling the vacancies that we have, what are the other resources—I do not want to steal Senator Hassan's thunder, but the bug bounty program is another example of diversifying our capabilities. What is the security outcome we are trying to achieve? That is what we need to be focused on. And how are the ways we can plug the gaps, whether it is National Guard—again, as long as we are standardizing, taking a similar approach from a day-to-day information security approach for when that bad day happens, that when we show up, we

all know how to respond, we all know how to act so we are not doing the business card game. I think that is only going to serve us that much better.

Senator PETERS. Great. Thank you so much.

Mr. KREBS. Yes, sir.

Chairman JOHNSON. Thank you, Senator Peters.

By the way, I think it is an excellent idea, the rotation. I like it so much I wish I would have thought of it myself.

What I would ask you to do is work with the different departments and make sure that they do not have a problem with it, because that is what we are going to do as Committee staff, go to DHS, do you have any issues with that? But try and do that work ahead of time. Again, I want to be completely supportive of it.

Senator PETERS. Thank you, Mr. Chairman.

Chairman JOHNSON. Senator Hassan.

#### **OPENING STATEMENT OF SENATOR HASSAN**

Senator HASSAN. Well, thank you, Mr. Chair, and I want to thank you and Ranking Member McCaskill for this hearing. Welcome, Mr. Krebs. And to the entire Krebs family, thank you. I am seeing Henry and Anna. You are doing great. You are being very polite, and you are doing better than most adults do in these hearings. So I just want to thank you for sharing your Dad with the people of our country, because he wants to and is doing really important things to keep us all safe. So we are really grateful.

Mr. Krebs, I wanted to follow up a little bit on what you just mentioned a moment ago about the bug bounty program. You and I have discussed the legislation that Senator Portman and I have, Senate bill 1281, the Hack DHS Act, which passed the Senate unanimously last week. Hack DHS requires the Department to establish a one-time bug bounty pilot program in order to assess the value of a bug bounty as a tool to secure DHS' systems from all types of cyber threats.

Last week, you were quoted as having questions about how a DHS bug bounty program would be funded and whether DHS would be given the necessary flexibility to implement a bug bounty in a safe and effective manner. I appreciate those concerns. The good news is that our Hack DHS bill addresses all of those concerns, as I think you and I have discussed.

Our bill gives DHS ample flexibility to implement the bug bounty pilot program as DHS sees fit. Under the bill the Secretary is empowered to exclude parts of DHS that it feels are too risky to open up to a bug bounty, and under our bill DHS is required to fully vet any hacker participating in the bug bounty program.

Additionally, the bill authorizes \$250,000 for DHS to run the bug bounty pilot program, which is double what it cost the Pentagon to run its pilot program.

Finally, my staff, Senator Portman's staff, and the staffs of Chairman Johnson and Ranking Member McCaskill have all worked closely with DHS to incorporate any DHS changes so that this bug bounty program could serve as a key tool for the Department to counter cyber threats.

So, Mr. Krebs, given that our bill addresses many of your concerns, can you share with us your opinion about the Hack DHS bill

and whether you think it would provide DHS with a valuable tool to strengthen the Department's cyber defenses?

Mr. KREBS. Yes, ma'am, as you and I discussed the other evening, I welcome any tool that is going to help us be better, and this is an example of a tool in the broader toolkit that will enable us to secure our networks. So, yes, ma'am.

Senator HASSAN. Thank you very much. I appreciate it.

That is all I have, Mr. Chair.

Chairman JOHNSON. Thank you, Senator Hassan.

Senator Lankford.

#### **OPENING STATEMENT OF SENATOR LANKFORD**

Senator LANKFORD. Thank you, Mr. Chairman.

Good to see you again. Thanks for the work that you have already done. Thanks to your family. The folks at this dais understand extremely well the cost to families and what that really means to your family, and so we appreciate very much the sacrifice that you and your family are making to be able to serve the country. So thank you for that.

Let me ask you a little bit about determining domestic threats, foreign threats, and a variation that is coming now where foreign actors are basically finding cyber criminals and using them as contractors. And so we have this strange hybrid of an area that is really a foreign cyber criminal that sometimes works for a foreign government and sometimes they are free-lancing and doing it on their own. As we are trying to be able to determine the threats as they are coming, how to respond to them and how to defend that, how are you filtering out and how should we as a Nation quantify this is domestic, in the United States, and this is foreign, this is a foreign actor, a foreign criminal actor as well? And what would the responses be different on that?

Mr. KREBS. So I think what we need to do is have a couple different axes at which we look at the broader threat. So on one side, we have the indiscriminate criminal threats, the ransomware campaigns. There may be some scanning and hacking and things like that. But it is those that are out there to make a quick buck or whatever. And then we have the nation-state level threat. And the gray space in between I think is—

Senator LANKFORD. The hybrid, right.

Mr. KREBS. You are hitting that. The issue here is that each of the adversary sets is going to have a different set of objectives and a corresponding set of pain points. So one nation-state, for instance, may be more financially motivated; another might be looking for geopolitical advancement. So whatever the response is, the deterrence package, the consequence package has to be tailored specifically to that adversary.

In the general cyber criminal space, law enforcement, which remains a challenge and is another part of the Federal Government, whether it is within DHS or the Federal Bureau of Investigation (FBI), that is going to require significant coordination with the international law enforcement community to do some of the overseas takedowns and extraditions. From a nation-state approach, the deterrence package is going to be wide-ranging, but it can in-

clude anything, as we have discussed, from sanctions to other instruments of national power.

Senator LANKFORD. So let me ask about the attribution of that, because initially when it hits, let us say, a pipeline company, it hits an electric grid, water, election system, whatever it may be, we know it exists. But trying to get attribution for it and then to be able to figure out what agency is then going to be able to follow up, either recommendations or how to respond, or who is going to handle that, is that domestic? It is hitting the United States, but was that someone local? So that is going to be who, is that going to be you, is that going to be FBI? Who has it? Or is it going to be international, is it going to be someone else? How is that working right now with the hand-offs, and what can be improved, the speed of both attribution and then the hand-off of who has it from there?

Mr. KREBS. So Presidential Policy Directive (PPD-41) is fairly clear in terms of the lanes in the road and who is doing threat response and who is doing asset response. I am, frankly, less concerned about if it is this bad guy trying to achieve this objective. What I am concerned about is managing risk and buying down risk, whether it is a single asset, understanding what is going on within that network, helping them get it straightened out, but then taking the piece out, whether it is an indicator or other signature, and then moving it into other aspects of not just that sector but other sectors. Because one thing we are increasingly seeing is while the adversary, particularly the nation-state adversary, is sophisticated and capable, they are not all the time just focused purely on the electricity subsector or the banking and finance subsector. They are looking a little bit more broadly, so it is important that we not limit ourselves to a sector-by-sector approach, which we have already talked about today.

Senator LANKFORD. Right, which would be helpful. So let me go to the risk side of it then. One of the lessons learned from Kaspersky and what happened here in the Federal Government with their distribution basically across multiple agencies and the speed of our response once we discovered more.

Mr. KREBS. So given the ongoing litigation, I cannot get too much into the specifics of Kaspersky, but what I can talk about is broader supply chain risk management. We are taking a couple different approaches at DHS. One is within NPPD we have kicked off—I believe you have gotten the briefing on the cyber supply chain risk management approach. What we are trying to do is provide intelligence and other information and inject it into the procurement process as left of procurement as possible. So help contract officers and procurement officials write Requests for Information and Sources Sought that are risk-informed. And then when they do get Sources Sought, we can then craft Requests for Proposals—again, risk-informed. When they get their proposals—again, risk-informed—injecting the appropriate risk information so that they can identify whether it is a first-tier, second-tier, third-tier contractor, what may be a risky proposition. And what that is really going to require is transparency in the proposal. So it is going to require procurement officials to drive more transparency, to drive more in-

formation provided. And that is just at the Federal procurement level.

Senator LANKFORD. So do you anticipate that your office will work with procurement officials governmentwide to be able to help develop some of those standards?

Mr. KREBS. Yes, sir, we are right now.

Senator LANKFORD. So is it, again, your assumption that they will then have a new item, a new piece of software, a new piece of hardware, a new refrigerator that goes in the lounge that has wireless fidelity (WiFi) capability on it, whatever it may be, is it your expectation that each product will then be signed off by your office, or there is a set of standards to say here is what to be able to watch for?

Mr. KREBS. So my hope is to get to the latter point, to get to a more scalable approach. If we are looking at every single transaction, we talk about backlogs. That one is going to be years.

Senator LANKFORD. That is what I would assume.

Mr. KREBS. What we need to do is educate the procurement officials so they can write smarter, more risk-informed contracts, so you will attest that you have disabled this feature, or you will describe the third-party code that was written into your software or baked into your product.

Senator LANKFORD. OK. When do you anticipate that would happen? I know that has already started. When do you think that would be complete?

Mr. KREBS. To answer this the right way would be to say it is never going to be complete because we are going to continue—

Senator LANKFORD. Because there is always new stuff, yes.

Mr. KREBS. Yes, sir. I would have to get back to you on exactly what our—

Senator LANKFORD. That is fair enough.

One of the key things that we are trying to be able to push is to be able to make sure we are getting ahead of that. One of the lessons learned on Kaspersky is speed.

Mr. KREBS. Yes, sir.

Senator LANKFORD. Once we actually find out about the threat, how to be able to respond to that, what does that mean getting the information out to multiple entities that need to get it quickly, giving them options to be able to transition from this to this, and to know that they can make that transition quickly and safely, but also then studying the new standards, trying to determine what questions need to be asked before we begin the process.

Mr. KREBS. And if I may add, one piece is that while we are focused on the tactical Federal procurement level, there is a broader national strategic conversation that needs to happen on supply chain risk management. We are seeing it in some of the 5G spaces. But what we need—sorry, out of the corner of my eye.

Senator LANKFORD. No, that is a good thing, actually. [Laughter.]

Mr. KREBS. What we need to do is actually look at what a holistic national supply chain conversation looks like, what the national critical functions are that underpin our very economy that ensure that the Federal Government can perform its duties on a day-to-day basis. And so we have to identify those national critical functions. We have to identify those critical components within those



functions and then identify what the transparency requirements are, what the certification or standardization requirements are. And then at a certain level, we may have to have conversations about reshoring and bringing manufacturing back to the United States, and that is going to require an entirely different strategy.

Senator LANKFORD. Thank you. I appreciate that. And, by the way, “Goodnight, Moon” is one of the all-time classic pieces of literature. [Laughter.]

Thank you.

Chairman JOHNSON. I think the lesson learned in Kaspersky, certainly one of the lessons is that within the intelligence and national security community, they knew full well that here is a cybersecurity business founded and operated by a former KGB officer, and it is probably not a real good idea to let that business continue to grow and infiltrate into our economy without mentioning something until this very late date.

I think our Committee Members have done a good job asking questions, so let me just kind of mop up on a few things or make some comments. Senator Harris was talking about data breach notification. Talk about the complexities of that issue, because it seems so simple. I mean, that is what I thought 6 years ago, and the top two things on cybersecurity are always information sharing and a national preemption of data breach notification just made so much sense, but it is far more complex than that. So first speak to that a little bit.

Mr. KREBS. The complexities happen at virtually every layer of government. So you have State data breach requirements. It is going to vary State to State. I think 47-plus States have actual data breach notifications. It is going to vary across sector, too. Banking and finance, payment cards, retailers, they are all going to have—whether it is personally identifiable information (PII) or Payment Card Industry (PCI), they are all going to have different thresholds for reporting given the impacted community. Then you throw in Health Insurance Portability and Accountability Act (HIPAA), you throw in other health information. It is challenging alone at the State level. And then once you bring it up to the Federal level, I believe the average number is about eight pieces of legislation per session.

Chairman JOHNSON. Talk about the entity itself being breached, the complexity of knowing you have been breached——

Mr. KREBS. Knowing the extent.

Chairman JOHNSON [continuing]. Doing the forensics, understanding exactly what happened before you are required to do something.

Mr. KREBS. Yes, I think one of the challenges that we are having is more, as you have mentioned, the complexity. It is the complexity of the systems we are talking about, the complexity of the information, the complexity of third-party risk. Who actually is owning or operating that system that may or may not have been impacted, what controls they had, what information was reviewed, scanned, exfiltrated. These are all questions that we are still trying to sort through as a community, and it is not always a baked answer.

I will add in the other complexity is in certain cases there are active investigations going on from a law enforcement or intelligence perspective. We are trying to keep eyes on the bad guy as they are moving around because this may be a novel approach. And so there is some sort of preserving of the environment for that sort of monitoring.

Chairman JOHNSON. As you heard from the Committee's questions, obviously election security is something we take very seriously, and we appreciate the fact that you realize that is a top priority.

I do want to just kind of summarize the way I think of this and see if you basically agree or how you would modify my approach. But to me there are basically three threats from the standpoint of election security. First of all, can someone get into voting machines and actually affect the vote tally? Let me lay them all out. Then, second, can they get into the voter file? And then, third, the threat is literally public confidence.

So when it comes to vote tallies, in our briefings it seems like, because these election machines are not tied to the Internet, some actually have WiFi capability, but they are supposed to be turned off. It seems like it is pretty difficult for somebody to actually affect the voting tally. Would you agree with that?

Mr. KREBS. I think what we saw at least in 2016 was the sophistication of the adversary was not at least what was observed—I know Eric Rosenbach, “Do not ever count the Russians out,” I think was his message. But based on what we saw, the voter tally access was complicated. The thing that I reiterate is this is not about achieving 100 percent security or perfect security. It is about achieving a resilient ecosystem where you have confidence at the end of the voting cycle that what was put in on the left end came out on the right end consistently. So that is why we continue to encourage at least some sort of paper trail with a scientifically significant on the other side audit.

So I think that if we can get into a situation where we are managing risk—and that is what we are doing. We are not trying to secure. We are managing—

Chairman JOHNSON. Again, I am actually asking these questions to really confirm the final risk of public confidence. Again, I do not want to blow anything out of proportion. I want to take the risk seriously. And so changing the actual voter count is going to be a very difficult thing for somebody to do, certainly nationally. They might be able to do it locally, but even that is pretty tough. Getting the voter files to me is a more significant risk. But, again, there are many controls. There are a number of things that we can do post-audit, recounts, that give us some indication something actually happened.

And so you take those first two risks—voter tally, voter file—it is pretty minimal. And if we have our eyes on this and you have election officials, you have a very dispersed—which I think enhances election security, we ought to be able to as much as possible increase public confidence in our elections. To me, that is the whole point of this thing. And I do not want a lot of the rhetoric out there decreasing public confidence.

Mr. KREBS. It is a good scare story. I think there has been a lot of progress lately. Just yesterday or today, I believe Orange County, California, released their voter security playbook. The same has happened in Kentucky and Cook County. The public confidence messaging piece has to catch up to the fear factor.

Chairman JOHNSON. I do not want to understate the threat.

Mr. KREBS. There is no minimization.

Chairman JOHNSON. I think there is a great danger in overstating it.

Mr. KREBS. That is right.

Chairman JOHNSON. Apparently, both of us met with the Chief Executive Officer (CEO) of Duke Energy.

Mr. KREBS. Back to back, I think.

Chairman JOHNSON. As you know, I am concerned about EMP/geomagnetic disturbances (GMD). But, again, Senator Harris talked about clearances, and that is certainly what the CEO of Duke Energy was talking about. This is a governmentwide problem. There is a huge backlog. Is there a certain level priority that we can slot some of these individuals in for security clearances?

Mr. KREBS. Specific to the EMP/GMD threat or—

Chairman JOHNSON. Well, I mean, again, based on the priority of the threats that we are recognizing.

Mr. KREBS. So, yes, sir, I believe there is some prioritization of the process. I do believe that across the Federal Government, I think the backlog is somewhere on the order of 800,000 folks that are in processing. But from a private sector clearance perspective, we are streamlining our approach for how we work with the private sector and how they are sponsored and how they are put through. Paperwork is paperwork. We still want to make sure that the folks that are getting the clearances have been adequately vetted and validated and make sure that there is not something lurking around that they may be held at risk. But there are ways that we are looking at to help streamline the—

Chairman JOHNSON. OK, because I think we do need to prioritize this based on the threat.

The CEO is taking over their industry-wide group on some of this, and I am actually pleased to hear that she seems to be taking EMP/GMD seriously. I do not think from a government standpoint we have done enough, and I do not think we are taking it seriously enough. So I guess you are going to be in charge of the agency that will be tasked certainly from the standpoint of DHS, the EMP Commission tasked DHS and DOE with certain quick fixes, which, according to GAO, have not been undertaken. We do not have the strategy yet. So, again, I just want your assurance that this is something you will take seriously. Let us get to the bottom of this. How serious a threat is this? I am not an electrical engineer, but it has driven me nuts over the last number of years that we just cannot come to a conclusion of how serious a threat this is and what we should really do to protect our Nation against what could be a catastrophic occurrence.

Mr. KREBS. Yes, sir, you have my assurance that we are taking this seriously.

Chairman JOHNSON. OK. Senator McCaskill, do you have anything else?

Senator McCASKILL. Yes, just a couple.

The binding operational directives (BOD), I know that you issued BOD to make it more difficult for bad actors to mimic legitimate email communications from Federal agencies. The binding operational directives gave a 90-day and a 120-day timeline for parts of the implementation, meaning some of those deadlines have already passed. Can you give us a report card of how many Federal agencies have complied with this?

Mr. KREBS. Ma'am, if I may, I would like to circle back with specifics.

Senator McCASKILL. Sure.

Mr. KREBS. The challenge with the Domain-based Message Authentication Reporting and Conformance (DMARC) implementation is that not every BOD is created the same. Not every network across the Federal agencies are created the same. In some cases there were email domains that, frankly, were either dormant or, frankly, forgotten about. So there is a lot of kind of collating of what is across the systems. That has led to some challenges in implementation, but I would like to come back and meet with your staff to—

Senator McCASKILL. That would be great.

Mr. KREBS. Yes, ma'am.

Senator McCASKILL. Because I would like to follow up with that. I do think it is something that we have not—and I think you are going to have to figure out a way to navigate this very complex area so that we can take that basic first step in every Federal agency in terms of email communication.

Mr. KREBS. Yes, ma'am.

Senator McCASKILL. It is obviously a vulnerability.

You stated in your policy questionnaire—you all have some responsibilities, some specific responsibilities outlined in the National Response Framework in emergency management, critical information protection, and communication restoration. You stated in your policy questionnaire that you identified 50 areas for improvement after the 2017 hurricane season. Obviously, you have no work to do in this new job. I can tell you really are going to be spending a lot of time figuring out how to stay busy. But I would be curious what you would consider are the top two or three items on that list in terms of what you learned in the aftermath of this brutal 2017 season, especially in terms of restoration of communication, because when I have talked to people that were on the ground, that was the biggest challenge in terms of getting stuff where it needed to go, the inability of people to talk to one another.

Mr. KREBS. So thank you for the question, and I came into this job as Assistant Secretary for Infrastructure Protection in August 2017. A week and a half later, Hurricane Harvey hit. From that time until today, I have still been focused on hurricane season 2017, getting ready for 2018. I made numerous visits to Puerto Rico, went down to Texas and Florida.

The two primary takeaways that I have from hurricane season: First, I needed to do across NPPD a better job of integrating our cyber and communication shop and our physical infrastructure shop. And what we have done since hurricane season is a tighter linkage and, in fact, collocation of the National Infrastructure Co-

ordinating Center (NICC), the physical side, into the National Cybersecurity and Communications Integration Center (NCCIC) has responsibility for Emergency Support Function (ESF) 2, the NICC supports ESF 3, 8, 9, 12, and, in part, 13. That is a Federal Protective Service (FPS) mission. But everything at some point has to come together from a visibility perspective. What we found in Puerto Rico with Hurricane Maria in particular, specific to ESF 2, was that we were able to work with the communications providers, a number of them, including AT&T. That was one of the areas that we were able to get infrastructure restoration frankly the quickest. So we were able to work with the Department of Defense through FEMA and the Joint Field Office (JFO) down in Puerto Rico to put Cell On Light Trucks onto C-5 Galaxies out of Dobbins Air Force Base north of Atlanta, Georgia. We put the trucks on the plane, flew them down, put them in location, popped them up, had others on barges coming down. We were able to get that core infrastructure, that lifeline infrastructure back up quicker than any lifeline infrastructure on the island. That to me is, frankly, a signal that I have a pretty important job here, not just on the cyber side but on the physical and the communication side as well. So there is the integration so that we can pass and flow information from the physical to the cyber comms shop.

The second piece, I have already alluded to it, lifeline infrastructure. One of the things that we need to take away from hurricane season is getting meals ready to eat (MREs), getting water, getting bags of ice, getting all that other stuff into a disaster zone is important. But so is getting comms up, lights on, things of that nature. So we need to be figuring out what the right balance is between life-sustaining operations and life-sustaining functions, and that includes communications and power, because if you do not have power, you are not going to get a lot of other stuff done. If you do not have communications, it is going to be that much harder to coordinate.

Senator McCASKILL. You are going to need a lot more MREs if you cannot get those two things done.

Mr. KREBS. Yes, ma'am, so, again, I think it is the integration across my shop, but also working with FEMA to prioritize the restoration of some infrastructure services, and we have taken that to heart. We have a number of strategic engagements and working groups with FEMA right now to improve that. So for hurricane season 2018 I think we will be in a better position from an infrastructure—

Senator McCASKILL. Well, if you would share the entire 50—list with our staff, we would appreciate it, so we can get an idea—

Mr. KREBS. Yes, ma'am, happy to give you a brief—

Senator McCASKILL. We are trying to follow up on some very bad contracting that occurred in this space, which we are trying to figure out how to make sure those mistakes are not made again. But we want to be prepared to do the best oversight we can moving forward, and that means knowing what you see are the problem areas going forward. Thank you to you and your family for your service.

Chairman JOHNSON. Thank you, Senator McCaskill.

Mr. Krebs, I think you have found, just by the questions here, the Committee has a fair amount of confidence in your ability, and

I think we will in a bipartisan fashion do everything we can to move this nomination along as quickly as possible. So, again, I want to thank you for your testimony and your willingness to serve and again thank your family. You know already this is a 24/7 type of position, and they know that as well.

The nominee has made financial disclosures and provided responses to biographical and prehearing questions submitted by the Committee. Without objection, this information will be made part of the hearing record,<sup>1</sup> with the exception of financial data, which are on file and available for public inspection in the Committee's offices.

The hearing record will remain open until 5 p.m. tomorrow, April 26th, for the submission of statements and questions for the record.

This hearing is adjourned.

[Whereupon, at 4:17 p.m., the Committee was adjourned.]

---

<sup>1</sup> The information submitted by Mr. Krebs appears in the Appendix on page 34.

# A P P E N D I X

---

## **“Nomination of Christopher C. Krebs to be Under Secretary, National Protections and Programs Directorate, Department of Homeland Security”**

### **Opening Statement of Chairman Ron Johnson**

**April 25, 2018**

*As prepared for delivery:*

Good morning. We are here to consider the nomination of Christopher Krebs to be the Under Secretary of the National Protection and Programs Directorate within the Department of Homeland Security.

A top priority for the Committee is to ensure that the Department of Homeland Security has the tools and resources in place to effectively secure our nation. That starts with leadership. I am pleased that our Committee has worked in a bipartisan manner to confirm key leadership posts at the Department, during the past and current administrations.

Mr. Krebs is nominated to fulfill a critical position within the Department of Homeland Security. The National Protection and Programs Directorate oversees a wide range of programs and responsibilities to help secure our nation, including:

- Cybersecurity programs that secure federal civilian agency networks, provide services to and support the private sector, and facilitate information sharing with partners;
- Critical infrastructure protection, including working with 16 sectors of industry;
- Emergency communications, such as providing support after disasters;
- Securing the nation's federal buildings by managing the Federal Protective Service;
- Regulating chemical facility security; and
- Managing the Office of Biometric Identify Management.

Needless to say, leading NPPD is a difficult job. As the Committee has heard at several hearings, the nation faces serious cyber-related threats—including nation-state cyber threats against our public and private sector networks. If confirmed, Mr. Krebs will be on the front line of the effort.

Mr. Krebs' experience, which includes both public and private sector work—including serving in a senior position with Microsoft—should serve him well as he takes on the ever-present challenge of mitigating risks to our nation's critical infrastructure. The Committee has heard how the private sector is best positioned to innovate and distribute products and services that will protect us against malicious cyber-attacks. I hope Mr. Krebs will challenge the Department to consider how the federal government can do more to support its partners in the private sector.

This Committee has consistently sought to assist the Department in focusing its cybersecurity and infrastructure protection mission. We included language to reform and rename the National Protection Program Directorate in our bipartisan DHS Authorization bill. More work is needed, and I look forward to partnering with Mr. Krebs to strengthen the Department's cybersecurity and infrastructure protection capabilities.



**U.S. Senate Committee on Homeland Security and Governmental Affairs  
Nomination of Christopher Krebs to be Under Secretary, National Protection  
and Programs Directorate, U.S. Department of Homeland Security**

**April 25, 2018  
Ranking Member Claire McCaskill**

**Opening Statement**

Thank you Mr. Chairman. I appreciate you holding this hearing and I want to thank you, Mr. Krebs, for your willingness to serve.

Today we convene to provide advice and consent for the President's nominee to be Under Secretary of the National Protection and Programs Directorate (NPPD) at the Department of Homeland Security.

NPPD is the DHS component responsible for cybersecurity and infrastructure coordination and protection. The name doesn't exactly roll off the tongue, but we're working on that. This Committee recently passed historic legislation reauthorizing DHS for the first time since its creation, and included in that bill was a measure to rename and reorganize NPPD, transforming it into the Cybersecurity and Infrastructure Security Agency (CISA). I'm hopeful that we can soon make that adjustment law.

While the current name of the Directorate sounds boring and uninspiring, the work NPPD does could not be more important. America continues to face significant threats to our critical infrastructure, both digitally and physically. Earlier this month, we heard from FEMA Director Brock Long about the

Administration's efforts to ensure that our communities are prepared for natural disasters that threaten lives, livelihoods, and infrastructure across the country. At our cybersecurity hearing yesterday, witnesses spoke about the myriad cyber threats facing our nation, including the continuing efforts of foreign actors to undermine our democracy. Yesterday the witnesses also discussed the tools we have in place and under development to tackle those problems and keep our systems and Americans safe. NPPD, and the dedicated women and men who work there, are an essential part of that solution.

I am looking forward to hearing from Mr. Krebs today about his vision for NPPD if he is confirmed by the Senate.

Since last summer, Mr. Krebs has been working two jobs at DHS. He is the Assistant Secretary for the Office of Infrastructure Protection, and simultaneously has been leading NPPD as the Senior Official Performing the Duties of the Under Secretary (SOPDUS). Like NPPD, SOPDUS is also a mouthful, but this hearing is an effort to streamline that title, too.

Mr. Krebs has a lot of experience advising private sector and government officials on cybersecurity and risk management issues. This is his second stint at DHS, having previously served in the George W. Bush Administration as a policy advisor overseeing international infrastructure protection efforts and developing the Chemical Facility Anti-Terrorism Standards (CFATS) program. He re-joined

DHS in March 2017, initially serving as Senior Counselor to Secretary Kelly on cybersecurity, critical infrastructure protection, and national resilience issues. Prior to that, Mr. Krebs worked in a variety of cyber-related positions outside of government, most recently as the Director for Cybersecurity Policy at Microsoft. Because the majority of critical infrastructure in this country is owned and operated by the private sector, NPPD must coordinate and work well with non-government entities. I'm encouraged that Mr. Krebs' unique experience both inside and outside DHS will be an asset to the Directorate.

Mr. Krebs has an impressive resume and background that I believe will enable him to thrive as Under Secretary for NPPD. Given the significant challenges and threats facing our country, it's long overdue that we have someone officially in the Under Secretary role leading this component. I welcome Mr. Krebs' testimony regarding this important post.

Thank you, Mr. Chairman.

**Statement of Christopher Krebs**

**Nominee for Under Secretary for the National Protection and Programs Directorate,  
Department of Homeland Security**

**Before the**

**U. S. Senate Committee on Homeland Security and Government Affairs**

**April 25, 2018**

\* \* \*

Chairman Johnson, Ranking Member McCaskill, and Members of the Committee – Thank you for the opportunity to appear before you today as the President's nominee for Under Secretary of Homeland Security for the National Protection and Programs Directorate (NPPD). I am honored to have been nominated for this position by President Trump, and I am grateful to have Secretary Nielsen's support.

More than anything else, I am especially grateful for the strong support of my family. I would like to take a moment to recognize them and introduce those who have joined us today. First, I would like to thank my parents for providing me the opportunity in life to succeed. I would also like to thank my brothers for keeping me honest and helping me develop my partnership-building skills. I would also like to thank my Father-in-law and Mother-in-Law for being there for me, my wife, and our children. Those kids have also joined us here today. They are what keeps me grounded. I come to work every day to make the world a better, safer place for their future. And last, but certainly not least, I would like to recognize my wife. Without her – her support, her patience, her strength, and her love – I would not be here today.

I also want to thank my friends, coworkers old and new, and everyone else who has supported me on this journey. I am humbled to have their support.

I am fortunate to have served at the Department of Homeland Security in several capacities. I was appointed to my current position as the Assistant Secretary for Infrastructure Protection by the President in August 2017, and I serve concurrently as the Senior Official Performing the Duties of the Under Secretary for NPPD. I have dedicated my career to risk management and critical infrastructure protection in both government and the private sector. I am passionate about this mission, and if confirmed, it will be my great honor to lead the Department's cyber and infrastructure security mission as the Under Secretary for NPPD.

This context is important. In our discussions prior to this hearing, many of you asked what drew me to this position. The answer is simple – I view this position as the pinnacle of national risk management in cyber and physical security. NPPD can do more to advance a national risk management agenda than any other single place in the U.S. government. No single stakeholder has the complete picture necessary to detect emerging systemic risk conditions or comprehensively manage systemic risk, making NPPD's coordination mechanisms, information sharing role, and ability to engage and inform policy- and decision-makers essential to success in our shared homeland security mission.

Success in this mission cannot be possible without the tireless work of NPPD's incredibly talented workforce. They are, without a doubt, our single greatest asset. NPPD employs a workforce of nearly 3,600 federal employees and approximately 18,000 contractors throughout the country. While serving as the senior official for NPPD, I have sought to place the employees first by creating a team-oriented culture; ensuring a diverse and inclusive environment; and helping good ideas rise to the top. If

confirmed, I will continue to look for ways to enhance the morale of the NPPD workforce by tirelessly representing the men and women of NPPD; increasing the visibility of our mission and organization; and assertively engaging leadership, industry, Congress, our stakeholders, and other external audiences.

NPPD's responsibilities have grown substantially since its inception over 10 years ago. This growth is driven by a dramatic shift in the threat environment that few could have anticipated at the Department's creation. Today, we face the challenge of managing risk in both the physical and digital worlds. This risk comes from Mother Nature; a diverse group of threat actors including nation states like Russia, China, Iran, and North Korea; as well as cybercriminals, terrorist groups, and other nefarious actors seeking to take advantage of our open society and the proliferation of technology to do us harm. They attack us anywhere they perceive vulnerability: in the cyber world, through the deployment of tools like BlackEnergy, WannaCry, NotPetya, and SamSam; and in the physical world, by utilizing small arms, improvised explosive devices, vehicles and other readily-available means to target innocent people as we gather to worship, attend a sporting event or concert, travel, or simply transit open public spaces. We must do everything we can to mitigate threats and enhance resiliency of our infrastructure.

The growth in this mission is also driven by our increasing reliance on linked systems and networks. Where it was once possible to define and defend perimeters around single systems or high risk assets, we now face the growing challenge of managing shared risk. To put it most simply, perimeters today often overlap or simply do not exist. As Secretary Nielsen often says, "Your risk is my risk, and my risk is your risk." Industry is shifting towards an integrated risk management approach, and as the leader in the federal government for managing risk to federal networks and national critical infrastructure, NPPD must also integrate this approach into its business model.

In all, I see three primary strategic goals for NPPD. First, NPPD must defend non-national security systems across civilian agencies and secure federal facilities. Second, NPPD must accelerate efforts to manage systemic physical and cyber risk to critical national functions. And third, NPPD must raise the security baseline across the country by providing stakeholders with the scalable tools and resources they need to secure their systems and infrastructure. NPPD must work to accomplish these goals by fostering voluntary, incentive-driven partnerships with a wide range of stakeholders. If confirmed, I will draw on my private sector experience and understanding of the unique value government offers to ensure NPPD emphasizes an approach that is customer-centric and requirements-driven.

Operationally, my top priority as the senior official for NPPD has been enhancing the resilience of our nation's election systems. In the face of unprecedented interference in our 2016 election by Russia, NPPD has worked closely with state and local election officials in thousands of jurisdictions across the country to ensure that each American's vote counts and is counted correctly. If confirmed, I will continue to make this my top priority as the Under Secretary.

If confirmed, I also pledge to work closely with this committee and the Congress to facilitate oversight of NPPD's activities and advance our shared legislative priorities, including restructuring NPPD, enhancing the security of our election systems, reauthorizing the Chemical Facility Anti-Terrorism Standards (CFATS) program, hardening critical infrastructure against vulnerabilities like electromagnetic pulse, and others. I want to thank this committee for including in its recent DHS authorization bill legislation that would transform NPPD into the Cybersecurity and Infrastructure Security Agency. Congress plays an active role in NPPD's success, and I look forward to working with this committee to pass this critical legislation.

Thank you again for the opportunity to appear before you today. I 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
<b>Under Secretary of Homeland Security, National Protection and Programs Directorate</b>	<b>February 13, 2018</b>

<i>Current Legal Name</i>			
First Name	Middle Name	Last Name	Suffix
Christopher	Cox	Krebs	

<i>Addresses</i>					
Residential Address (do not include street address)			Office Address (include street address)		
			Street: 3801 Nebraska Ave, NW		
City: Alexandria	State: VA	Zip: 22302	City: Washington	State: DC	Zip: 20016

<i>Other Names Used</i>						
First Name	Middle Name	Last Name	Suffix	Check if Maiden Name	Name Used From (Month/Year) (Check box if estimate)	Name Used To (Month/Year) (Check box if estimate)
n/a					Est <input type="checkbox"/>	Est <input type="checkbox"/>

<i>Birth Year and Place</i>	
<u>Year of Birth</u> (Do not include month and day.)	<u>Place of Birth</u>
1977	Atlanta, GA

<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>
Emily	Page	Krebs	

<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>	<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)
Emily	Page	Hebda		X	03/1981 Est	10/2006 Est

<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			

## 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>
George Mason University School of Law	Law School	08/2003	05/2007	J.D.	05/2007
University of Virginia	College/University	08/1995	05/1999	B.A.	05/1999
Georgia Perimeter College	College (summer courses)	06/1997	07/1997	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, USPS 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)
Other Federal Employment	Department of Homeland Security	Assistant Secretary for Infrastructure Protection	Washington, DC	08/2017	Present
Other Federal Employment	Department of Homeland Security	Senior Counselor to the Secretary	Washington, DC	03/2017 Est	08/2017 Est
Non Federal Employment	Microsoft	Director for Cybersecurity Policy	Washington, DC	02/2014	03/2017



Federal Contractor	Obsidian Analysis	Principal	Washington, DC	01/2012 Est	02/2014
Federal Contractor	Dutko Worldwide	Vice President	Washington, DC	01/2009 Est	12/2011
Other Federal Employment	Department of Homeland Security	Policy Advisor	Washington, DC	10/2007	01/2009
Federal Contractor	Systems Planning and Analysis	Senior Staff	Alexandria, VA	08/2005	10/2007
State Government	City of Alexandria, Office of the Commonwealth's Attorney	Law Clerk	Alexandria, VA	01/2005	08/2005
Federal Contractor	Intermedia Group, Inc.	Homeland Security Project Coordinator	Washington, Dc	02/2005	08/2005
Federal Contractor	Potomac Management Group	Assistant Project Manager	Alexandria, VA	01/2002	02/2005
Unemployed				10/2001 Est	01/2002 Est
Non Federal Employment	Adams & Garth Staffing	Staff	Charlottesville, VA	09/2001	10/2001
Unemployed				07/2001 Est	09/2001 Est
Non Federal Employment	Gallagher Marine Systems, Inc.	Drills and Training Coordinator	Alexandria, VA & Philadelphia, PA	04/2000	07/2001
Non Federal Employment	Applied Environmental, Inc.	Industrial Hygienist	Arlington, VA	12/1999	04/2000
Unemployed				08/1999 Est	12/1999 Est
Non Federal Employment	University Dive Center	Shop Manager	Charlottesville, VA	10/1997	08/1999

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

Name of Government Entity	Name of Position	Date Service Began (month/year)	Date Service Ended (month/year) (check box if estimate) (check
---------------------------	------------------	---------------------------------	--

		(check box if estimate)	"present" box if still serving)
n/a			

#### **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.**

I previously worked for Microsoft Corporation, a large information technology company with significant U.S. Government sales and contracts.

In connection with the nomination process, I have consulted with the U.S. Office of Government Ethics and the U.S. Department of Homeland Security's Designated Agency Ethics Official (DAEO) to identify any potential conflicts of interest. Any potential conflicts of interest will be resolved in accordance with the terms of the ethics agreement that I signed and transmitted to the Department's DAEO, which has been 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.**

During my tenure as Director for Cybersecurity Policy at Microsoft, I worked closely with colleagues at the company and in industry to develop policy positions on matters that impacted our collective interests, including but not limited to the Cybersecurity Act of 2015, encryption policy, cross-border data flows, Wassenaar Arrangement, supply chain, and other policy issues. I also worked to ensure those positions were used to inform the company's legislative and government affairs engagement strategies, and met occasionally with congressional staff to discuss those issues.

#### **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.

Partial athletic scholarship to the University of Virginia for track and field. 1995 – 1996.

## 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>
American Bar Association	08/2013-08/2014; 01/2006-08/2007	Member
Virginia State Bar	10/2007-Present	Associate Member
National Cyber Security Alliance	12/2016-03/2017	Vice Chair

## 7. Political Activity

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

No.

<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.

None.

<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.

None.

<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>
Secretary Napolitano: The First Week, Seven Directives	Securitydebrief.com	1/26/2009

- (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>
--------------------	-----------------------	--------------------------

Hearing: Examining DHS's Cybersecurity Mission	House Committee on Homeland Security / Cybersecurity and Infrastructure Protection Subcommittee	10/03/2017
Hearing: Roles and Responsibilities for Defending the Nation from Cyber Attack	Senate Armed Services Committee	10/19/2017
Hearing: Cybersecurity of Voting Machines	House Oversight and Government Reform Committee / Subcommittee on Information Technology and Subcommittee on Intergovernmental Affairs	11/29/2017

(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>
International Cyber Crime Arrests through Private/Public Collaboration	RSA Conference 2012 – Panel participant	03/01/2012
Cybersecurity, Technology, and Social Networking in Crisis Management	RSA Conference 2013 – Panel participant	02/28/2013
Keynote Address: Challenges in Cybersecurity	2014 Minnesota Governor's Homeland Security and Emergency Management Conference	02/14/2014
Closing Remarks: Looking Ahead: Key Transatlantic Challenges in Cyberspace	Mini-Conference hosted by Carnegie Endowment for International Peace & Microsoft Innovation & Policy Center	12/15/2016
Fundamentals of Incident Response	Homeland Security Law Institute, Washington, DC – Panel participant	09/26/2017
Remarks on Cybersecurity	Internet Security Alliance Fall 2017 Board Meeting, Ernst & Young, Washington, DC – Extemporaneous remarks	09/26/2017
Remarks on Cybersecurity	4th annual CA Technologies Government Summit: "Let's Talk" Washington, DC – Extemporaneous remarks	10/12/2017
Cybersecurity Forum 2017	Information Technology Industry Council and Hogan Lovells, Washington, DC – Panel participant	10/19/2017

Mozilla Cyber(in)security Summit	Half-Day Summit hosted by Mozilla, Washington, DC – Panel participant	10/24/2017
Reality Check: Securing the Internet of Things	Morning Summit hosted by Bloomberg Government and Visa, Washington, DC – Panel Participant	10/25/2017
Remarks on Cybersecurity	Wall Street Journal Pro Cybersecurity Executive Forum, New York, NY – Extemporaneous remarks	12/13/2017
Planning Now, Looking ahead to November 2018	National Association of Secretaries of State 2018 Winter Conference – Panel participant	02/17/2018

### 9. Criminal History

Since (and including) your 18<sup>th</sup> 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.)

Yes.

- 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?

Yes.

- 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:

08/1995

a. Is this an estimate?

Yes.

B) Description of the specific nature of the offense:

In August 1995, I was ticketed for Minor in Possession of Alcohol. I was 18 at the time and in college.

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:

No.

2) Firearms or explosives:

No.

3) Alcohol or drugs:

Yes.

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

Madison County, Virginia, 22727, USA

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, I received a ticket and summons to appear.

1) Name of the law enforcement agency that arrested/cited/summoned you:

Madison County Sheriff

2) Location of the law enforcement agency (city, county, state, zip code, country):

538 South Main Street, Madison, VA 22727, USA

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.

1) If yes, provide the name of the court and the location of the court (city, county, state, zip code, country):

Madison County Circuit Court, 1 Main Street, Madison, VA 22727-0220

- 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:

I was charged with Minor in Possession of Alcohol, and I pleaded guilty.

- 3) If no, provide explanation:

n/a.

- G) Were you sentenced as a result of this offense:

Yes.

- H) Provide a description of the sentence:

I was fined, charged for court costs, and my license was suspended for 90 days. I paid the fine, and the charge was expunged from my record.

- I) Were you sentenced to imprisonment for a term exceeding one year:

No.

- J) Were you incarcerated as a result of that sentence for not less than one year:

No.

- K) If the conviction resulted in imprisonment, provide the dates that you actually were incarcerated:

n/a

- L) If conviction resulted in probation or parole, provide the dates of probation or parole:

n/a

- M) Are you currently on trial, awaiting a trial, or awaiting sentencing on criminal charges for this offense:

No.

- N) Provide explanation:

In August of 1995, I was 18 years old and beginning my first year of college. The vehicle I was riding in was pulled over for speeding. I had a beer in my hand, and I was subsequently charged with Minor in Possession of Alcohol. I pleaded guilty with explanation. My license was suspended for 90 days, and I was fined. After the 90-day period, my license was reinstated and the charge was expunged from my record.

# **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**

**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)


### 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)

### 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.



This 22 day of Feb, 2014

**REDACTED**UNITED STATES OFFICE OF  
GOVERNMENT ETHICS  
★

February 20, 2018

The Honorable Ron Johnson  
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 Christopher C. Krebs, who has been nominated by President Trump for the position of Under Secretary, National Protection and Programs Directorate, 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

David J. Apol  
Acting Director and General Counsel

Digitally signed by DAVID APOL  
DN: cn=DAVID APOL, o=Office  
of Government Ethics, ou=U.S. Government, email=DAVID.APOL@  
O.E.G.E., c=US, postalCode=20541, serial=1001, version=3  
Date: 2018.02.20 19:04:41 -0500

Enclosures **REDACTED**

February 15, 2018

Joseph Maher  
Designated Agency Ethics Official  
Department of Homeland Security  
Washington, D.C. 20528-0485

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 Under Secretary, National Protection and Programs Directorate, Department of Homeland Security.

As required by 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 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 officer, director, trustee, general partner or employee; and any person or organization with which I am negotiating or have an arrangement concerning prospective employment.

I terminated my employment with Microsoft Corporation on March 18, 2017. I will not participate personally and substantially in any particular matter involving specific parties in which I know Microsoft is a party or represents a party for a period of one year after I terminated my employment at Microsoft, unless I am first authorized to participate, pursuant to 5 C.F.R. § 2635.502(d).

I resigned from my position with the National Cybersecurity Alliance on March 16, 2017. For a period of one year after my resignation from the National Cybersecurity Alliance, I will not participate personally and substantially in any particular matter involving specific parties in which I know that the National Cybersecurity Alliance is a party or represents a party, unless I am first authorized to participate, pursuant to 5 C.F.R. § 2635.502(d).

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 or municipal bonds that qualify for the exemption at 5 C.F.R. § 2640.201(a), or obligations of the United States.

I will meet in person with you during the first week of my service in the position of Under Secretary in order to complete the initial ethics briefing required under 5 C.F.R. § 2638.305. Within 90 days of my confirmation, I will document my compliance with this ethics agreement by notifying you in writing when I have completed the steps described in this ethics agreement.



I understand that as an appointee I must continue to abide by the Ethics Pledge (Exec. Order No. 13770) that I previously signed and that I will be bound by the requirements and restrictions therein in addition to the commitments I have made in this ethics agreement.

I have been advised that this ethics agreement will be posted publicly, consistent with 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

A handwritten signature in black ink, appearing to read 'C. Krebs', with a stylized flourish at the end.

Christopher C. Krebs

**U.S. Senate Committee on Homeland Security and Governmental Affairs**

**Pre-hearing Questionnaire**

**For the Nomination of Christopher C. Krebs to be  
Under Secretary of Homeland Security – National Protection and Programs Directorate  
Department of Homeland Security**

**I. Nomination Process and Conflicts of Interest**

1. Did the President give you specific reasons why he nominated you to be the next Under Secretary of Homeland Security – National Protection and Programs Directorate (NPPD) at the Department of Homeland Security (DHS or the Department)?

**While I have not had a conversation with the President about my nomination, I understand the Secretary recommended my nomination to the President. I have worked closely with the Secretary for years, and I share her priorities and approach to cybersecurity and critical infrastructure security.**

2. Were any conditions, expressed or implied, attached to your nomination? If so, please explain.

**No, other than to uphold and defend the Constitution, implement the laws of our Nation, and ensure the security of the American people.**

3. Have you made any commitments with respect to the policies and principles you will attempt to implement as Under Secretary? If so, what are they, and to whom were the commitments made?

**No. I am committed only to uphold the Constitution, obey and enforce the laws of our country, and support the men and women of NPPD that work every day to protect our Nation's infrastructure, physical or digital.**

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.

**I have discussed my nomination and related conflict of interest obligations with the DHS Designated Agency Ethics Official to identify any potential conflicts of interest. I submitted my ethics agreement to the Office of Government Ethics and subsequently to the Committee. I have recused myself from particular matters associated with Microsoft and the National Cyber Security Alliance (NCSA). I will follow policies and accepted practices in ensuring that the appropriate senior official(s) at the Department executes any responsibilities that may be covered by the recusal.**

## II. Background of the Nominee

5. What specific background, experience, and attributes qualify you to be the Under Secretary?

My experience working to protect physical and cyber critical infrastructure in both government and industry qualifies me to serve as the Under Secretary. But perhaps more importantly, my understanding of NPPD's mission, my familiarity with its capabilities, and my experience with what the organization needs to be successful are what positions me for success in this role. Having worked at DHS, within NPPD, and as a private sector stakeholder in our shared cybersecurity and critical infrastructure mission, I have a unique perspective on what historically has worked in this mission space, and what has not. Having spent most of my career in this mission space, I bring a wealth of institutional knowledge, combined with a broad understanding of where NPPD can best support federal and private sector efforts. More specifically, I am intimately familiar with the voluntary nature of NPPD's critical infrastructure protection mission, and have demonstrated success throughout my career in building partnerships to achieve shared infrastructure security outcomes, dating back to the establishment of the National Infrastructure Protection Plan (NIPP), but also including my role as a facilitator in the development of the National Institute of Standards and Technology's (NIST) Cybersecurity Framework, a contributor to the National Cybersecurity Incident Response Plan, and other national cybersecurity policies. I believe I am the right leader at the right time to help NPPD focus on its core missions and become the premier cybersecurity and infrastructure protection agency this country deserves. I know the mission, I know the organization, and I know what NPPD's stakeholders need from their federal partners.

6. Please describe your experience working in the private sector and how it relates to the mission of the NPPD.

My experience in the private sector, both advising critical infrastructure companies and working in a large technology company, has afforded me the opportunity to refine my understanding of the appropriate balance between government and industry, as well as the shared responsibility in securing our nation's infrastructure. More specifically, I understand the unique value that government offers to the private sector, such as information and intelligence sharing, developing a shared understanding of national risk, or the ability to facilitate actions that reduce federal barriers to private sector action. It is these areas, particularly those where there is no existing private sector capability or no viable business model within industry, where NPPD can make the most impact in managing critical infrastructure and cybersecurity risk. Ultimately, NPPD is an organization that has little ability to compel action, so instead, we must find ways to provide capabilities or services that add value for our customers and stakeholders and fill capability gaps.

## 7. Please describe:

## a. Your leadership and management style.

I lead by setting forth and communicating a vision of success. I provide team members with the resources and guidance necessary to achieve that vision, and I hold both them and myself accountable for achieving it. I am a firm believer in helping the team understand the importance of accomplishing a task and what success looks like, but I encourage the team to identify its own path to achieve success. This outcomes-based approach to leadership is critical in the dynamic cybersecurity mission area, as it emphasizes a team approach and encourages an array of inputs and perspectives – there is no single correct answer, and innovation, critical thinking, and diversity of opinion will increase our likelihood for success. I also encourage team members to consider their approach to every opportunity before them and then determine whether leading, supporting, or focusing their efforts elsewhere will help the team achieve our shared objectives. Within this leadership style, accountability is a critical component, as is ensuring that the team understands that success is rewarded, and that falling short of goals presents opportunities to improve and correct.

My management style is similarly rooted in clearly communicating expectations and roles to team members, empowering them to complete tasks as assigned, and ensuring that they have the resources to be successful. I also believe that large, dispersed organizations require thoughtful delegation of management and decision-making authorities in order to succeed. As a part of this approach, my management style emphasizes ensuring the right people are in the right jobs with the right responsibilities. This means each job or role has an expected function or task assigned to it and, as a part of a team, each team member is expected to do his or her part. Everyone has the opportunity to be successful, and the opportunity to find the right fit. Again, accountability is critical to ensuring success as a team. I believe in building a management team that understands their roles and lanes, and empowering them to lead and make decisions, while rewarding innovative approaches and critical thinking.

## b. Your experience managing personnel.

I have managed people and teams of different sizes and complexities over the course of my career, from small, high performing teams to thousands of geographically-dispersed employees. My management experience culminated in my current role as the Senior Official Performing the Duties of the Under Secretary (SOPDUS), where I have managed the NPPD workforce since August of 2017. I value open communication, transparency, and setting clear expectations. Regardless of the number of employees I have managed, I have always viewed the workforce as a team, and ultimately the most important asset in executing our mission. My priorities are empowering, guiding, and most critically growing employees.

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

**In my current role as the SOPDUS of NPPD, I have the privilege of leading a federal workforce of approximately 3,600 FTE.**

### **III. Role of the Under Secretary of Homeland Security – NPPD**

8. Please describe your view of the NPPD's core mission and the Under Secretary's role in achieving that mission.

**NPPD's core mission is clear – (1) protect federal networks and facilities, (2) identify and manage physical and cyber systemic risk to critical infrastructure, and (3) raise the security baseline across the Nation's critical infrastructure. The Under Secretary's role is to look across the risk landscape to anticipate emerging risks to infrastructure, look to DHS leadership to anticipate and understand priorities, and help inform decision-making processes. More directly, the Under Secretary ensures the organization as a whole is well-positioned to manage risk, provide clear strategic guidance and direction to operational subcomponents, and ensure that the operational subcomponents have the mission support needed to be successful. The Under Secretary must also guide strategic positioning for NPPD, including messaging, engaging external audiences, and visibly representing the organization.**

9. In your opinion, is NPPD currently fulfilling its cybersecurity responsibilities? If not, what would you do differently as Under Secretary?

**I believe NPPD is fulfilling our cybersecurity responsibilities. But we can always do more, and if confirmed, I will continue to push the organization to keep reaching for new and innovative ways to fulfill the cybersecurity mission. With emerging cybersecurity threats and new vulnerabilities, NPPD must continue to execute our authorities, enhance collaboration with our stakeholders, and keep striving to align our services with requirements from our government and critical infrastructure partners. Cyber by its very nature tends to move more quickly than government responds or intelligence operates, so my goal is to increase information and intelligence sharing with our stakeholders, decrease the time it takes to react, and continue investments in automated tools that can enable us to take proactive action to reduce vulnerabilities and mitigate potential threats.**

**As the SOPDUS, cybersecurity is my top priority, and I engage regularly with the NPPD cybersecurity leadership team to ensure we are keeping pace with demand from our partners within government and the private sector. I am confident in the NPPD cybersecurity leadership team's ability to continue executing the Department's authorities and responsibilities in this critical mission area.**

10. In your opinion, is NPPD currently fulfilling its responsibilities for critical infrastructure security? If not, what would you do differently as Under Secretary?

Under the *Homeland Security Act of 2002*, and amplified by *Presidential Policy Directive 21 – Critical Infrastructure Security and Resilience*, the Department of Homeland Security is responsible for providing strategic guidance on the protection of critical infrastructure, promoting a national unity of effort, and coordinating the overall federal effort to promote the security and resilience of the Nation's critical infrastructure. Various additional authorities, directives, and orders, such as the *Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014* and *Executive Order 13636 - Improving Critical Infrastructure Cybersecurity*, help to clarify or expand upon the Department's critical infrastructure security responsibilities. Within the Department, many of the critical infrastructure security responsibilities assigned the Department are delegated to NPPD.

NPPD engages in a variety of activities in order to meet these responsibilities. In general, these activities include assessing vulnerabilities at the asset and system levels; sharing strategic risk analysis and timely, actionable information; and providing tools and training to mitigate identified risks. While I believe NPPD is fulfilling its responsibilities for critical infrastructure security, I also believe that there are ways in which NPPD could do so more efficiently and effectively.

If confirmed, one of my top priorities would be to ensure that NPPD uses sound risk management practices to secure critical infrastructure in the most cost-effective manner possible. To fulfill this priority, I would review existing NPPD programs against the current risk landscape to ensure NPPD's resources are properly aligned to actual risk; track, analyze, and share information on emerging threats to help critical infrastructure owners and operators build in security and resilience to potential threats as they construct or upgrade the Nation's infrastructure; and routinely engage critical infrastructure owners and operators to understand their needs and work with them to design trainings, assessments, and other services to most efficiently and effectively meet their needs.

#### IV. Policy Questions

##### *Management, Workforce and Accountability*

11. What do you believe are the most pressing internal and external challenges currently facing NPPD? Which challenges will you prioritize and what do you plan to do to address each of those challenges?

Internally, NPPD must continue to mature, consolidate, and integrate its management functions and business processes in order to effectively and efficiently execute its role as lead for securing cyberspace and critical infrastructure. As NPPD evolves, it must continue to develop in-house capability for human capital, facilities management, budget, strategic planning, external affairs, and other mission-enabling business management activities, and reduce reliance on support from the Department. I believe this can be accomplished by establishing a dedicated management and mission support element to execute these functions centrally for

NPPD and provide executive oversight, clear direction on roles and responsibilities within the organization, and accountability for strategic, management, and operational roles. If confirmed, working with the Secretary and the Department's Management Directorate, one of my top priorities will be to ensure that the entire NPPD leadership team – including subcomponent leadership – has clear direction on, and a shared understanding of, NPPD organizational roles and responsibilities.

Externally, we must improve our relationships with private sector and government partners in order to better execute our mission, with a focus on delivering stakeholder-defined, requirements-based services and capabilities. As a part of this process, we must ensure our stakeholder engagement mechanisms are appropriately focused and inclusive of the critical infrastructure community. While we have established relationships with numerous critical infrastructure owners and operators via our partnership mechanisms, our information sharing mechanisms, and our operational relationships, there are thousands of other organizations that lack a full understanding of DHS' capabilities and service offerings. Those organizations therefore do not draw on our support to prepare for or respond to an incident. It is especially important with our growing role that federal and nonfederal cybersecurity partners know who we are, what our mission is, and what services and assistance are available.

These external and internal challenges are linked, and overcoming them will be my top priorities. If confirmed, I will address these challenges by setting expectations for internal and external success, ensuring we have the right leadership in place to achieve this success, and holding both that leadership and myself accountable for achieving this success.

12. In your view, what are the highest priorities in both urgency and importance for enhancing cybersecurity and critical infrastructure? Why?

Within NPPD's authorities, I recognize three key priority areas in terms of cybersecurity and critical infrastructure:

- (1) **Protecting Federal Networks:** DHS must continue to prioritize working with our federal executive branch partners to secure and defend non-national security systems across civilian agencies. Given the Secretary's risk management authorities under FISMA, NPPD has the ability to manage cybersecurity risk most directly across federal networks. Using the tools and capabilities of the Department, including the National Cybersecurity Protection System (NCPS), Continuous Diagnostics and Mitigation (CDM) program, and our incident response capabilities, NPPD can continue to help agencies improve their network protection posture.
- (2) **Managing National and Systemic Critical Infrastructure Risk:** DHS must continue to work with the infrastructure community to evolve our understanding of critical infrastructure risk, understand core infrastructure

functions that, if compromised, pose the greatest risk to our economy and national security preparedness. These functions include a broad range of services across various sectors including electricity delivery; key financial services activities (e.g., wholesale payment systems); positioning, navigating, and timing (PNT); and cloud computing and managed services. By focusing on these systems or activities that underpin key services, we can prioritize our efforts, drive down risk, and increase resilience across cyberspace. This mission area is critical as no one stakeholder has complete risk information to detect emerging systemic risk conditions or completely manage systemic risk, making NPPD's coordination, information-role, and ability to engage and inform policy and decision makers essential.

- (3) Raising the security baseline across the critical infrastructure community – providing scalable tools and resources for the critical infrastructure, more broadly, to enhance security, improve resilience, and reduce risk to their own systems and assets.

Within this prioritization framework, we can focus efforts to achieve the most effective approach to critical infrastructure risk management.

In addition, the 2016 elections demonstrated clearly that nation-state adversaries seek to undermine confidence in one of our core values as a democratic society – free and fair elections. Strengthening the resilience and security of the state and local systems that administer our elections is my top priority. As the SOPDUS, I led efforts to coordinate with federal agencies and support state and local election officials with their responsibility to administer elections within their jurisdiction. I am pleased with the progress made so far establishing transparent and repeatable processes and procedures to help share the information, intelligence, and best practices our state and local partners need to better protect their systems.

Another top priority of mine is the protection of government networks. The federal government collects vast amounts of information as it works to carry out its essential functions, and the American public trusts us to keep that data safe. Our adversaries, from nation-state actors to common criminals, are constantly looking for paths into networks across the .gov and .mil domains. If confirmed, I will work to ensure NPPD along with our partner departments and agencies have the tools and capabilities they need to properly secure government networks and protect our information, national secrets, and critical infrastructure and systems from those seeking to do us harm.

An additional top priority is to better apply risk management to NPPD's critical infrastructure protection mission. Critical infrastructure across the nation faces new and constantly emerging threats from cybercrime to intellectual property theft to malicious nation-state activity. These threats affect the full range of critical infrastructure across and throughout all sectors – not just the most obvious targets in each sector. In a world of finite resources and seemingly infinite threat vectors,



we must ensure decision-makers have all the information they need to manage risk and protect their systems and infrastructure against known threats and vulnerabilities. If confirmed, I will work to ensure NPPD is communicating all known threat and vulnerability information to our critical infrastructure stakeholders and enabling them to prioritize their mitigation efforts according to risk.

13. What measurements would you use to determine whether your office is successful?

Measuring success for any homeland security enterprise is challenging because usually success means we have prevented something from happening. For NPPD, success means we are receiving and sharing information in a timely manner, deploying resources where requested by our stakeholders, and providing actionable security recommendations which will raise the overall level of security across the nation. However, recognizing that perfect security is virtually impossible, we will continue moving towards an “assume breach” posture, ensuring that we are prepared to minimize the damage an attacker can inflict. Useful metrics in this vein are (1) time to detection of the adversary, (2) time to investigate the attack, and (3) time to mitigate the damage and evict the adversary. Our goal should be to get these time values to hours if not minutes, where they may now be weeks or even months.

I will also track trends that provide insight into our overall level of security and the usefulness of the products and services we offer, such as rate of compliance with DHS Binding Operational Directive mandates, our ability to implement cybersecurity hygiene practices across federal networks, and increases in the use of DHS services and capabilities by our stakeholders.

14. What do you consider to be the principal challenges in the area of human capital management at NPPD?

Without question, the principal human capital management challenge facing NPPD is the ability to recruit and retain cybersecurity personnel. Managers often become overwhelmed responding to the day’s tasks and have little time to spend planning aggressive hiring strategies. And when they do find the time to begin filling out their teams, they are hamstrung with cumbersome and outdated HR systems and hiring procedures. As SOPDUS, I have already directed my staff to explore every possible approach to strengthen our cyber workforce, and if confirmed, I will ensure we continue executing on those lines of effort.

Another principal human capital management challenge at NPPD is morale. As the latest federal Employee Viewpoint Survey shows, NPPD ranks very low in leadership and workplace satisfaction scores. Strengthening morale starts at the top, so it is important that NPPD have a confirmed leadership team in place to set a clear vision for the organization. If confirmed, I will work to communicate that vision to the men and women of NPPD, to empower them to perform their duties, to

ensure they have the tools they need to do their jobs, to hold them and myself accountable, and to have their backs when they need it.

15. What do you consider to be the principal challenges facing management of the NPPD?

NPPD's success is dependent upon our employees successfully executing their individual piece of the whole mission. However, NPPD has faced significant uncertainty over the last few years regarding what the organization will look like in the future. This uncertainty makes it extremely challenging for management to motivate employees and encourage integration among operating units. If confirmed, I look forward to continuing to work with Congress to establish the Cybersecurity and Infrastructure Security Agency and begin building the premier cybersecurity and infrastructure protection agency this nation deserves.

- a. What experience from your past positions best equips you to address these challenges?

Over the course of my service at DHS, where I began as an onsite contractor, moved up through the ranks to become an advisor to an Assistant Secretary, a counselor to the Secretary, an Assistant Secretary, and now the SOPDUS for NPPD. Through this experience, I developed a unique perspective of the management challenges facing NPPD. I have a clear sense of what it takes to be successful at NPPD, having seen various approaches succeed, and other approaches fail. If confirmed, I will draw on my experiences at DHS to ensure management priorities and direction are clearly communicated to the entire NPPD leadership team, and that those leaders are empowered to execute strategies that advance those priorities. Above all, I will promote a culture of professionalism and respect, where performance is acknowledged and rewarded, constructive guidance is delivered in a way that is actionable, and leaders are held accountable.

16. How would you handle employee disciplinary issues within NPPD? How would you respond to underperforming employees within NPPD?

As the SOPDUS, I am familiar with how employee disciplinary actions are handled. For employee disciplinary matters, NPPD follows DHS management directives, which provide policy and guidance for administering the DHS Employee Discipline and Adverse Actions Program. Actions taken pursuant to this program comply with the requirements of all pertinent laws, rules, regulations, and Office of Personnel Management guidance, and they ensure due process.

It is important in any disciplinary process that penalties are fair and transparent. To that end, NPPD utilizes a table of penalties, which serves as a guide to offenses and penalties for managers, supervisors and human resource professionals to use in determining the appropriate penalty when taking

disciplinary or other adverse actions in response to employee misconduct. The NPPD table of penalties mirrors and in some cases augments the DHS table of penalties.

For responding to underperforming employees, it is important that we provide managers with the tools they need to manage their direct-reports, and that we hold managers accountable for the overall performance of their team. NPPD managers have a multitude of tools, including performance guides that support NPPD's goal of promoting and sustaining a high-performance culture. This guidance is posted on NPPD's intranet sites and is available for all supervisors and employees at NPPD.

There are also ways to help employees enhance their work performance before it becomes a problem, such as training, peer assistance, performance counseling, and performance improvement plans. NPPD uses all of these avenues to help enhance employees' work performance. The Office of Human Capital also issues written annual, mid-cycle and end-of-year guidance on the performance management process generally, including ways to deal with poor performance Agency-wide. To assist managers, the Office of Human Capital also provides "Performance Improvement Process" Job Aid designed to provide an overview of the performance improvement process and recently added a section to its supervisory training offerings that helps managers find ways to deal with poor performers.

And finally, NPPD also utilizes quarterly progress reviews to encourage supervisors to conduct continuous and informal performance progress discussions with employees throughout the year. This helps managers and employees engage in a regular dialogue about performance, making it easier to collectively identify and correct any underperformance before the end of the rating period.

This is an overview of the measures in place to help managers handle employee disciplinary and performance issues. If confirmed, I would work to ensure NPPD continues executing on these lines of effort.

17. While serving as the Senior Official Performing the Duties of the Under Secretary for NPPD, what policies have you initiated, implemented, or improved to enhance morale in NPPD?

During my tenure, I have sought to place our employees first – instituting policies that ensure employees hear from me as to why it is we do what we do, create a team-oriented culture, protect and empower the worker, and give opportunities for good ideas to rise to the top. First and foremost, I have overseen implementation of a robust communications campaign to better engage the workforce. This campaign includes messages from the SOPDUS, a weekly e-newsletter called "Vision," a daily NPPD Operations Infographic, a DHS News Briefing, and the new "NPPD At A

Glance” - an initiative to help highlight some of the great work going on at NPPD and more effectively communicate NPPD’s capabilities and accomplishments to our stakeholders. We are also actively participating in the DHS Leadership Year to include hosting a series of events that connect leadership and the workforce. I have participated in the annual NPPD annual awards ceremony to recognize employee accomplishments. During my tenure, we have also taken steps to enhance the NPPD Diversity and Inclusion Council, which is charged with developing program activities that foster a more inclusive and collaborative work environment. Recognizing the important role health and well-being play in morale, we established a work/life program with educational events and activities, including the implementation of the Workplace Fitness Program that permits employees to devote a portion of their work week toward exercise. This is an overview of some of the policies and procedures NPPD has implemented during my tenure. If confirmed, I will continue to look for opportunities to enhance the morale of the NPPD workforce by fearlessly representing the men and women of NPPD; increasing the visibility of our mission and organization; pushing out our products, capabilities, and service offerings; and assertively engaging leadership, industry, Congress, our stakeholders, and other external audiences.

18. If confirmed, will you work to ensure that GAO and the Inspector General have the access they need to carry out their evaluation, audit, and investigation functions?

If confirmed, I would work to ensure these entities continue to receive access to NPPD in accordance with all applicable federal laws and regulations.

19. Protecting whistleblower confidentiality is of the utmost importance to this Committee,

- a. During your career within the private sector, how did you handle similar issues?

I have always followed whistleblower protection laws, though to my knowledge I have never formally received a whistleblower complaint. If confirmed, I will comply with all whistleblower, laws, rules and regulations.

- b. How do you plan to implement policies within NPPD to encourage employees to bring constructive suggestions forward without the fear of reprisal?

Having served as the SOPDUS since August 2017, I am familiar with existing NPPD and DHS policies that ensure employees have the ability to share constructive input without fear of reprisal. A strong leader trusts his or her employees to execute the mission every day, and constructive feedback from those closest to the mission is a great way for leadership to find opportunities for improvement. If confirmed, I will work to ensure policies in this area continue to be communicated clearly and frequently to the workforce so we do not miss any opportunities to improve.

The NPPD Open Door Policy is currently under development by the Office of Human Capital. This policy will encourage employees to provide constructive feedback and input to their managers and leadership without suffering adverse consequences or fear of reprisal.

Additionally, NPPD employees are covered by DHS policies that provide employee protections for reporting impropriety and illegality, and further encourage them to bring forward constructive suggestions, noteworthy achievements, and recommendations to improve service to the public. The policies providing coverage are as follows:

- DHS Human Relations Directive MD250-04 (protects whistleblowers)
- DHS Employee Recognition Guide 255-02-001, Instruction 255-03-001
- DHS Anti-Harassment Directive 256-01; (mandatory annual training for all DHS employees)
- DHS Administrative Grievance system Instruction 256-02-001

- c. Do you commit without reservation to work to ensure that any whistleblower within NPPD does not face retaliation?

**If confirmed, I will work to ensure any whistleblower within NPPD does not face retaliation, in accordance with all applicable federal law.**

- d. Do you commit without reservation to take all appropriate action if notified about potential whistleblower retaliation?

**If confirmed, I will take all appropriate action in accordance with all applicable federal law.**

#### *Cybersecurity*

20. Cyber threats are increasing on a daily basis. What do you view to be the most significant current and potential cybersecurity threats facing our nation?

I generally group cybersecurity threats into two categories: opportunistic threats and targeted threats. In the former, particularly broader campaigns or opportunistic attacks like ransomware attacks, cyber threat actors – nation state or cybercriminal – use the same tactics over and over to gain unauthorized access to networks. Their jobs are made easier due to the general lack of knowledge of basic cyber hygiene and best practices in our country throughout both government and the private sector. We often find that networks are left wide-open due to outdated or unpatched software, generic administrative log in/passwords, loose administrative privileges, or a lack of knowledge about how to deal with simple phishing campaigns. Targeted threats are generally more nefarious, and can utilize the same types of known vulnerabilities as well as lesser-known, more sophisticated avenues of attack.

We have made substantial progress raising the overall level of cybersecurity in our federal civilian networks by deploying capabilities and tools in these networks, as well as by issuing several Binding Operational Directives to compel specific actions, helping protect against much of the opportunistic attacks. However, to better protect against both opportunistic and targeted threats, we must continue to shift toward a layered defense model that not only focuses defense efforts at the perimeter but also emphasizes the detection, rapid investigation, and mitigation of potentially nefarious activity. We can make this process more effective by limiting administrative access and privileged accounts across networks, but also segmenting networks to limit lateral movement. If confirmed, I will continue ongoing efforts at NPPD to engage our partners and stakeholders to share information about known vulnerabilities, patches and best practices, and enhance our service offerings for the protection of networks and the testing of system resilience and security.

21. If confirmed, what steps do you intend to take to improve the nation's cybersecurity, both with respect to the government and private networks?

Safeguarding and securing cyberspace is a core homeland security mission. Malicious cyber actors target the paths of least resistance, lowest effort for the biggest payoff, and simplicity. Many information technology system compromises exploit basic vulnerabilities such as email phishing, insecure password practices, default and improper configuration, and poor patch management. As indicated in my response to Question 20, if confirmed, I will work to continue ongoing efforts to engage our partners and stakeholders to share information about known vulnerabilities, patches, and best practices, and enhance our services offerings for the protection of networks and the testing of system resilience and security. Progress made on these fronts will measurably decrease the Nation's cybersecurity risk.

It is also critical that NPPD enhance its network protection efforts by constantly improving our capability and service offerings and assisting our partners with the deployment of tools and capabilities to protect their networks. If confirmed, I will work to provide our partner organizations with information and technical capabilities they can use to secure their networks, systems, assets, information, and data by reducing vulnerabilities, ensuring resilience to cyber incidents, and supporting their holistic risk management priorities. I will also continue to engage stakeholders by providing timely and operationally-useful cybersecurity threat information that assists government and private sector partners with the prioritization and management of cybersecurity risks. I will also work to continue promoting the standardization of information technology and cybersecurity capabilities that enable our partners to control cybersecurity costs, improve asset management, and enhance incident detection, reporting, and response capabilities.

And finally, we must continue working with our federal and private sector partners to manage cybersecurity risk to our nation's most critical infrastructure. As outlined in Section Nine of Executive Order 13636, NPPD fulfills the Department's

responsibility to identify these entities by applying a risk-based approach to determine where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security. Once we have identified these entities, it is incumbent upon us to work with the relevant federal partners and the infrastructure owners to enhance their systems' security and resilience. If confirmed, I will work to expand our efforts to protect these so-called "Section Nine" entities by applying a collaborative approach to risk management that leverages knowledge and expertise from public and private sector partners and Sector-Specific Agencies.

22. Please describe your views on the appropriate role of private sector entities in working with DHS to improve our nation's cybersecurity.

The private sector is a critical stakeholder in our collective efforts to improve the security and resilience of our nation. They own the overwhelming majority of the U.S. critical infrastructure, and as a result, their individual risk posture influences the security of our nation. Through increased information sharing and situational awareness, robust policy discussions at Sector Coordinating Councils (SCC), operational coordination during incidents with individual companies and their Information Sharing Analysis Centers (ISACs), and other similar engagements, we have increased our mutual cooperation over the last decade and improved our collective ability to manage risk and mitigate threats. Having worked in and with the private sector throughout my career, I know firsthand the benefits of these key stakeholder partnerships and the role stakeholders can play in enhancing the security of our nation. The federal government must continue to engage, partner with, and enlist the help of the private sector to help better defend our networks and critical infrastructure against cybersecurity threats and vulnerabilities.

23. Today there are more than 20 agencies across the federal government with roles and responsibilities associated with U.S. cyber capabilities.

- a. What is your understanding of the NPPD's responsibilities for cybersecurity, and what role do you believe NPPD should play in relation to these other agencies?

**NPPD's cybersecurity responsibilities focus on two key areas: federal network protection efforts and critical infrastructure cybersecurity efforts.**

On federal network protection, DHS has specific authorities under FISMA to protect federal networks. These authorities enable the Secretary to issue Binding Operational Directives for specific network protection activities, but also manage and deploy technical services like the NCPS and CDM. DHS serves as a centralized point for network protection coordination and risk management. CDM gives DHS the ability to understand risk to federal networks more broadly, identify activities in one agency that could be affecting other agencies, and lead broader incident response and threat hunting activities.

Concerning the cybersecurity of critical infrastructure, NPPD plays a key role in coordinating national cybersecurity network protection efforts. DHS's unique authorities allow us to convene public and private sector partners, and through authorities provided under the Cybersecurity Information Sharing Act (CISA), to share cyber threat information in a protected manner. It is with these authorities that DHS coordinates the overall federal effort to promote security and resilience across all critical infrastructure sectors. The policies that serve as the foundation for these efforts are enshrined in the National Infrastructure Protection Plan, Presidential Policy Directive (PPD) 21: Improving Critical Infrastructure Security and Resilience, PPD-41: United States Cyber Incident Coordination, and the National Cyber Incident Response Plan (NCIRP).

Within this policy and operational framework, DHS partners with key stakeholders to drive better cybersecurity by promoting the development and adoption of best practices and international standards, through services like risk assessments and other technical offerings, and by improved engagement efforts to advance cybersecurity risk management efforts. DHS must also expand operationally meaningful cybersecurity information sharing efforts to empower those protecting networks from cyber threats.

Ultimately, DHS may not have the sector-specific expertise in sectors where we are not the Sector-Specific Agency. However, we do have broad cybersecurity expertise and the ability to aggregate data and threats to identify trends and more broadly understand threat activities. We have built, in effect, a hub and spoke model where DHS NPPD is the central coordination and integration point for national critical infrastructure cybersecurity efforts, connecting the dots across critical infrastructures as cyber threat activity unfolds.

24. How will you address the challenge of recruiting, hiring, training, and retaining the necessary personnel with critical cyber security expertise?

NPPD addresses this challenge in a variety of ways. First, we leverage various unique hiring authorities including direct-hire authority for certain job series; excepted service hiring authority for certain cyber positions; Schedule A hiring authority to noncompetitively appoint persons with disabilities; Veterans Recruitment Appointment (VRA) authority; VEOA (30% or more Disabled Veterans) authority; and others. Approximately 57% of NPPD's workforce is comprised of veteran hires. We also work to identify and participate in veterans hiring events, student programs like the Scholarship for Service (SFS), and broader federal cyber/tech hiring events with our federal partners. To reach more passive candidates as well as private sector candidates, we utilize LinkedIn and other social media.

To retain cyber talent, NPPD leverages the Pathways and Recent Graduate programs, which provide a great option to grow NPPD's talent pipeline and create entry-level assignments where we are better able to compete with the private sector.



We are also working to finalize an Employee Referral Bonus program, which will help encourage employees to refer candidates for hard-to-fill cyber positions. We also utilize all the traditional retention incentives available to NPPD including a student loan repayment program, recruitment bonuses, and the Cyber Pay Program to incentivize employees who retain cyber certifications. If confirmed, I would work to continue executing on these lines of effort.

- a. Do you think the department needs new recruitment and hiring authorities and if so, what would you request?

While I believe the Department's authorities in this area are adequate, it is clear we need to rethink aspects of the federal hiring systems to address the realities of today's rapidly changing human capital environment. The current hiring system takes too long to bring in new employees, and it disenfranchises applicants with non-traditional work experience. If confirmed, I will work with the Department to ensure NPPD fully utilizes existing hiring authorities and flexibilities. I will also work to foster a broader dialogue with OPM, OMB, and Congress to identify opportunities for improving the federal hiring system and making government more competitive with the private sector when it comes to recruiting and retaining cybersecurity talent.

- b. The federal government has few entry level cybersecurity positions. What if anything would you do to address that?

In general, I believe that federal positions should be filled at the lowest level capable of accomplishing the duties. While there may be limited entry-level cybersecurity positions with the federal government as a general rule, NPPD is expanding its cybersecurity workforce and is always looking to fill cybersecurity positions at the entry level. As I indicated in my initial response to Question 24, we utilize a variety of programs including SFS, the Pathways Program and Recent College Graduates program to fill these positions. If confirmed, I would work to ensure we continue filling open positions at the lowest possible level and look for additional opportunities to recruit new entry-level candidates.

25. According to a November 1, 2017 Department of Homeland Security Office of Inspector General (DHS OIG) report, *Biennial Report on DHS' Implementation of the Cybersecurity Act of 2015*, the Department could improve its cyber threat information sharing. In particular, DHS's Automated Indicator Sharing (AIS) system "does not provide the quality, contextual data needed to effectively defend against ever-evolving threats," and it "does not provide adequate information to effectively protect federal and private networks." The Inspector General also reported that some federal and private sector participants found that DHS was not sharing useful information and identified weaknesses in the security controls for DHS's systems for sharing information.

- a. How do you define success for cybersecurity information sharing across the public and private sectors?

I define success for cybersecurity information sharing as getting timely, actionable threat and mitigation information to a broad set of stakeholders in order to enable them to take steps to protect their systems and networks.

As the Inspector General pointed out, NPPD met the requirements of the Cybersecurity Act of 2015 in standing up and operating the AIS capability. If confirmed, I will work to ensure NPPD continues to refine and advance our sharing efforts on that front.

It is also important to note that AIS is just one of several efforts ongoing to share cybersecurity threat indicators. NPPD regularly issues technical alerts with timely and actionable information and appropriate context. For example, when North Korea launched the WannaCry cyberattack last year, the NCCIC quickly coordinated with our appropriate partners and issued an alert with key indicators and valuable context. NPPD also shares threat indicators through our Cyber Information Sharing and Collaboration Program through a collaborative environment where analysts learn from each other to better understand emerging cybersecurity risks and effective defenses.

- b. If confirmed, how do you plan to align DHS's programs, including AIS, toward that vision and measure their success?

While AIS provides a critical capability by allowing network defenders to share cyber threat indicators at network speed, these indicators are most useful to our customers if they include the information, context, and capabilities needed to make them actionable.

If confirmed, I will work to continue building out our stakeholder and customer engagement and communications capabilities to ensure our programs have a keen understanding of who our customers are and that our customers understand how our capabilities and services can help them secure and defend their systems. I will also ensure these capabilities apply a robust customer feedback loop to guide program improvement and increase the value of our service offerings. And on the programmatic side, I will direct program managers to prioritize qualitative metrics while at the same time maintaining our commitment to share as much threat indicator data with as many customers as possible.

- c. If confirmed, how will you ensure that the information shared is actionable and is effectively put into use by participants?

If confirmed, I will ensure our information sharing programs deliver value and we continue to seek ways to share additional context and information in conjunction with the threat indicators we provide. This will help customers better understand the threats and how to incorporate mitigation efforts in their

operational response plans. But ultimately, DHS cannot force our partners to action; it is up to them to act on these indicators and appropriately defend their networks.

- d. Please describe your plans, if confirmed, for how DHS and NPPD will improve cybersecurity threat information sharing, including ensuring that the information is timely and actionable for recipients to integrate into their cybersecurity defensive capabilities.

As indicated in my response to Questions 25b and 25c, we must seek a better understanding of our customers' needs, do a better job of demonstrating the value of the services and capabilities we provide, and help our customers better understand the threat information they receive. If confirmed, I will work to continue building out our stakeholder and customer engagement and communications capabilities to support these efforts, establish regular customer feedback and ensure that feedback guides program improvements, and ensure information sharing program managers to find ways to share additional context and information in conjunction with the threat indicators we provide.

- e. Please describe your plans, if confirmed, for increasing collaboration with federal, state and local government, and private sector participants in AIS.

As SOPDUS, I recognized early on that our cybersecurity service offerings, including AIS, needed robust stakeholder and customer engagement capabilities in order to better understand customer needs and demonstrate to the customer the value of our service offerings and capabilities. If confirmed, I plan to continue staffing out NPPD's external affairs and customer engagement teams and establish an ongoing customer feedback loop to guide program improvements. This feedback is critical in determining ways to better engage customers who require technical assistance, training, additional resources, or other specialized services to make it easier for them to participate in AIS.

26. DHS's EINSTEIN program has received numerous critiques from the Government Accountability Office (GAO), DHS OIG, and private sector experts, including criticism of the program's cost as well as needs for improvement in capabilities and adoption. How are you working to address these challenges and develop and deploy new capabilities through EINSTEIN to address emerging threats to federal networks?

One way NPPD is working to address these challenges is by leveraging existing investments to move beyond current reliance on signatures. These pilot efforts are yielding positive results and leading to the discovery of previously unidentified malicious activity, and demonstrating our ability to capture data that can be rapidly analyzed for anomalous activity using technologies from commercial, government, and open sources. The pilot efforts are also defining the future operational needs for tactics, techniques, and procedures as well as

the skill sets and personnel required to operationalize a broader, non-signature-based approach to cybersecurity.

Like any intrusion and prevention capability, EINSTEIN will never be able to block every threat. Although it is a major tool in our overall toolkit, it is just one part of a broader layered cybersecurity defense. It must be complemented with systems and tools working inside agency networks—as effective cybersecurity risk management requires a defense-in-depth strategy that cannot be achieved through only one type of tool. NPPD's Continuous Diagnostics and Mitigation (CDM) program provides cybersecurity tools and integration services to all participating agencies to enable them to improve their respective security postures by reducing the attack surface of their networks as well as providing DHS with enterprise-wide visibility through a common federal dashboard.

Another challenge to the adoption of EINSTEIN tools and capabilities is the lack of dedicated resources at departments and agencies to deploy and sustain their cybersecurity capabilities. We will continue to rely on program like EINSTEIN and CDM as important layers in our overall cybersecurity defense approach, but ultimately, we need to continue exploring cost-effective investments and dedicated funding at the department and agency level that support our collective goal to protect entire systems from perimeter to the data.

27. Several reports from GAO and the Inspector General have highlighted challenges across NPPD in measuring or determining effectiveness for major cybersecurity programs, including the EINSTEIN program and National Cybersecurity and Communications Integration Center (NCCIC) capabilities. How do you plan to improve management of these programs within NPPD and ensure effectiveness of these capabilities in protecting American networks and assets?

While NPPD's major cybersecurity programs are generally managed appropriately, there are always areas for improvement. If confirmed, I will continue to refine NPPD's management and mission-support services. One key piece of this puzzle is effective performance measurement. If our programs have clear expectations and outcomes that they must meet, then all stakeholders within NPPD can collectively work toward those common programmatic goals. We are currently re-examining our key performance indicators under the Government Performance and Results Act and our Agency Priority Goals. It is essential that we can demonstrate that our programs are substantially increasing cybersecurity within our mission space.

28. Please describe the role of the federal Protective Service (FPS) in assisting NPPD in fulfilling its cybersecurity mission.

The Federal Protective Service (FPS) is responsible for law enforcement and security services for federally-owned and leased facilities nationwide. This includes law enforcement, physical security, and security of automated facility technologies

such as building and access control systems. As federal facilities become increasingly automated, threats and crimes targeting facility automation systems pose a greater risk to overall facility security.

FPS assists NPPD in fulfilling its cybersecurity mission by identifying risks to federal facility automation systems under the purview of FPS, recommending mitigations to reduce those risks, securing FPS-protected systems, and responding to or investigating incidents involving cyber physical assets protected by FPS. FPS fulfills this mission primarily through the facility security assessment process, which includes questions designed to identify risks to federal facility automation systems. FPS works with its customers to reduce the risks to those systems by recommending mitigation actions that can alleviate the risks. In addition, when incidents occur involving FPS-protected systems, FPS leverages its law enforcement authorities under 40 U.S.C 1315 to respond and investigate. FPS has territorial law enforcement jurisdiction over all federal property, allowing the agency to enforce, in most cases, all federal laws, state laws (under certain conditions), and federal regulations relating to property management.

- a. If confirmed, what changes will you make to ensure the roles and responsibilities of the FPS are appropriately aligned with the mission of NPPD?

FPS is charged with the important mission of protecting federal employees and facilities nationwide, and it is essential they continue to receive appropriate support and resources to implement this mission. The GAO is currently conducting a review of FPS' organization and an analysis of alternative organizational placement options. I look forward to reviewing the findings of that review when it is completed and will use the information in that report to inform a robust conversation among all affected parties. Regardless of the outcome of that conversation about FPS's organization placement, for as long as FPS remains a part of NPPD, I will continue working to ensure FPS' roles and responsibilities are aligned to their mission and that they receive the organizational support necessary to accomplish that mission.

29. One of the core missions of FPS is to conduct facility security assessments, including asking questions on cybersecurity. Are you aware that FPS is conducting facility security assessments in regards to cybersecurity? Please explain.

I am aware that FPS's facility security assessment process contains questions that cover initial screening for cybersecurity risks associated with automated facility systems. Facility security assessments evaluate approximately 1,000 variables, covering four major countermeasure components. Should an initial assessment identify the need for a more in-depth cybersecurity screening, FPS would document the basic configuration and management of systems installed at the facility; evaluate relevant threat actors, capabilities, and events applicable to building and security technologies; and assess potential physical impacts of adversaries who may utilize

technological exploits enhance criminal activity perpetrated against FPS-protected properties.

- a. To your knowledge, to what extent, and how often, do Protective Security Advisors receive training on cybersecurity vulnerabilities, prior to conducting federal building security assessments?

FPS facility security assessments are conducted by FPS' Inspector cadre, who are federal employees and sworn law enforcement officers. FPS Inspectors do not receive additional cybersecurity training, nor is it required to conduct facility security assessments. NPPD's Cybersecurity and Protective Security Advisors, who are deployed regionally to support stakeholder engagement around the nation, are equipped to provide cybersecurity and infrastructure protection advice and assistance primarily to our state, local, and private sector partners and stakeholders across the nation.

- b. If confirmed, would you recommend any changes to how these assessments are conducted?

If confirmed, I would work with FPS to ensure any information gleaned from the FSAs or resulting investigations are shared with other law enforcement and U.S. Intelligence Community (IC) partners to help add to the understanding and analysis of cyber threats and vulnerabilities.

#### *Critical Infrastructure*

30. What do you consider to be the top emerging threats to U.S. critical infrastructure and what do you need to do to position NPPD to be ready to address them?

I see two primary emerging threats: (1) information warfare, including foreign influence campaigns, against the U.S. and other like-minded nations and (2) the adversaries focus on gaining access to industrial control systems (ICS) systems. On the first, while new technology will always present a high risk, I am most concerned about the impact of information warfare, because critical infrastructure owners and operators often have difficulty understanding this type of threat and how to defend against it without damaging civil rights, civil liberties, and privacy protections. In addition, there is no easy solution to mitigate this threat. If confirmed, I will continue to direct resources to better understanding this threat, work with all stakeholders in government, industry, academia, civil liberties groups, and others to devise solutions and increase awareness of the threat. Ultimately, I see more information sharing and capacity/awareness as the greatest defense we have to foreign influence campaigns.

As adversaries increase their focus on ICS systems, our increasingly connected society and the reliance on networked systems for critical infrastructure continues to introduce risk. Adversaries are looking to move from business networks, or "IT"

networks, to operational networks, or OT. Operational systems historically have lagged behind IT systems in the level of security or defense. Unfortunately, the consequences of an attack on OT systems can be greater, particularly from a physical manifestation of cyber effects. If confirmed, I will work with industry, particularly ICS companies, to share information on threats, study trends, identify best practices and behaviors that limit network connections and remote access to an as-needed basis, and centralize federal capabilities (e.g., ICS-CERT) to ensure mitigation actions are not only effective but timely. It is critical to recognize that a single ICS system may be deployed across multiple sectors and industries. As a result, efforts that over emphasize or concentrate ICS security work in any one sector risk artificially segregating critical threat and vulnerability information and limit the overall effectiveness of federal ICS security efforts.

31. How do you plan to balance the challenges that NPPD faces protecting critical infrastructure with private sector ownership of most of this infrastructure?

Recognizing that most critical infrastructure is owned by the private sector, public-private partnership has guided the Department's critical infrastructure security efforts since its inception. As a result, the culture of security at DHS is appropriately attuned to this challenge. If confirmed, I would look for opportunities continue to engaging infrastructure owners and operators to identify infrastructure that is critical to the homeland security enterprise; identify vulnerabilities to those assets, systems, and networks; evaluate potential consequences resulting from exploitation of vulnerabilities to those assets, systems, and networks; and develop mitigation measures. A key part of this would be the continued, routine sharing of information between and among public and private sector partners, to include infrastructure owners, to help inform risk management decisions and investments. Information sharing, enabled by effective coordination and communication within and across key partnerships, drives successful risk management and strengthens the protection and resilience of our critical infrastructure.

32. Please describe your assessment of the threats posed by electromagnetic pulses (EMPs), geomagnetic disturbances (GMDs), cyberattacks, and physical attacks to our nation's critical infrastructure.

All of these named threats present real risks to our Nation's critical infrastructure and require continued monitoring of the threat. NPPD must ensure we are appropriately sharing actionable information with our stakeholders about these threats so they can take appropriate action. NPPD has well-established programs related to physical risks to critical infrastructure, including EMP/GMD risks and is an active part of the Department's current efforts to understand the risk and work with industry to develop and deploy cost effective mitigations to increase resilience. Over the last few years, NPPD has built additional capability related to cyber risks. If confirmed, I will continue to ensure there is an appropriate balance amongst our

programs in order to best engage and deliver services with critical infrastructure owners and operators to mitigate the wide range of risk.

33. The FY2017 National Defense Authorization Act required DHS to prepare a strategy for EMP/GMD threats. What should NPPD's role be in preparing for and mitigating EMP/GMD threats?

**As the lead for the security and resilience of critical infrastructure, NPPD plays an important role understanding all threats to infrastructure, including EMP and GMD. NPPD is responsible for understanding the threat and potential consequences to critical infrastructure, sharing this information with our stakeholders so they can make risk-informed decisions, and ensuring there remains national-level attention in planning and exercising so we are better prepared. If confirmed, I will work to ensure NPPD remains focused on mitigating the EMP/GMD threat.**

34. In March 2016, GAO examined the steps DHS and the Department of Energy have taken to address the key recommendations of the 2008 EMP Commission report, and revealed that several recommendations remain open and unimplemented. A February 2018 GAO report, *"Electricity Suppliers Have Taken Actions to Address Electromagnetic Risks, and Additional Research Is Ongoing"*, found that DHS needs to do more to define roles for EMP/GMD work and collect additional risk inputs to further inform risk assessment efforts.

- a. Please describe your understanding of the 2008 EMP Commission Report.

**The 2008 EMP Commission Report is a thorough document that includes recommendations in several critical sectors, with an emphasis on impact to the energy sector and electric power in particular. I have reviewed the report and related correspondence to the Department from the Commission.**

- b. If confirmed, will you commit to thoroughly investigate the open recommendations from the 2008 EMP Commission report and work to implement them into DHS's national security strategy?

**If confirmed, I will continue working to address open recommendations from the 2008 EMP Commission Report. As this Committee is aware, in 2016, the GAO released a report, *federal Agencies Have Taken Actions to Address Electromagnetic Risks, but Opportunities Exist to Further Assess Risks and Strengthen Collaboration*, in which GAO reviewed progress against many of the recommendations in the 2008 EMP Commission report. The Department continues to address and take action on those open recommendations and I am committed to ensuring NPPD appropriately leads and contributes to those recommendations.**

- c. Please describe your understanding of the February 2018 GAO report.



The February 2018 GAO report on EMP primarily focused on actions taken by electricity suppliers and ongoing research needs. There were no specific recommendations for DHS, but our ongoing work related to researching impacts to critical infrastructure as discussed in the 2016 GAO report on EMP was noted. The 2018 GAO report points to need for additional research and data before imposing costly requirements on electricity suppliers, specifically in the area of high-altitude EMP.

- d. If confirmed, will you commit to better define DHS roles and responsibilities for EMP/GMD preparedness and collect additional risk inputs?

**Yes, if confirmed I will remain committed to defining DHS roles and responsibilities and collecting additional risk inputs for EMP/GMD preparedness.**

35. The Chemical Facility Anti-Terrorism Standards (CFATS) program is set to expire at the end of this year. In 2013, committee Ranking Member Tom Coburn completed an assessment of the program which found failures to meet deadlines, validate security plans, and inspect facilities. If confirmed, how will you monitor the program's metrics, performance, and management?

During the years immediately following the initial authorization of the CFATS program, DHS faced challenges implementing the program. Many of these challenges were highlighted in Senator Coburn's report. However, over the last five years, the CFATS program has made great strides, and is now a model infrastructure security regulatory program. NPPD streamlined the site security plan inspection and review process, resulting in the effective elimination of the site security plan approval backlog in 2016, approximately four to six years ahead of prior GAO estimates. NPPD also simplified the web-based tools used by chemical facilities to submit information to the program, greatly reducing the compliance burden on the regulated community. NPPD also updated the CFATS risk-tiering engine to more accurately reflect the current threat environment, more accurately calculate potential consequences from chemical incidents, and more fully account for facility characteristics and actions that reduce vulnerability. These modifications have helped NPPD assess the risk of more than 40,000 facilities and conduct over 6,500 inspections to date at the approximately 3,500 facilities determined to be high risk.

If confirmed, I will continue to monitor closely the program's performance, metrics, and management through a variety of mechanisms. These include program-specific Government Performance and Results Act metrics, annual operating plans containing internal performance metrics, quarterly performance reviews, and performance plans with clear expectations for senior leadership. I will also work to sustain Congressional oversight of the program by improving the timeliness of semiannual reports detailing various aspects of CFATS implementation. Finally, I

will also work to ensure GAO retains its current level of access and all requested information and data necessary to support its ongoing and future audits and oversight activities.

36. If confirmed, please describe how NPPD will assist the Department in securing the nation's election infrastructure in preparation for the 2018 midterm elections and thereafter.

Our election process is governed and administered by state and local election officials in thousands of jurisdictions across the country. These officials manage election infrastructure and ensure its security on a daily basis. NPPD is committed to working with these officials and ensuring a coordinated response from DHS and its federal partners as we support state and local officials' efforts to plan for, prepare for, and mitigate risk to election infrastructure.

In order to ensure a coordinated approach from the federal government, NPPD brings together stakeholders from across the Department and other federal agencies as part of an Election Task Force (ETF). The ETF increases the Department's efficiency and effectiveness in understanding, responding to, communicating, and sharing information related to cyber threats to election infrastructure and other election infrastructure security issues. The ETF provides actionable information and assistance to help election officials strengthen their election infrastructure by reducing and mitigating cyber risk.

To help coordinate efforts between the ETF and non-federal partners, NPPD established an Election Infrastructure Subsector (EIS) Government Coordinating Council (GCC) and Sector Coordinating Council (SCC). The EIS GCC, which includes representatives from DHS, the Election Assistance Commission (EAC), and 24 state and local election officials, established subsector goals and started development of an EIS Sector-Specific Plan. The SCC, composed of election infrastructure industry representatives, serves as the election industry's principal entity for coordinating with the government on security activities.

In addition to working with the EIS-GCC and SCC, NPPD continues to directly engage state and local election officials – coordinating requests for assistance, risk mitigation, information sharing, and incident coordination, resources, and services. Specific services offered by NPPD include:

- Sharing threat and vulnerability information through the NCCIC and NPPD Cyber Security Advisors and Protective Security Advisors;
- Increasing the availability of free technical assistance, such as cyber hygiene scans, phishing campaign assessments, and on-site cyber risk and vulnerability assessments (RVAs);
- Sponsoring up to three election officials in each state for security clearances, facilitating their ability to receive indicators of concern and information on any identified threats or vulnerabilities before an incident occurs;

- Offering on-site assistance in identifying and remediating cyber incidents;
- Supporting election officials with incident response planning including participating in exercises and reviewing incident response playbooks; and
- Providing guidance and tools to improve the security of polling sites and other physical election infrastructure.

If confirmed, I will continue to collaborate closely with state and local election officials, election equipment vendors, and other partners to ensure that we are working together to secure this vital infrastructure sector.

37. Do you have any cybersecurity concerns regarding chemical facilities?

As with virtually all critical infrastructure, cyber systems and networks at chemical facilities, such as ICS or Supervisory Control and Data Acquisition (SCADA) systems, often present vulnerabilities that can be exploited by sophisticated adversaries. As a result, cybersecurity must be a key part of a comprehensive security approach for chemical facilities. This has long been the Department's position, and NPPD has a long history of working with the chemical sector on chemical facility cybersecurity.

Under the CFATS program, the Department requires high-risk chemical facilities to develop and implement site security plans that meet cybersecurity requirements set forth in CFATS Risk-Based Performance Standard 8 – Cyber. For chemical facilities not subject to CFATS security requirements, NPPD, in its role as Sector Specific Agency for the Chemical Sector, works closely with representatives of the chemical industry to develop and encourage the use of tools, such as the *Chemical Sector Cybersecurity Framework Implementation Guide*, to help chemical facilities implement strong cybersecurity practices. If confirmed, I will work to ensure that NPPD continues to work with its partners throughout the chemical sector to assist them addressing cybersecurity concerns at chemical facilities.

*National Security, Election Security, and Reorganization*

38. What plans do you have to improve NPPD's intelligence coordination with DHS's Intelligence and Analysis office?

Access to reliable and timely intelligence is critical for NPPD to carry out our mission. As SOPDUS, I have made improving both access to and review of intelligence a priority, as well as prioritizing a close working relationship with DHS Under Secretary for Intelligence & Analysis (I&A) David Glawe. Early in my tenure, I established at NPPD an Intelligence Briefing Team which serves as a key link to I&A and ensures senior leaders in both organizations are aware of the intelligence briefed to the Secretary and other senior leadership. My team also participates in daily Intelligence and Operational synchs with I&A and other operational components. These efforts help establish a common understanding of the threat picture and encourage unity of effort as we execute our shared mission. If

confirmed, I will continue to work with Under Secretary Glawe and I&A leadership to ensure NPPD intelligence requirements are provided to our intelligence partners and that actions related to sharing information, particularly with private sector and state and local government partners, are well-coordinated within the Department.

39. What is the biggest challenge the Department faces as it works with election agencies and election service providers to bolster election infrastructure cybersecurity?

The Department faces a number of challenges in its efforts to bolster election infrastructure cybersecurity, including the sophistication of the adversaries attempting to disrupt our infrastructure, the distributed nature of elections management in the U.S., historical underinvestment in modern and secure election systems, the sensitivity and associated classification of election infrastructure-related threat and intelligence information, and the lack of Departmental authority to compel cooperation from our stakeholders or mandate any standards, measures, or other requirements on election infrastructure owners and operators. The biggest challenge, however, may simply be the sheer size and diversity of the election infrastructure community compounded by the cost of retiring legacy elections systems in favor of voter verifiable paper audit systems. It is difficult to work with each jurisdiction directly, as each of the hundreds of state and local jurisdictions field their own unique election system, operate in unique political environments, take different approaches to security, and have different risk tolerance.

Having said that, this challenge is not insurmountable. Through development of standardized best practices, broad information sharing, and the use of force-multipliers such as the Multi-State Information Sharing and Analysis Center (MS-ISAC), the National Association of Secretaries of State (NASS), and the National Association of State Election Directors (NASED), NPPD is able to get maximum reach and impact for the finite resources available to address this important issue.

40. What do you consider to be the top emerging threats to our election infrastructure, and how are you positioning NPPD to address them?

Cyberattacks carried out by nation-state actors continue to be the most significant threat to our election infrastructure. As discussed in response to question 36, NPPD is working with state and local election officials and other partners on a variety of efforts to enhance the security and resilience of election infrastructure against both physical and cyber threats. Foreign influence and disinformation campaigns are also a threat to election infrastructure, as we saw in the 2016 elections. As a part of our incident response efforts with the election community, we are working on crisis communications playbooks and protocols so that when disinformation is detected, trusted voices can weigh in with the public to correct the record. It is imperative that the American people have confidence in our election infrastructure and that their vote counts and is counted correctly.

41. The NPPD is proposing to reorganize into three directorates.

- a. Do you believe this reorganization will make NPPD more cost-effective and efficient, while improving the effectiveness of the directorates? Please explain.

**H.R. 3359, *Cybersecurity and Infrastructure Security Agency Act of 2017*, which was passed by the House and passed out of the Senate Homeland Security and Governmental Affairs Committee as a part of the DHS Reauthorization Act, would establish three operationally-focused divisions: Infrastructure Security, Cybersecurity, and Emergency Communications. At the same time, the Act would streamline the organization and focus the new Agency on cybersecurity and critical infrastructure security, by moving the Office of Biometric Identity Management to the Management Directorate of the Department and begin charting a course for FPS.**

**Regardless of the final organizational structure of NPPD, I am committed to finding efficiencies within the organization. As our mission continues to grow, it is essential we eliminate duplication and redirect as many resources as possible toward the most critical mission activities. We must also integrate and consolidate mission support functions so that operational elements have the most effective and efficient business support possible. If confirmed, I will continue to review current programs to ensure they are targeted toward mitigating the highest risks to critical infrastructure and to continue looking for opportunities for new or revised business processes which may result in efficiencies.**

- b. If you are confirmed and the NPPD is reorganized, what actions will you take to hire, train, and staff cyber positions?

**My response to Question 24 outlines a variety of actions I have overseen implemented in my current position as the SOPDUS to enhance NPPD's ability to hire, train, and staff cyber positions. If confirmed, I would work to continue executing on these lines of effort.**

#### **V. Relations with Congress**

42. 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 comply.**

43. 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 would without reservation.**

44. 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 would comply without reservation.**

**VI. Assistance**

45. Are these answers your own? Have you consulted with NPPD, DHS or any other interested parties? If so, please indicate which entities.

**I have written and reviewed all the responses in this document, and the answers are my own. In preparing responses to these questions, I consulted with my senior counselors and legislative affairs staff at NPPD, and with legal counsel at DHS.**

**Minority  
Supplemental Pre-Hearing Questionnaire  
For the Nomination of Christopher Krebs to be  
Under Secretary, Department of Homeland Security,  
National Protection Programs Directorate**

**I. Nomination and Conflicts of Interest**

1. Has the President or his staff asked you to sign a confidentiality or non-disclosure agreement?

No.

2. Has the President or his staff asked you to make any pledge or promise if you are confirmed as Secretary?

**No. Although, if confirmed as the Under Secretary, I assume I will be asked to pledge the Oath of Office to the Constitution, and to sign the ethics pledge required of all political appointees under Executive Order 13770.**

3. During your tenure in this Administration, have you asked any federal employee or potential hire to pledge loyalty to the President, Administration or any other government official?

No.

**II. Background of the Nominee**

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

**The ongoing efforts to secure the nation's election infrastructure have presented and continue to present politically difficult choices for me and our stakeholders. While we all agree on the need for action, we often find ourselves in situations where any action generates negative reactions among some subset of our stakeholders. For example, when this Administration began, DHS was receiving a significant amount of push back from stakeholders on the designation of state and local election systems as critical infrastructure. I felt it was important to maintain that designation and formally commit to an ongoing partnership with election officials and other stakeholders in that community. That commitment has resulted in improved relationships and a measurable reduction in risk to election systems. However, not all of our stakeholders support this approach. There is much more work to be done, and much of that work is outside of the Department's control. So it is important to continue in earnest conversations between Congress, the Administration, state and local election partners, and other stakeholders on how best to support their efforts to manage risk and deploy more resilient election systems.**

5. If confirmed, what experiences and lessons learned since leaving DHS will you bring to the position of Under Secretary for NPPD?

My experience in the private sector, both advising critical infrastructure companies and working in a large technology company, has helped refine my understanding of the appropriate balance between government and industry. More specifically, I understand the unique value that government offers to the private sector, for example intelligence sharing, developing an understanding of national risk, or the ability to facilitate actions that reduce federal barriers to private sector action. If confirmed, I will use my experience in these areas to identify opportunities for NPPD to make the most impact as we work to manage critical infrastructure and cybersecurity risk. It would be my intention to focus specifically on areas where private sector capability may be lacking, or where there is no viable business model within industry.

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

While our work is far from complete, I am most proud of my role leading the Department's efforts to help state and local governments improve the security of their election systems. We established the Election Task Force to coordinate and prioritize DHS election security related efforts, and have fully supported to the establishment of the GCC and SCC. In addition, we have and will continue to sponsor state election officials for security clearances, while also pressing for rapid declassification of intelligence to ensure relevant information is reaching election officials at all levels. In less than a year, we have made a real difference supporting our state and local partners' efforts and helping them manage risk in their jurisdictions.

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

With every success comes the opportunity to reflect on failures and lessons learned. In our efforts to ramp up support services to our election infrastructure partners, we often focused too much providing programmatic and technical support. In doing so, we overlooked the value and importance of communicating with stakeholders, in particular crisis communications. As a result, we failed to gain the confidence of our partners in the early stages and lost precious time working to overcome the resulting challenges. We have since made strategic hires and dedicated additional communications and external affairs resources to ensure we are properly coordinating and communicating with our stakeholders.

8. Please list the following information for your positions at Potomac Management Group; Intermedia Group, Inc.; Systems Planning and Analysis; the Department of Homeland Security (Bush 43); Dutko Worldwide; Obsidian Analysis; Microsoft; and the Department of Homeland Security (Trump 45):

- a. Please describe your role and responsibilities in the position.



**Potomac Management Group (PMG):** At PMG, I served as an assistant project manager for a US Coast Guard contract focused on evaluating oil spill response plans for compliance against regulations stemming from the Oil Pollution Act of 1990. I provided policy guidance and advice to customers, and oversaw junior analysts in their daily duties.

**Intermedia:** At Intermedia, I served as project coordinator in support of a U.S. Coast Guard customer on the development of the National Strategy for Maritime Security required by HSPD 13/NSPD 41. I provided input to the Maritime Infrastructure Recovery plan, including a policy review, white paper development, and other policy coordination related activities.

**Systems Planning and Analysis (SPA):** At SPA, I served as Professional Staff in support of a DHS Office of Infrastructure Protection (IP) customer. I drafted policy documents, developed operational and training guidance, developed concepts of operation for incident response including several hurricanes, and supported strategy and policy efforts for the development of the CFATS program. I worked closely with DHS IP leadership to understand the agency's priorities and direction, and assisted in the development of the policies to carry out that guidance.

**DHS:** At DHS, I served as a Policy Advisor to the Assistant Secretary for IP, overseeing international infrastructure protection efforts, providing strategic direction to the CFATS program at its inception, and advising the Assistant Secretary and the Office of the Secretary on infrastructure protection related issues.

**Dutko:** At Dutko, I served as Vice President for a start-up risk management firm, advising commercial customers on infrastructure protection and risk management strategies and approaches, including cybersecurity incident response planning efforts. I supported federal exercise efforts, including National Level Exercise 2010 and 2012. I was responsible for managing business development efforts focused on private and public sector customers. I managed policy, tracking efforts across a small team and identified trends in Executive Branch and Legislative Branch policy developments.

**Obsidian:** At Obsidian, I served as a Principal, leading the firm's cybersecurity and infrastructure security related business line. I also served as the Deputy Program Manager for National Level Exercise 2012, the largest civilian cybersecurity exercise in the U.S. In this capacity, I worked closely with federal and industry partners to devise a practical exercise scenario while also encouraging meaningful private sector participation.

**Microsoft:** At Microsoft, I served as Director for Cybersecurity Policy and lead the company's U.S. cybersecurity policy-related efforts. I provided guidance to the company's engineering and legal teams on emerging cybersecurity policy

trends, anticipating changes or opportunities to act or improve security. I also worked with Executive Branch and Legislative Branch officials to communicate industry perspective and expertise into the policy process. I served as Microsoft's representative to the President's National Security Telecommunications Advisory Council (NSTAC), and also on the Executive Committee of the Information Technology Sector Coordinating Council (IT SCC).

**DHS:** At DHS, I served as Senior Counselor to the Secretary, advising on infrastructure and cybersecurity related issues. In this role, I focused on identifying policy opportunities, translating and communicating priorities to operational components, and ensuring interagency efforts reflected DHS equities. I currently serve the Department in two capacities: Assistant Secretary for Infrastructure Protection, leading the Office of Infrastructure Protection, and the SOPDUS, leading NPPD.

- b. Please describe who you reported to and where your position fit in within the hierarchy of the organization. Please include individuals to whom you directly reported and relevant dates.

**PMG:** I reported to the Program Manager. The Coast Guard program was the company's largest. I worked in this position from 2002 to 2005.

**Intermedia:** I reported to the Program Manager. Intermedia was a subcontractor to Anteon Corporation. I worked in this position from February 2005 to August 2005.

**SPA:** I reported to the Vice President responsible for the Homeland Security segment of the company. I supported that Vice President from August 2005 to October 2007.

**DHS:** I reported to Bob Stephan, the Assistant Secretary for Infrastructure Protection (IP), from October 2007 to January 2009. IP is a subcomponent of NPPD, a headquarters component of DHS.

**Dutko:** I reported to Bob Stephan, Managing Director for Dutko Global Risk Management (DRGM). DGRM was an operating element of Dutko. I worked at Dutko from January 2009 to December 2011.

**Obsidian:** I reported to the Chairman and CEO of Obsidian Analysis. I led the cybersecurity and infrastructure business segment. I worked at Obsidian from January 2012 to February 2014.

**Microsoft:** I reported to the Senior Director with the Trustworthy Computing group within the Legal and Corporate Affairs group from February 2014 to July 2015. I then reported to the U.S. Government Affairs team within the

reorganized Corporate External and Legal Affairs team from July 2015 to March 2017.

**DHS:** As Senior Counselor, I reported to the Chief of Staff, Kirstjen M. Nielsen. As Assistant Secretary for IP and SOPDUS, I report to Secretary of Homeland Security Kirstjen M. Nielsen.

- c. In this role, what was the largest number of people that you directly managed at any one time?

**PMG:** two.

**Intermedia:** zero.

**SPA:** two.

**DHS:** zero.

**Dutko:** two.

**Obsidian:** 22.

**Microsoft:** two.

**DHS:** As Senior Counselor, I did not manage any employees. As Assistant Secretary and SOPDUS, I manage a federal workforce of approximately 3,600 FTE.

- d. In this role, what was the largest number of people that directly reported to you at any one time?

**PMG:** two.

**Intermedia:** zero.

**SPA:** two.

**DHS:** zero.

**Dutko:** two.

**Obsidian:** six.

**Microsoft:** two.

**DHS: As Senior Counselor, I had no direct reports. As Assistant Secretary and SOPDUS, I have two direct reports.**

- e. Please describe the circumstances of your departure from the organization.

**In all cases, I departed my previous employer amicably to pursue other opportunities.**

***Federal Contracting Experience***

9. In your biographical questionnaire, you describe several positions in which you worked as a "federal contractor." During the course of your tenure as a federal contractor did you consult, advise, assist or support any client in their interactions with the White House, TSA or DHS? If so, please describe that work.

**No, I did not consult with, advise, assist, or support a client in their interactions with the White House or TSA while working as a federal contractor. My response to Question 9a below outlines the support I provided to elements of DHS while working as a federal contractor.**

- a. During your tenure in the private sector did you consult, assist or otherwise work on any federal contracts or solicitations on behalf of an employer or client? If so, please list each client or employer, the contract, the contract number, the contracting agency, the amount of the contract and describe your work on the contract including whether your client or employer fulfilled the contract in its entirety.

**I supported the development of proposals in response to various solicitations in accordance with formal teaming agreements with potential prime contractors and other subcontractors.**

**At PMG, I worked on contracts issued by the US Coast Guard pertaining to oil spill response planning. To my knowledge, the contract was performed satisfactorily and in its entirety. Any records pertaining to federal contracts with this employer are no longer available to me as they were the property of the company, which has ceased operations.**

**At Intermedia, as a subcontractor to Anteon, I worked on contracts issued by the US Coast Guard pertaining to the development of the National Strategy for Maritime Security called for in HSPD-21. To my knowledge the contract was performed satisfactorily and in its entirety. As a subcontractor to Anteon, I was not privy to the contract information.**

**At SPA, I worked on contracts issued by the DHS Office of Infrastructure Protection (IP) from 2005 to 2007. I primarily worked on-site at DHS facilities. I provided infrastructure security policy and programmatic support, including**

chemical facility security issues. I was not privy to the contract information. To my knowledge, the contract was performed satisfactorily and in its entirety.

At Dutko Global Risk Management, I served as a subcontractor to a number of companies, including Obsidian Analysis and L-3 Communications. As a subcontractor, I was not privy to full contract information, only that information related to work I performed. In addition, Dutko Global Risk Management's parent company was acquired and no longer operates under that name, in part because the principals supporting the endeavor departed the company. I provided homeland security policy and critical infrastructure protection related expertise. To my knowledge, the contract was performed satisfactorily and in its entirety.

At Obsidian, I served as Deputy Program Manager on National Level Exercise (NLE) 2012. Obsidian was the Prime Contractor to this contract. The contract was with FEMA. The contract name was "NLE 2012 and Other Support Services," and the contract number was HSFEEM11C0387. The contract value was approximately \$9.3 million. In this role, I developed cybersecurity related exercise scenarios, facilitated exercises, coordinated industry participation, and lead lessons-learned development. I also supported the National Preparedness Assessment Division, conducting lessons learned exercises for Hurricane Sandy and other natural disasters. The contract name was "NPAD Preparedness Analysis and Reporting," and the contract number was HSFE2013F0073. The contract value was approximately \$18.9 million. To my knowledge, the contracts were performed satisfactorily and in their entirety.

- b. Were there any matters during your tenure as a federal employee that you were recused from working on as a result of your prior work in the private sector? If so, please describe.

I am currently recused from particular matters related to Microsoft Corporation and the NCSA.

*Department of Homeland Security*

10. In your role as Counselor to the Secretary of the Department of Homeland Security:

- a. What do you consider your greatest success and greatest failure in this role? What lessons did you take away from each experience?

As Counselor to the Secretary, I generally helped develop policy matters and provide the Secretary's direction to headquarters and operational Components, including the NPPD and FEMA. In that role, I worked with FEMA to develop and execute a Cabinet-level seminar for hurricane season, convening Cabinet members to walk through the National Response Framework and related emergency support functions as well as the respective roles and responsibilities

of the departments and agencies. My primary take away from this experience was the value of bringing together decision makers to discuss their respective authorities and responsibilities. I learned that while one official may understand their own agency's role, they may not necessarily understand another agency's role.

I also worked closely with NPPD to monitor and coordinate DHS activities in response to cybersecurity events, including WannaCry and NotPetya. My takeaway from incident response was the value of trust-based relationships for effective cybersecurity response, and the need to work closely and communicate clearly with industry and interagency partners during an incident response.

*Positions Held Outside United States Government*

11. Please describe your role and responsibilities in any positions hold outside of the United States government for the last ten years, including the National Cyber Security Alliance.

I was the Microsoft representative to the NCSA, and served concurrently as the Vice Chair of the NCSA from November 2016 to March 2017. In that capacity, I provided executive guidance and helped set priorities for the NCSA, including strategies for increasing awareness of cybersecurity issues across a range of stakeholders.

I also served on the Executive Committee of the IT SCC, an industry body that coordinates with the federal government on infrastructure protection and cybersecurity issues. The IT SCC operates within the NIPP Partnership Framework. In that role, I contributed to SCC policy positions and working groups focused on cybersecurity-related risk management priorities.

*Accountability*

12. During your career as a federal employee, have you ever used a personal email account or device to conduct official government business?

No, not to my knowledge.

- a. If so, please list in what government positions you have used a personal email account or device to conduct official government business, describe your general practice for doing so, and what specific steps you have taken to ensure that federal records created using personal devices and accounts were preserved.

I do not recall ever using a personal email account or device to conduct official government business. As a standard practice, if I receive an email on a personal account discussing official government business, I immediately forward the email to my work email address.

- b. During your tenure as a federal employee or member of the beachhead team, have you used a smartphone app including, but not limited to, WhatsApp, Signal, Confide, and others that support encryption or the ability to automatically delete messages after they are read or sent, for work-related communications? If so, please indicate which application, when it was used, how often and with whom.

**No, I have not used smartphone apps with the described capabilities for work-related communications.**

13. During your career, has your conduct as a federal employee ever been subject to an investigation, audit, or review by an Inspector General, Office of Special Counsel, Equal Employment Opportunity Commission, Department of Justice, or any other federal investigative entity? If so, please describe the review and its outcome.

**No, not to my knowledge.**

14. During your career as a federal contractor, has your employer or a client been subject to suspension or debarment arising from a contract or solicitation that you worked on, been cited for failing to fully perform on a contract that you worked on, or received a less than satisfactory rating on any contract on which you consulted or performed?

**No, not to my knowledge.**

15. If confirmed, do you pledge to implement recommendations made by the Office of Inspector General, the Office of Government Ethics, the Office of Special Counsel and the Government Accountability Office?

**If confirmed, I commit to doing so.**

16. Have you ever received a formal performance review related to your management experience? If so, please list the position and describe the outcome of the review.

**No, not that I recall.**

#### **IV. Policy Questions**

##### ***Management***

17. As Counselor to the Secretary what was your role in reviewing or providing input on executive actions or other administration policies that impacted DHS?

**As Counselor to the Secretary, I provided policy, technical, and programmatic insight into cybersecurity and infrastructure-related administration policies. This included work on Executive Order (EO) 13800, Cybersecurity of Federal Networks and Critical Infrastructure. In general, I reviewed and refined input or contributions provided by DHS components pertaining to Executive Orders, including EO 13800.**

*Emergency Management*

18. Do you believe that man-made climate change has contributed to the growth in the frequency, magnitude, and financial impact of natural disasters in recent years? If yes, please explain how NPPD can use this information to improve its responsiveness and ability to prepare for disasters. If no, please explain why not.

The 2017 hurricane season was one of the most active on record, with a succession of major storms impacting various parts of the U.S. As we continue to observe increases in the frequency, magnitude, and financial impact of natural disasters, it is imperative NPPD study both the impact of these disasters on our nation's critical infrastructure and assess the effectiveness of NPPD's response in order to improve our ability to prepare for, respond to, and recover from future natural disasters.

To that end, I directed NPPD's National Infrastructure Coordinating Center (NICC) to review all aspects of NPPD's response and short-term recovery efforts in support of Hurricanes Harvey, Irma, and Maria. Their work highlighted the processes and procedures that contributed to NPPD's successes during the 2017 hurricane season and identified the gaps that challenged NPPD efforts internally and externally. Through this effort, we identified approximately 50 areas for improvement. NPPD currently is prioritizing those areas for action, which will enable us to take the lessons learned from the historic 2017 hurricane season and improve our ability to respond to future incidents and natural disasters.

19. In the span of four weeks, Hurricanes Harvey, Irma, and Maria brought unprecedented devastation to communities in Texas, Florida, Puerto Rico, the U.S. Virgin Islands, and surrounding areas. In early October, the deadliest series of wildfires in California history ravaged the state, causing more than \$3 billion in insured losses.

- a. Please describe your role in these recovery efforts in the current administration.

As the SOPDUS, I oversaw NPPD's efforts in support of the overall federal response to the 2017 hurricane season. Under my leadership, NPPD conducted a wide-range of activities in support of federal response and recovery efforts, including immediate response actions, deployment of resources and personnel to affected areas, and sustained response operations. To support these response and recovery efforts, I activated NPPD's Critical Infrastructure Crisis Action Team (CI-CAT), which surged for over 60 days to facilitate response and recovery efforts. I personally took numerous trips to areas impacted by Hurricanes Harvey, Irma, and Maria, and worked directly with senior leaders at the federal, state, territorial, and local levels to help facilitate the restoration of critical infrastructure in the impacted regions.

As the situation on the ground across multiple states and territories unfolded, we saw many changes to the daily operations and priorities of NPPD. I quickly



realized the need to utilize capabilities from across the Directorate and worked with CI-CAT leadership to rapidly expand CI-CAT capabilities to ensure a more cohesive and inclusive approach to incident response. I directed NPPD to integrate a National Coordinating Center for Communications liaison desk into the CI-CAT to enhance our capabilities. I also ordered the formation of a Future Operations Cell, allowing NPPD to provide a comprehensive picture of current operations, the projected future outlook, and an overview of critical infrastructure issues associated with ongoing hurricane response efforts. To support this new function, I instructed NPPD's Office of Cyber and Infrastructure Analysis (OCIA) to develop numerous analytical products that were used to inform policy decisions by Department leadership, illustrate the current situation to members of Congress, and provide decision support tools to our private sector partners.

Finally, throughout the 2017 hurricane season, I, along with members of my senior leadership team, engaged in unprecedented collaboration with our colleagues at the FEMA to support the overall federal response. Under my guidance, NPPD assumed an active role in supporting the National Response Coordination Center, the National Business Emergency Operations Center, and the newly established Business Infrastructure Industry Solutions Group, and NPPD field staff leveraged relationships with those partners most directly affected by this hurricane season to support response and recovery efforts.

- b. What do you see as notable successes and failures by the Trump Administration and DHS regarding the initial response to these four disasters?

As SOPDUS, my focus during each of these disasters was to identify ways in which NPPD resources could be brought to bear within our existing authorities to assist in the response to and recovery from the disasters as quickly as possible. I believe NPPD largely enabled more effective response by integrating private sector response efforts with the federal government's response. There is always room for improvement, as my leadership team and I have identified various areas for improvement within NPPD, including tighter integration across our own organization, as well as with FEMA and with industry.

On the positive side, I believe NPPD was particularly successful at facilitating information sharing, maintaining situational awareness, enhancing coordination, and enabling improved response and recovery activities across our across NPPD and with external federal, state, territorial, local, and private sector partners. The flexibility and scalability of NPPD's CI-CAT allowed us to support efforts to respond to multiple disasters simultaneously, and the partnerships that NPPD has fostered for years at both the National and regional levels enabled NPPD to break down barriers and speed up restoration and recovery activities. Specific success stories supported by NPPD's efforts include facilitating the expedited restoration of communications capacities in impacted areas, providing assistance to secure priority access to parts for generators for use in Puerto Rico, and

aiding the timely transportation of vital pharmaceutical supplies manufactured in Puerto Rico to the United States.

Despite the many successes, there were a number of areas identified for improvement. There is limited governing documentation regarding restoration of critical infrastructure, and this lack of clear doctrine often led to a need for ad hoc solutions. Similarly, while overall coordination efforts between NPPD and FEMA were unprecedented, these efforts were also complicated at times due to the lack of standardized coordination protocols and procedures. Access and reentry to facilities in impacted areas, which is a key priority for private sector stakeholders, was not as seamless as it could have been, with differences in rules across jurisdictions often creating impediments to reentry. If confirmed, I would be committed to addressing these and other areas of improvement to support NPPD's role in helping the Nation respond to and recover from future disasters.

- c. As of early March 2018, Puerto Rico still did not have 100% of its power restored. In your role as the Senior Official Performing the Duties of the Under Secretary for NPPD, what efforts have you led to manage the situation in Puerto Rico and bring its infrastructure back online? Are you satisfied with the progress and current status of affairs? If not, what do you plan to do to prioritize such efforts and ensure results for the people of Puerto Rico?

In the aftermath of Hurricane Maria, I personally took multiple trips to Puerto Rico. This enabled me to see firsthand both the hurricane's devastating impact on the island and the hard work being performed by federal, territorial, local and private sector responders side by side with the local population. As the SOPDUS, it was my responsibility to oversee NPPD's efforts in support of this whole-of-community response effort. As described in greater detail in response to Question 19a, this included overseeing immediate response actions, deployment of resources and personnel to affected areas, and sustained response and recovery operations.

NPPD's work as part of the whole-of-community response and recovery efforts has resulted in restoration of nearly all of Puerto Rico's power, communications systems, water treatment, and other key lifeline functions; however, there still is more work to be done. As discussed previously, PPD-21 and the National Response Framework, as well as the operational decisions made by FEMA leadership, outline the respective responsibilities for sector-specific leadership. In the case of this past hurricane season, NPPD's responsibilities largely focused on characterizing national and regional risk, and enabling decision makers to determine response courses of action. However, in some cases, like communications restoration, NPPD is the lead federal agency and assisted telecommunications providers in getting their equipment and assets down to Puerto Rico to reestablish cellular communications.

**NPPD is committed to continuing to work within our existing authorities to help finish the restoration of Puerto Rico's infrastructure.**

20. What do you believe the role of the federal government should be in long-term recovery efforts and what metrics should the government use to determine whether federal responsibilities have concluded for providing assistance after a natural or man-made disaster?

While long-term recovery efforts are first and foremost a local responsibility, response and recovery to significant natural disasters often is a whole-of-community effort, requiring contributions from the federal, state, local, territorial, tribal, and private sector levels as well as members of the public in the affected communities. The extent of the role of the federal government in long-term recovery efforts resulting from any natural or man-made disaster is dependent on a variety of factors specific to the incident. These include the scope of the damage caused by the disaster, the affected community's disaster recovery capabilities, and the state or territory's desire for federal government assistance.

For smaller incidents generally within the capabilities of the state or local community, the federal government likely would play a very limited role, perhaps simply facilitating information sharing and providing subject matter expertise and guidance upon request. For large incidents that exceed the capabilities and resources of the affected community, the federal government may need to take a major role in long-term recovery efforts. This could include providing both financial and other resources to actually design and implement long-term recovery projects.

21. To what degree do you believe the federal government should be financially responsible for restoring the power grid, repairing damaged water lines, and meeting other disaster-related needs in Puerto Rico?

Hurricane Maria was the strongest hurricane to make landfall in Puerto Rico in nearly 100 years. The hurricane wreaked havoc on the infrastructure in Puerto Rico, causing damage that far exceeded the territory's resources. In recognition of this, Puerto Rico has requested federal government assistance, including financial assistance, under the Stafford Act. Given the extent of the damage, I believe federal financial support for infrastructure recovery efforts in Puerto Rico is appropriate, consistent with the parameters set forth in the Stafford Act and other authorized funding mechanisms.

22. What steps should the federal government take, in your opinion, to ensure that infrastructure repairs made in disaster-affected communities are designed to better withstand future disasters?

I agree with my colleague FEMA Administrator Brock Long, who provided perspective on this topic during his testimony to the Senate Committee on Homeland Security and Governmental Affairs in October 2017. I believe that building more resilient communities is the best way to reduce risks to people, property, and taxpayer dollars. Developing resilient capacity ahead of an incident limits potential consequences,

ultimately reducing loss of life and economic disruption. When communities are impacted, they should strive to rebuild damaged infrastructure better, tougher, and stronger.

Accordingly, I believe that it is the federal government's responsibility to ensure that when federal funds are used to rebuild disaster-affected communities, resiliency should be considered in the evaluation and design of the project and, where cost-effective, included in the project. It has long been an NPPD principle to encourage state, local, and private sector owner and operators to consider security and resiliency during the initial design phase of any major infrastructure investment. If I am confirmed, NPPD will continue to provide that guidance to its stakeholders, both pre- and post-disaster.

23. What is your position on the effectiveness of preparedness grant programs in preparing state and local first responders to prevent and respond to potential terrorist attacks?

Although I am not an expert in measuring the effectiveness of preparedness grant programs, I do believe that federal investments have significantly enhanced the ability of state and local first responders to prevent and respond to potential terrorist attacks.

24. In your opinion, is the country prepared to withstand a significant cyber incident? If not, why not, and what more should be done to ensure that the United States is prepared for such an occurrence?

The constantly evolving nature of the technology we integrate into our infrastructure, as well as our adversaries' intent to identify vulnerabilities and exploit to satisfy their objectives, make it challenging to assess readiness at any given time. As mentioned previously, achieving perfect security is nearly impossible, and is not a risk-based approach. Instead, we need to make security investments across the risk management spectrum, to include planning for response and recovery. My sense is that as a nation, we are making progress. The limited impact of campaigns like WannaCry and NotPetya demonstrate that we are getting better at implementing good cyber hygiene and best practices. Yet, as ransomware attacks become increasingly common, we have more work to do. Addressing threats to our Nation's cybersecurity and critical infrastructure requires a coordinated approach not just from the federal government, but also our private sector; state, local, tribal, and territorial government; and international partners. We must focus on actively working with our partners and stakeholders to understand risk, mitigate known threats and vulnerabilities, and build resilience into our systems and infrastructure. This approach will help ensure that when we are attacked, we can minimize the impact and restore essential services as quickly and efficiently as possible.

#### *National Security*

25. The nation faces a wide range of threats, but DHS and NPPD have finite resources to address them.

- a. If confirmed, what principles will guide your decision-making regarding the use of risk analysis and risk-based resource allocation to set priorities within the Department?

Critical infrastructure owners and operators, which include private sector companies as well as federal, state, and local governments, face a multitude of threats. Trying to understand which threats present the highest risk and which threats can best be mitigated is a complex task. If confirmed, I am committed to ensuring that NPPD programs are taking into account the threat and risk mitigation options so we can deliver effective products and services.

- b. How will you determine if some threats or events require enhanced emphasis and investment or have already received sufficient focus?

If confirmed, one of my top priorities would be to ensure that NPPD uses sound risk management practices to guide our activities. I would review existing NPPD programs against the current risk landscape to ensure NPPD's resources are properly aligned to actual risk; track, analyze, and share information on emerging threats to help critical infrastructure owners and operators build in security and resilience to potential threats as they construct or upgrade the Nation's infrastructure; and routinely engage critical infrastructure owners and operators to understand their needs and work with them to design trainings, assessments, and other services to most efficiently and effectively meet their needs.

Another important and effective way to understand whether our activities are effective is to establish robust customer feedback mechanisms. Through this type of engagement, we can better understand customer needs and assess current levels of risk. After analyzing this information and evaluating it in the context of overall risk, we can make informed decisions about how best to allocate finite resources.

#### *Election Infrastructure/Integrity*

26. How many times have you met with senior White House or National Security Council officials to discuss Russia's interference in U.S. elections? Please detail with whom those meetings took place and when.

Strengthening the cybersecurity and resilience of our nation's election infrastructure is a top priority for me. I typically discuss these topics multiple times daily with a variety of executive branch officials, including, but not limited to, White House, NSC, DHS, Department of Justice (DOJ), Federal Bureau of Investigation (FBI), IC, Election Assistance Commission, and National Institute of Standards and Technology officials. These discussions occur in a variety of different circumstances including structured meetings, informal discussions, phone conversations, working meetings and other types

of engagements. Unfortunately, due to the sheer volume, I am not able to provide a full account of the many meetings and discussions I have had on these topics.

27. How many times did you meet with the DHS Secretary on Russia's interference in the U.S. election and /or protecting election infrastructure? Please detail with whom all meetings took place and when.

Strengthening the cybersecurity and resilience of our nation's election infrastructure is a top priority for both me and the Secretary. As I indicated in my response to Question 26, I discuss these topics multiple times daily with different executive branch officials. These discussions occur in a variety of different circumstances including structured meetings, informal discussions, phone conversations, working meetings, and other types of engagements. Unfortunately, due to the sheer volume of my discussions on these topics with Secretary Kelly, Acting Secretary Duke, and Secretary Nielsen, I am not able to capture a full account of the many meetings and discussions I have had on these topics.

28. How many times did you meet with executive branch officials other than White House and DHS personnel on Russia's interference in the U.S. election and /or protecting election infrastructure? Please detail with whom all meetings took place and when.

Please see my response to Question 27.

29. Do you agree with the U.S. Intelligence Community's assessment that the Russian government interfered in the 2016 U.S. Presidential election?

Yes.

- a. If so, does the President's dismissal of those facts concern you?

The President publically stated on November 11, 2017, that he agrees with the Intelligence Community's assessment.

- b. Do you think the DHS designation of election infrastructure as critical infrastructure should stand?

Yes.

30. Please describe the work you have done while at DHS during the current Administration to stand up this critical infrastructure subsector.

DHS designated election infrastructure as a subsector of critical infrastructure on January 7, 2017. Since that time, I have led DHS efforts to stand up the critical infrastructure subsector. These efforts include the establishment of a DHS ETF and an Election Infrastructure GCC in October 2017, and the establishment of an Election Infrastructure SCC in February 2018. These bodies serve as mechanisms for

coordination and information sharing within the subsector, and enhance election officials' understanding of the threat landscape by providing a mechanism to share threat and risk information. NPPD also funded and supported the establishment of the Election Infrastructure ISAC. Personally, I have directed strategic hires at NPPD, like adding former Election Assistance Commissioner Matt Masterson to my staff as a Senior Advisor on Election Security. I have also invested considerable time and effort in building relationships with Secretaries of States from all over this country. I have directed the prioritization of assessments and services to the election infrastructure subsector, and I continue to work tirelessly with my interagency partners to ensure the federal government fully supports election infrastructure security efforts.

31. Do you think the Department needs additional resources and or authorities to fully address the problem in time for the 2018 elections? If yes, please describe.

DHS, specifically NPPD, plays a critical role in supporting state and local election officials as we work collectively to increase the security of the nation's election infrastructure ahead of the 2018 elections. I believe the Department's existing authorities are sufficient to address this problem, and with passage of the Omnibus Appropriations Act, I believe NPPD is adequately resourced to enhance its election infrastructure security activities in FY 2018.

With passage of the FY 2018 Omnibus Appropriations Act, Congress made available \$26.2M of funding dedicated to support NPPD's election infrastructure security activities in FY 2018. NPPD will use this funding to meet emerging requirements in this space ahead of the 2018 elections, specifically:

- Adding capability to offer Offensive Security Assessments / Remote Penetration Testing for all states who request it – up to one assessment per state, per year;
- Developing and distributing a cybersecurity tabletop exercise package stakeholders can use to exercise their cyber incident response plans;
- Increasing the number of Hunt and Incident Response teams by five to provide capacity for 20 hunt engagements per year for election infrastructure;
- Executing additional stakeholder outreach and engagement activities, including the establishment of the Sector Specific Agency to carry forward necessary strategic activities for this subsector;
- Analyzing the most popular voting systems prior to 2018 elections;
- Sustaining additional sensors deployed by the MS-ISAC and conducting analysis on the increased data flow they provide; and
- Developing a comprehensive national-level election system characterization to help provide a better understanding of the myriad election systems deployed across the US.

These key investments will help ensure NPPD is resourced to do accelerate its election infrastructure activities ahead of the 2018 elections. However, state and local officials will likely require additional assistance to retire legacy systems and deploy modern secure and

resilient systems. While the \$380 million Congress provided the Election Assistance Commission in the FY 2018 Omnibus for the establishment of a program to provide federal assistance to state and local election officials was a substantial down payment on those efforts, it will only partly address the problem.

#### *Infrastructure Protection*

32. Looking across the critical infrastructure space, what are the top five threats currently facing U.S. critical infrastructure and how would you position NPPD to best counter them?

Emerging threats in the critical infrastructure space are one of my top concerns. Here are the top five emerging threats that I believe are facing our critical infrastructure:

- Information warfare and influence operations,
- More traditional cyber threats that target infrastructure including industrial control systems,
- Emerging technology and the vulnerabilities associated with using new technology, both within infrastructure operations and due to unforeseen risks posed by incorporating new technology within the supply chain,
- Less sophisticated physical attacks such as improvised explosive devices and unmanned aerial systems, especially those targeting open infrastructure designed to facilitate use by large numbers of people, and
- Natural disasters and large-scale events we cannot foresee or control, which as the 2017 hurricane season demonstrated, can devastate critical infrastructure.

NPPD is best positioned to counter these threats by continuing to partner with infrastructure owners and operators to share the information and experience we have and, when appropriate, work with these stakeholders to develop mitigation measures. If confirmed, I will continue working to mature our relationships with critical infrastructure owners and operators so we are able to better identify threats and respond accordingly.

33. In your opinion, should any adjustments be made to the Chemical Facility Anti-Terrorism Standards (CFATS) program?

The CFATS program is a great example of how government and the private sector can work together through a regulatory regime to enhance the security of critical infrastructure. Implementation of the CFATS program has made the nation's communities more secure by ensuring high-risk chemical facilities are developing and implementing appropriate security plans.

Having said that, I believe CFATS could be more effective and efficient. For example, streamlining inspections, under existing CFATS regulations, is just one way to increase efficiency. To this end, I have already directed the CFATS program leadership to evaluate this and similar opportunities to increase efficiency, and where appropriate, to begin implementing these improvements. If confirmed, I look forward to further



exploring these and other ideas for making the CFATS program more effective and efficient.

#### **Whistleblower Protections**

34. If confirmed, how will you ensure that whistleblower complaints are properly investigated and what specific steps will you take to ensure that NPPD employees feel free to report waste, fraud, and abuse to senior Department leadership, including you, the Inspector General, and to Congress without fear of reprisal?

I understand the importance of ensuring employees are aware of the avenues available to report suspected instances of waste, fraud, abuse, and whistleblower retaliation, and I am committed to an environment where NPPD employees feel confident making any reports they believe appropriate. To ensure reports are properly investigated, whistleblower complaints must be directed to the proper investigative body, typically the DHS Office of the Inspector General (OIG) for whistleblower complaints and the U.S. Office of Special Counsel (OCS) for prohibited personnel practice complaints such as whistleblower reprisals. For matters referred to NPPD by the DHS OIG, the NPPD Office of Compliance and Security (OCS) maintains an Internal Affairs program which ensures all incoming allegations of misconduct are routed to the appropriate level of leadership for investigation, administrative inquiry, or management action.

As SOPDUS, I have worked to ensure NPPD communicates to its employees the various means available to report waste, fraud, abuse, or retaliation. NPPD leverages existing DHS OIG procedures for reporting, including the OIG Online Allegation Form, phone line, fax, and U.S. Mail. NPPD employees can also file prohibited personnel practice complaints directly with the OCS using the OCS website's e-filing application. OIG and OCS contact information is posted throughout NPPD worksites, and it can be easily found on the NPPD and FPS public-facing websites as well as the NPPD intranet websites. My staff is also engaged in an ongoing initiative with the DHS Office of Civil Rights and Civil Liberties (CRCL) to post this information at all FPS-staffed security posts.

Additionally, NPPD employees, like all DHS employees, are required to complete NO FEAR Act training every two years. This training provides federal employees with information on their rights and the remedies available under the antidiscrimination, retaliation, and whistleblower protection laws. NPPD also publishes the NPPD Vision, a weekly e-newsletter featuring stories about employees and resources for employees including updates on training, professional development and other NPPD and DHS-related news. Through this channel, NPPD leadership communicates information pertaining to the options available to NPPD employees for reporting suspected misconduct. NPPD also maintains an Ombudsman program that provides employees information on formal means available to address complaints or concerns, while also facilitating prompt informal resolution of NPPD personnel concerns. The Ombudsman

program also provides NPPD leadership with a candid perspective on systemic personnel issues.

**I believe NPPD has adequate procedures in place to ensure employees have awareness of and access to whistleblower reporting channels, and if confirmed, I would work to ensure these procedures are maintained.**

**Congressional Relations**

35. If confirmed, do you agree without reservation to reply to any reasonable request for information from the Ranking Member of any duly constituted committee of the Congress?

**If confirmed, I would comply without reservation.**

36. If confirmed, do you agree without reservation to reply to any reasonable request for information from members of Congress? If directed by the administration to systematically ignore oversight requests from minority members of Congress, will you comply?

**If confirmed, I would comply without reservation.**

37. If confirmed, do you commit to take all reasonable steps to ensure that you and your agency comply with deadlines established for requested information?

**If confirmed, I would take all reasonable steps to comply with such deadlines.**

38. If confirmed, do you commit to protect subordinate officials or employees from reprisal or retaliation for any testimony, briefings or communications with members of Congress?

**If confirmed, I will ensure subordinates are protected from reprisal or retaliation for communications with Members of Congress.**

39. If confirmed, will you direct your staff to fully and promptly respond to Freedom of Information Act requests submitted by the American people?

**If confirmed, I will work to ensure NPPD Freedom of Information Act officials are in compliance with FOIA statutory requirements and take all reasonable steps to respond to requests submitted by the American people.**

40. If confirmed, will you ensure that political appointees are not inappropriately involved in the review and release of Freedom of Information Act requests?

**If confirmed, I will ensure that political appointees are not inappropriately involved in the review of Freedom of Information Act requests.**

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

  
(Signature)

This 5 day of April, 2018

**Senator Rand Paul  
Post-Hearing Questions for the Record  
Submitted to Christopher C. Krebs**

**Nomination of Christopher C. Krebs to be Under Secretary, National Protection and  
Programs Directorate, U.S. Department of Homeland Security**

**April 25, 2018**

*On the discovery of "Stingrays" in and around Washington, DC:*

DHS recently acknowledged it has observed "anomalous activity in the National Capital Region (NCR) consistent with International Mobile Subscriber Identity (IMSI) catchers," also known as cell-site simulators or "Stingray" devices. The American public has a legitimate interest in understanding the security implications of these devices, including their surveillance and location tracking capabilities. On April 18, 2018, I, along with Senators Wyden, Gardner and Markey, sent you a letter requesting public disclosure of unclassified information regarding IMSI catchers in the NCR and other malicious activity on American cellular networks.

1. In evaluating your nomination, a commitment to transparency and protecting American civil liberties are of paramount importance; please provide your response to this Congressional request at this time.

I received your letter dated April 18, 2018. The documents you requested contain information marked "For Official Use Only" (FOUO). As a result, this information is not currently eligible for public release, and must be handled in accordance with DHS Management Directive 11042.1 *Safeguarding Sensitive but Unclassified (For Official Use Only) Information* (MD 11042.1). If confirmed, I commit to ensuring the documents are reviewed by a supervisory or management official who has the appropriate technical understanding of the subject matter and program management responsibility over the originator and the information. If that review results in a determination that some or all of the information is no longer FOUO, I would not hesitate to remove the FOUO marking.

*On border searches:*

Within DHS, NPPD is best positioned to understand security risks associated with illegal or stolen digital material. Your expertise may inform how DHS handles cyber security issues outside NPPD's jurisdiction, such as warrantless searches at the border. Court precedents have established a border search exception to the Fourth Amendment, reasoning that the government has a special interest in containers at points of entry because of the threat of introducing physical contraband. By contrast, electronic contraband can be instantly shared from

anywhere in the world. In fact, border crossing is the most expensive, most attributable, and slowest method available for sharing such contraband.

1. Do you believe the government has any more interest in data on a phone in Brownsville, Texas, than on a phone in Brownsville, Kentucky?
2. What properties distinguish digital contraband from physical contraband?
3. Should government maintain a unique border search exception to the Fourth Amendment to inspect a U.S. citizen's most personal digital papers and effects without a warrant or suspicion?

In response to all three questions above:

As I understand it, Customs officers have statutory authorization to conduct a border search of travelers, conveyances, and merchandise crossing the United States border. Border searches may be performed at the border (the territorial boundaries of the United States that exist on land, sea, and air) or the functional equivalent of the border (e.g., the airport where an international flight to the United States lands). I have not been involved, directly or indirectly, with the interpretation or execution of the Department of Homeland Security's border search authorities. Similarly, I have no knowledge of how law enforcement officers distinguish digital contraband from physical contraband, or whether such a distinction makes a difference in the context of a border search. I do believe that lawfully conducted border searches are a valuable tool for law enforcement. My understanding of the current state of jurisprudence is that the Supreme Court has long recognized that the border search doctrine operates as an exception to the warrant and probable cause requirements of the Fourth Amendment, and the government should maintain this exception, subject to a change in law or precedent.

*On encryption:*

Nearly all Americans protect their private and commercial communications with encryption tools like Virtual Private Networks (VPN) and Transport Layer Security (TLS). A number of governments have deliberately compromised the integrity of popular encryption tools. Of course, a flaw designed to make encryption more tractable by one government may be exploited by another.

1. Are flaws impacting the confidentiality of popular encryption tools a national security threat?

Flaws impacting the confidentiality of popular encryption tools can pose a national security risk. Insecure encryption tools open a large number of network users, including the general public, to unauthorized intrusions that could expose sensitive and personally identifiable information.

*On cybersecurity compliance and federal requirements:*

DHS has issued only six Binding Operational Directives (BOD) since 2014. Despite modest requirements, agency compliance is poor. For instance, only 57% of federal websites and 47.1% of federal email domains met BOD18-01 deadlines.

1. How do you plan to enforce existing and future directives? Are BOD's a sufficient tool? How do you plan to use BOD's going forward?

DHS works closely with our federal agency partners to ensure compliance with binding operational directives (BODs). While compliance by BOD varies, I would rate overall compliance across all BODs as good. The compliance rate of BOD 18-01 is one exception to this success story for three reasons. First, configuring strong email authentication across agency enterprises is not an easy task. While the Federal government leads industry in DMARC adoption, more work is certainly necessary. Next, compliance with BOD 18-01 actions in many cases requires industry service providers to comply with several actions such as those related to disabling weak encryption. While the BOD has driven change at several providers, several actions require major corporations to make significant technical changes for all their customers in order to ensure compliance with their Federal customers. And lastly, implementing the BOD 18-01 actions requires subject matter expertise, resources, and in some cases technical capabilities beyond the capability of some agencies. As a result, it will take some time and planning to get the proper resources in place to execute on these actions.

BODs have historically been issued by the Secretary of DHS to federal departments and agencies as high-priority items whose implementation status is followed closely by DHS senior leadership. When implementation issues arise, DHS engages with department or agency Chief Information Officers and Chief Information Security Officers to determine why and develop an implementation plan. If the department or agency continues to be in non-compliance, the DHS Assistant Secretary for Cybersecurity and Communications engages with his or her counterparts at each non-compliant agency. When additional attention is needed, DHS works with the Office of Management and Budget. Ultimately, the Secretary or Deputy Secretary of DHS will, at their discretion, contact their counterparts at each non-compliant agency.

BODs have generally been successful in highlighting and mitigating cybersecurity risks to federal networks. For example, BOD 15-01 reduced the number of outstanding critical vulnerabilities to Internet-facing systems across the federal government by over 99%. It also altered the way federal agencies review and respond to DHS cyber hygiene scans. In addition, BOD 16-01 and 16-02 have been successful in identifying and addressing long-standing issues related to End-of-Life Systems and legacy IT. Across all BODs, NPPD has observed positive organizational changes that have helped achieve an enhanced cybersecurity posture in federal networks.

The Department's current BOD authorities have proven sufficient to drive significant cybersecurity change, impact cross-government performance, and mitigate substantial cyber threats and risks to federal information systems. Going forward, NPPD plans to continue leveraging the BOD to advance government-wide actions, implement critical requirements, and raise awareness and emphasize the urgency of specific actions to secure federal information systems. In support of these goals, NPPD plans to develop BODs that address both strategic priorities and longer-term initiatives, as well as urgent matters such as ongoing and imminent threats.

**Ranking Member Claire McCaskill  
Post-Hearing Questions for the Record  
Submitted to Christopher C. Krebs**

**Nomination of Christopher C. Krebs to be Under Secretary, National Protection and  
Programs Directorate, U.S. Department of Homeland Security**

**April 25, 2018**

**ELECTION SECURITY FOLLOW-UP**

Yesterday Assistant Secretary Manfra testified before this Committee. Regarding in-depth risk and vulnerability assessments (RVAs) DHS offers, Assistant Secretary Manfra confirmed that 17 states had requested the service. When I asked if any states were “waiting right now for an assessment that they have not been able to get,” Assistant Secretary Manfra said, “Nobody in the election community is waiting for an assessment.”

Q: Have all 17 states that requested RVAs from DHS already received the service and the request has been completed?

DHS has received requests for in-depth risk and vulnerability assessments from 17 states. Of the 17 requests, nine are complete, six are scheduled, and two are being scheduled.

We also received RVA requests from seven local jurisdictions and one private sector company, for a total of 25 election-related RVAs. We expect that number to increase as we approach the upcoming 2018 midterm elections.

It is important to emphasize that there is no backlog or waitlist for an organization to receive an election-related RVA. Due to the in-depth nature of these assessments, organizations that request an RVA may have to conduct preparatory work before the assessment can be conducted. All organizations that request an election-related RVA will receive that RVA when they are ready for the RVA.

**CYBERSECURITY**

Cyber threats evolve very quickly. Hackers are constantly learning of new vulnerabilities and ways to exploit them. The federal budgeting and appropriations process, on the other hand, is not very nimble. It is a rigid system that provides little leeway for federal agencies to adapt to new cyber threats.

Q: Do you think we need to modify or adjust the appropriations and/or contracting processes to provide more flexibility as technology and innovations rapidly evolve?



Flexibility in the procurement process could help DHS and other agencies to identify and deploy innovative technologies in a more rapid, agile manner, enabling network defenders to keep pace with the evolving threat environment. The appropriations process should also provide flexibly for departments and agencies to make the capital investments necessary to retire legacy IT systems and move to more modern platforms that are easier to defend, more efficient, and that provide better services to tax payers.

We have seen global cyberattacks like WannaCry and NotPetya indiscriminately affect a variety of networks. The attacks were not isolated to just the financial or healthcare sectors, but instead spread quickly to other systems with the same vulnerabilities.

Q: Do you think we should update or modify how critical infrastructure is categorized, or do you think the 16 sectors, although they share some characteristics, are discrete enough to remain separate?

I believe the current critical infrastructure sector categorization serves as a useful baseline organizing function for the nation's approach to critical infrastructure risk management. The 16 sectors provide the necessary context by which we can collectively view the nation's critical infrastructure and related interdependencies. Within this underlying context, however, we recognize that many assets, systems, networks, and the threats they face often cut across a sector or sectors. We are increasingly taking a risk-based approach to understanding the national cybersecurity risk management challenge. This approach requires an understanding not just of the threat and the targets, but also the underlying vulnerabilities and associated consequences of potential successful exploitation of a vulnerability. This approach allows us to identify what is truly critical and focus efforts accordingly. It is important to recognize that as our adversaries shift their focus and tactics, our priorities and judgements with respect to the criticality of infrastructure may also shift. Therefore, the 16 sector approach remains a flexible and effective coordination mechanism for infrastructure security and resilience activities among the relevant entities.

Q: DHS has the capability to help federal agencies with incident response if necessary. In 2016, the Obama administration announced that it planned to increase DHS's cyber defense teams from 10 to 48. Is that still the government's policy? If so, how many teams are there now and how often are they deployed?

The NCCIC currently fields 20 cyber-focused teams of varying capability and focus, and, if confirmed, I intend to continue prioritizing the build-out of these capabilities. The Hunt and Incident Response Team (HIRT) program has 11 incident response teams. They can deploy up to four fully-equipped teams simultaneously, and we expect to increase that capability to six by the end of the calendar year. These teams are deployed regularly, and have 25 completed or pending deployments so far in FY 2018. In addition to incident response capabilities, the National Cybersecurity

Assessment and Technical Services program has capacity for nine simultaneous Risk and Vulnerability Assessment (RVA) teams. These teams provide stakeholders with proactive risk mitigation services to minimize exposure and close vulnerabilities prior to exploitation.

NPPD remains committed to increasing our internal incident response capability. We are also working with the General Services Administration (GSA) to explore mechanisms that can provide departments and agencies with greater and faster access to such capabilities from commercial providers.

#### **CYBER WORKFORCE**

In 2014, special authorities were granted to DHS to help recruit and retain critical talent and close gaps in the cybersecurity workforce. These authorities were modeled after DOD programs which are already in use to bring in critical talent.

Q: If a model already exists for doing this, why is it taking DHS so long to develop its program and implement its authorities?

DHS leads implementation of the Cyber Personnel Management System across the Department. The DHS Office of the Chief Human Capital Officer (OCHCO) has benchmarked DOD programs and determined that they are still very much aligned with traditional Title 5 authorities. DHS seeks to build a more modern and flexible system that can help the Department recruit and retain cyber talent both now, and into the future. Accordingly, developing and deploying this modern system takes time and pragmatism to get right.

In the meantime, NPPD continues to utilize the excepted service direct hire authority provided in the 2014 law. About 9% of the Department's cyber workforce is hired through this mechanism.

Q: What's your deadline for implementing these authorities? When can we expect these authorities to be used?

As noted above, approximately 9% of the Department's cyber workforce is hired through the excepted service direct hire authority provided in the 2014 law. DHS anticipates delivery of the new Cyber Personnel Management System in late FY 2019.

Q: Have you done a workforce or gap analysis of what types of positions you need, how many, and where? What positions do you need, how many, and where?

In coordination with DHS, NPPD developed an FY 2018 Cyber Workforce Plan focused on various job series in the cyber workforce, rather than just singling out the Information Technology Specialist (2210). Those series include 0301 (Cyber

Program Manager), 0343 (Management Analyst), 2210 (Information Technologist), and 0840 (Engineering) job series, which all align to the relevant National Initiative for Cybersecurity Education (NICE) Framework specialty areas. NPPD identified 1164 positions within our workforce as cyber positions, and we currently have 811 of these positions filled. We are focused on recruiting in all program areas to close the gap. To date, NPPD has completed an environmental scan of the workforce plan to gain an understanding of the environmental factors impacting hiring for cyber positions. NPPD continues to develop staffing targets for the upcoming years, and we are prioritizing those positions most critical to the mission. We anticipate having a full understanding of the positions we need to hire and where in the organization those positions fit by the end of FY 2018.

### **EMERGENCY MANAGEMENT**

When disasters strike, NPPD has several specific responsibilities outlined in the National Response Framework – mostly in the form of critical infrastructure protection and communications restoration.

Q: You stated in your policy questionnaire that NPPD has identified “50 areas for improvement” following the 2017 hurricane season. Please provide the Committee with a list of those areas for improvement NPPD identified.

At my direction, following the conclusion of the 2017 hurricane season, the National Infrastructure Coordinating Center (NICC) reviewed all aspects of NPPD response and short-term recovery efforts in support of Hurricanes Harvey, Irma, and Maria. This effort resulted in the development of an NPPD 2017 Hurricane Season After Action Report (AAR) that identifies the processes and procedures that contributed to NPPD’s success during the 2017 hurricane season, as well as gaps that challenged NPPD. The AAR, which currently is undergoing final review, highlighted approximately 50 areas for improvement across various categories of activities. If confirmed, I commit to providing these recommendations to the committee once the final review is complete.

As you may be aware, the FEMA Administrator told this Committee that building “survivable communications” networks is his top priority for increasing our preparedness for future disasters.

Q: What role do you believe NPPD has to play in this effort?

Under Emergency Support Function #2 of the National Response Framework, NPPD has primary responsibility for coordinating the restoration of communications infrastructure following a disaster. During the 2017 hurricane season, I saw first-hand the impact that loss of communications can have during a natural disaster, as well as the challenge of restoring communications after they have been lost. I agree with FEMA Administrator Long’s characterization of the value of building survivable communications networks. If confirmed, I would direct

NPPD to assist Administrator Long in this endeavor to the extent allowable within our existing authorities. This could include performing vulnerability and risk assessments of existing communications networks, providing guidance and best practices on establishing more resilient communications networks, and convening stakeholders to identify ways to work collaboratively to implement these more resilient networks.

#### **CHEMICAL FACILITY ANTI-TERRORISM STANDARDS**

Q: Do you think the Chemical Facility Anti-Terrorism Standards (CFATS) program should be reauthorized? Why or why not?

Terrorists around the world continue to demonstrate both the intent and desire to use chemicals as weapons. The Chemical Facility Anti-Terrorism Standards (CFATS) program is a key component of our nation's ability to counter the threat of the misuse of chemicals, and it continues to drive down the risk of misuse of chemicals by terrorists within our borders. Through this smart and flexible regulation, thousands of security measures have been implemented to make the nation more secure. Moreover, because of CFATS, thousands of chemical facilities have made changes to their chemical holdings or the manner in which they store their hazardous materials, reducing the risks both to the facility and to the surrounding community. The CFATS program is a great example of how government and the private sector can work together through a regulatory regime to enhance the security of critical infrastructure and should be reauthorized.

Q: What, if any, legislative changes do you think should be made to the CFATS program? How should cybersecurity threats be better incorporated into CFATS' risk based performance standards, if at all?

Existing statutes provide NPPD with the authorities necessary to administer the CFATS program. However, changes to a few key areas could make the program even more efficient and effective. For example, creating a process to allow stakeholders to petition the Department for exclusion of specific products or materials from Appendix A reporting requirements could enhance the CFATS Expedited Approval Program and Personnel Surety Program. In addition, changes to the CFATS whistleblower retaliation claims process could enhance its overall effectiveness.

Cybersecurity at chemical facilities is an ongoing concern. The systems and networks at chemical facilities, such as Industrial Control Systems, Supervisory Control and Data Acquisition systems, and inventory management systems, often present vulnerabilities that can be exploited by sophisticated adversaries. As a result, cybersecurity is a key part of a comprehensive security approach for chemical facilities. Under CFATS, high-risk chemical facilities must implement security plans that meet cybersecurity requirements set forth in CFATS Risk-Based

Performance Standard (RBPS) 8 – Cyber. While the Department should periodically review the cybersecurity requirements mandated by RBPS 8 to ensure that they address the latest cybersecurity threats, I believe that the current CFATS program adequately incorporates cybersecurity.

Some of the threats we face today involve small amounts of chemicals that can be mixed in a small container, like a backpack – rather than a larger vessel, like the truck bomb that was used in the Oklahoma City attack more than two decades ago.

Q: Do you think the types and quantities of chemicals that are regulated under CFATS are appropriate, or do you think the law should be updated to reflect the current threat environment?

CFATS is designed to help prevent mass casualty events involving chemicals by requiring high-risk chemical facilities to implement comprehensive security programs. While updates to the regulations are worth considering, I generally believe that the types and quantities of chemicals that are regulated under CFATS are appropriate for the CFATS mission. The comprehensive security approach required under CFATS, however, likely would not be a cost-effective approach to addressing smaller scale threats involving chemicals due to the small amount of chemicals necessary to carry out such threats, the large number of chemicals that could be used as or in small scale weapons, and the wide-spread availability of those chemicals at home improvement stores, agricultural supply retailers, pool stores, hobby shops, convenience stores, and beyond.

Rather than modifying the CFATS chemicals of interest list, it may be more effective to explore a separate approach to address small scale chemical threats that incorporates both voluntary and regulatory programs focused on the point-of-sale of the chemicals. This is consistent with the recommendations made by the National Academy of Sciences in their recent report, *Reducing the Threat of Improvised Explosive Device Attacks by Restricting Access to Explosive Precursor Chemicals*.

#### **MEDIA MONITORING**

On April 3, 2018, NPPD issued a Request for Information for “Media Monitoring Services.” According to the attached Scope of Work, NPPD is seeking a contractor to collect information from more than 290,000 news sources and to compile a searchable database of journalists and media influencers.

Q: Under what legal authority is this solicitation being made?

DHS, on behalf of NPPD, issued a Request for Information (RFI) to determine options for commercially-available media monitoring services to help the organization keep track of breaking news and current events. This RFI is only one part of a multi-step process that may ultimately result in the acquisition of services.

DHS often engages privacy, civil liberties, and legal experts to ensure compliance with all appropriate policies and procedures in the acquisition and eventual execution of these services. If the RFI leads to a procurement, the use and implementation of such services will be in accordance with the law and existing DHS practices, policies, and laws including those on privacy, civil liberties, and the operational use of social media platforms.

Q: What is the status of this solicitation? How many firms responded to the RFI, what did NPPD learn for their responses, and what is your agency's next course of action?

DHS has not issued a solicitation. DHS issued an RFI to obtain additional information on capabilities available in the commercial market. 30 firms responded to the RFI. DHS is currently working to complete a market research report based on the responses to the RFI. Going forward, this report will assist with the development of a procurement strategy.

Q: How does this solicitation relate to current efforts at other entities, including the Department of State and National Monitoring Center? In your view, would DHS media monitoring be duplicative of these efforts?

This RFI sought additional information on media monitoring capabilities available in the commercial market. If the RFI results in a procurement, the services sought will be tailored to NPPD's specific mission areas and requirements. Any services obtained will not be duplicative of media monitoring services in use at other departments and agencies.

Q: Why is NPPD interested in building a searchable database of journalists and media influencers?

Over the past ten years, the cyber and infrastructure security threat environment has grown significantly, as has the breadth and volume of reporting on these topics. It is critical that NPPD understand trends in this reporting and analysis and have the ability to engage the journalists and experts reporting on issues within this mission space. Many mature organizations in the private and public sectors have capabilities similar to those outlined in the RFI. NPPD is also somewhat unique in that our name does not clearly reflect the organization's mission. As a relatively unknown organization, particularly compared to other more established, clearly branded Federal agencies, communication and engagement with external audiences is difficult. A searchable record of media coverage within NPPD's mission space will allow NPPD to identify journalists who cover our issues, share news and policy announcements with the right journalists, and better understand who to invite to engagements and events.

Q: How will this data be used by NPPD?

If the RFI results in a procurement, NPPD external affairs personnel would leverage available data and incorporate reports and analysis from media monitoring services into NPPD's public information, public awareness, and incident communications programs in order to better reach federal, state, local, and tribal officials; industry and non-governmental partners; academia; and the general public.

Q: Who will have access to the data – both internally at NPPD/DHS and externally?

Access to data would be determined in part by the final terms of any potential award. If confirmed, and if this RFI results in a procurement, I commit to providing the committee with additional information on who will have access to data compiled using this service.

Q: What is the anticipated cost to the federal government of building this system?

NPPD is not building a system. If this RFI results in a procurement, NPPD would seek to purchase services that exist in the commercial market place. While NPPD is not far enough along in the procurement process to provide a detailed cost estimate, we anticipate that the annual cost for services of this nature would fall below the FY 2017 Simplified Acquisition threshold of \$150,000. If confirmed, and if this RFI results in a procurement, I commit to providing the committee with a more detailed cost estimate when it becomes available.

Q: To what extent was the Department's Office for Civil Rights and Civil Liberties involved in drafting and/or reviewing the RFI, and what actions will NPPD/DHS take to ensure that First Amendment freedoms are protected?

The DHS Office of Civil Rights and Civil Liberties was not involved in drafting or reviewing the RFI. If the RFI results in a procurement, the use and implementation of any media monitoring service will be in accordance with existing DHS practices, privacy, civil rights and civil liberties, legal, and operational use of social media policies.

**Senator Gary C. Peters  
Post-Hearing Questions for the Record  
Submitted to Christopher C. Krebs**

**Nomination of Christopher C. Krebs to be Under Secretary, National Protection and Programs Directorate, U.S. Department of Homeland Security**

**April 25, 2018**

1. The attempted takeover of a dam in New York State by Iranian hackers, the successful intrusion into computer systems at U.S. power plants by Russian hackers, and recent ransomware attacks that crippled municipal systems in Atlanta and Baltimore emphasize the need for NPPD to continue to work proactively with non-federal entities to raise the baseline level of security and response capabilities across the country. However, according to the 2017 National Preparedness Report, more states and territories rate themselves as lacking proficiency in cybersecurity than any other core capability. DHS preparedness grant programs can be critical tools to mitigate both physical and cyber risks to critical infrastructure, but spending on cybersecurity-related activity is a fraction of that for other core capabilities.

**What specific steps would you take to encourage recipients of DHS preparedness grant funding to use these programs to address their self-reported lack of proficiency in cybersecurity?**

NPPD is working with FEMA to develop grant guidance which would provide grant recipients with recommendations for better using preparedness grant funding to address cybersecurity gaps. NPPD will be available to support FEMA and grant recipients as they make decisions regarding use of funding.

**What role do you envision for NPPD in working with FEMA and states to improve baseline cybersecurity proficiency?**

NPPD and FEMA are already partnering to coordinate support to our partners in the State, Local, Tribal, and Territorial (SLTT) cyber community and increase overall baseline preparedness. For the FY18 grant cycle, NPPD and FEMA worked to refine FEMA's grant guidance and develop a stakeholder communication and technical assistance plan. The technical assistance plan ensures SLTT grant recipients have the necessary guidance and support to develop meaningful, measurable and compliant investment justifications. Going forward, the SLTT cyber community will be represented at Homeland Security Grant Program and Urban Area Security Initiative planning activities within the states and urban areas. While investment decisions are ultimately up to the states and urban areas, placing SLTT cyber community representatives in these planning activities ensures cyber



threats, risks, and capability gaps are considered in the development of grant investment plans.

For FY19, NPPD and FEMA will continue this line of effort and begin analyzing SLTT baseline preparedness information from across both Components. The findings and analysis will be used to help further guide future year grant guidance.

**Because critical infrastructure assets often cross state or municipal boundaries, how would you incentivize regional and cross-boundary cooperation and encourage different jurisdictions to pool their resources in order to improve resiliency and mitigate risks to critical infrastructure assets?**

As DHS established the infrastructure protection mission following the terrorist attacks of September 11, 2001, it focused primarily on national level risk in order to better understand overall risk to critical infrastructure. In recent years, NPPD has increased focus on better understanding shared risk at the regional level and providing actionable recommendations and information to our partners to mitigate these risks. NPPD has deployed additional staff to the field so they better understand local and regional infrastructure and can work directly with state and local government and provide sector partners to drive down regional risk. Through these relationships, we are able to advise our partners on how best to use their resources to address shared risk.

2. Although voting machines are not directly connected to the internet, there is an opportunity for bad actors to infiltrate election management computers that are used to program voting machine ballots. Various jurisdictions outsource ballot programming to small, outside vendors. For example, in my state, 75% of Michigan counties use just two companies with about 20 employees each. Bad actors could target these companies, which due to their size may lack the resources to implement sufficiently robust security protocols, and infect election management computers in order to spread malware to voting machines.

**What proactive engagement is DHS doing with election infrastructure and management vendors of all sizes to make them aware of DHS capabilities or assist in risk and vulnerability assessments?**

There are a few avenues by which we can improve the security of election technology sold by vendors to states, including working with states to help them develop security standards and requirements for purchased equipment, and working directly with vendors to help them better understand the threat environment and continue to improve their security practices.

On the first, a number of states have established standards and guidelines governing voting machines, and many vendors have submitted their equipment through a

voluntary compliance process run by the US Election Assistance Commission (EAC) and the National Institute of Standards and Technology (NIST). All certification information testing is publicly available at EAC.gov. Additionally, most states have certification testing processes to evaluate the appropriateness of the systems for use in the state. Recognizing that there is more to be done, we are engaging election officials through the Government Coordinating Council on funding considerations, security best practices, and guidance for consideration by election officials to ensure vendors deliver certain security outcomes in election equipment. Auditability is an important assurance mechanism for any critical process, representing one example of a security best practice for voting systems.

On the second, while we do not have a full understanding of which individual vendors follow cybersecurity best practices, DHS continues to work with vendors of voting systems to better understand their products and service offerings. I am pleased to report that some private sector vendors have established an Election Infrastructure Sector Coordinating Council (SCC) under the DHS-administered Critical Infrastructure Partnership Advisory Council framework. The SCC provides a forum for sharing threat information between the Federal government and council partners, advancing risk-management efforts, and providing federal agencies with insight into the security landscape faced by industry. Additionally, as part of the Election Infrastructure Subsector, DHS prioritizes the availability of cybersecurity-focused resources to vendors.

**Does the classified nature of sensitive information about threats to election systems present an impediment to engaging private election infrastructure vendors, and what is being done to overcome this issue?**

No. NPPD has procedures in place to share classified threat information with all of our stakeholders, including election infrastructure vendors, as needed. While I am pleased with the progress NPPD has made on this front, we remain committed to further improving our information sharing processes.

3. This Committee has jurisdiction over the decennial census, and cybersecurity is a critical determinant of a successful census in 2020. Because the 2020 Census will be the first conducted primarily online, ensuring the security of back-end data collection systems and the thousands of mobile devices that will be used to conduct in-person follow-up will be necessary to safeguard sensitive data. Respondents must also trust that the Census Bureau will protect their information, and cybersecurity challenges risk impacting response rates. As the lead entity responsible for the security of federal systems, NPPD has a role to play as well.

**What is the extent of NPPD's working relationship with the Census Bureau?**

NPPD has established and maintains robust relationships with Department of Commerce and the Census Bureau, and provides targeted support and service delivery across the Department of Commerce. These relationships are critical to

NPPD's federal cybersecurity initiatives and our ongoing efforts to deploy capabilities to federal departments and agencies. NPPD works closely with the Department of Commerce and has supported the Department of Commerce's efforts to implement all of NPPD's priority cybersecurity programs such as Continuous Diagnostics and Mitigation (CDM), EINSTEIN, Trusted Internet Connections (TIC), and Automated Indicator Sharing.

Both the Department of Commerce and the Census Bureau have also been active participants and partners in other NPPD-provided services such as incident response exercises, High Value Asset assessments, Risk and Vulnerability Assessments (RVAs), and threat information exchanges. NPPD and the Census Bureau are also exploring opportunities to collaborate on additional cybersecurity services, including a red team assessment. Red team assessments are 90 day engagements where NPPD tests the participating Department's or Agency's ability to detect and respond to activity typically associated with a nation state actor. The information gained through these assessments can help NPPD and the participating department or agency better understand their readiness to identify adversary activity on their network and determine if they have the proper controls in place.

More broadly, the Office of Management and Budget (OMB), NPPD, the Department of Commerce, and the Census Bureau are working together to coordinate additional DHS programmatic support and technical assistance to the Census Bureau. NPPD meets regularly with the Census Bureau's Chief Information Officer (CIO) and cybersecurity team to discuss needs, share information, and coordinate service delivery. NPPD has and will continue to work closely with the Department of Commerce and the Census Bureau on a focused engagement in support of the decennial census.

**What can NPPD do to help improve the security of Census Bureau systems and networks, including the security of the mobile devices that will be used by census enumerators in 2020?**

In accordance with the Federal Information Security Modernization Act of 2014 (FISMA), departments and agencies are responsible for securing their own systems and networks and managing risk across their enterprise. NPPD helps departments and agencies better manage their cyber risk by working to raise the federal cybersecurity baseline; sharing information; measuring, motivating, and driving performance; and responding to cyber incidents.

NPPD has and will continue to actively engage the Census Bureau in support of efforts to secure and safeguard their systems and networks related to the 2020 Census. NPPD meets with the Census Bureau CIO and cybersecurity team regularly to coordinate activities and ensure the implementation of government-wide operational requirements as well as to collaborate and provide technical assistance. NPPD will continue to work with the Census team on recommended security architecture enhancements, and to provide guidance related to security

capabilities in support of the Census hybrid cloud and the application platform. NPPD is aware that the Census Bureau acquired mobile device services to address this need. We will continue collaborating to ensure both compliance and security needs are met regarding continuous monitoring, intrusion detection, and inspection capabilities are consistently applied. NPPD is working closely with the Census Bureau to identify and make recommendations based on gaps, challenges, and issues highlighted throughout testing and this ongoing engagement.

**In what ways can the relationship between NPPD and the Census Bureau be strengthened further?**

NPPD continues to drive interagency collaboration and information sharing as a cornerstone to securing federal information systems. Under FISMA, federal agencies are responsible for securing their own systems and networks and managing risk across their enterprise. NPPD helps agencies manage their risk by sharing information, providing technical assistance, and leading focused engagements. NPPD plans to continue providing the Census Bureau with technical assistance, advice, guidance, and information in support of specific Census Bureau activities. NPPD is working with OMB and other partners to review Census 2020 requirements and identify any additional assistance or capabilities that can be offered to Census 2020.

NPPD is also working with the Department of Commerce CIO as a part of the collective efforts to secure federal information systems across the Department, including Census 2020 data and systems. It is paramount that NPPD continue to foster these relationships, and we are prepared to support the development and execution of Census-developed plans to increase the cybersecurity of systems and networks in support of Census 2020.

**Senator Kamala D. Harris  
Post-Hearing Questions for the Record  
Submitted to Christopher C. Krebs**

**Nomination of Christopher C. Krebs to be Under Secretary, National Protection and  
Programs Directorate, U.S. Department of Homeland Security**

**April 25, 2018**

1. The Office of Biometric Identity Management (OBIM) within the National Protection and Programs Directorate (NPPD) is responsible for collecting biometric data that can be used by DHS. Having led the California Department of Justice, which has a significant data collection division, I've seen first-hand how important it is to make sure we collect these data in a responsible manner. Large biometric data collection efforts can result in inaccuracies which then poses serious civil rights concerns when the data are used later down the line for law enforcement purposes. A Government Accountability Office (GAO) study in 2016 found that the Federal Bureau of Investigation (FBI) had not taken sufficient steps to evaluate the risk of its biometric data collection tools being used to incorrectly identify individuals that could then become the target of investigations. Specifically, the FBI developed a privacy impact assessment (PIA) at the time that it deployed its new biometrics database, the Next Generation Identification-Interstate Photo System (NGI-IPS) in 2008, but did not update that assessment in a timely manner after NGI-IPS underwent significant changes.<sup>1</sup>
  - a. When was the last time OBIM conducted a full privacy impact assessment (PIA) on its own biometric data collection efforts?

OBIM, then the US-VISIT Program, last completed a full privacy impact assessment of the Automated Biometric Identification System (IDENT) on December 7, 2012. Following the initial assessment, the PIA has been updated continually with multiple appendices to provide transparency into biometric data sharing efforts. The most recent update was published in November 2017. Recent appendices have described international information sharing with Mexico, Bulgaria, New Zealand, and Australia, as well as latent fingerprint interoperability with Texas. Additionally, the DHS Privacy Office published a PIA in April 2018 for biometric data sharing with Greece and Italy, conducted under the auspices of the Preventing and Combating Serious Crime (PCSC) Agreements. Because IDENT is the repository for all DHS Components that collect biometrics, Components may have also conducted impact assessments on their own biometric collections and programs.

---

<sup>1</sup> Government Accountability Office [GAO], 2016. FBI Should Better Ensure Privacy and Accuracy. (GAO Publication No. 16-267). Washington, D.C.: U.S. Government Printing Office.

Looking ahead, OBIM recently awarded the contract for Increments 1 and 2 of the Homeland Advanced Recognition Technology (HART), the replacement system for IDENT. OBIM's privacy personnel will work closely with the DHS Office of Privacy to complete a comprehensive PIA that will describe the technological advances found in HART as well as updated privacy analysis sections describing risks areas and mitigation activities.

- b. What progress has been made on mitigating any privacy risks identified in that assessment?

The IDENT PIA identifies privacy risk areas and mitigations. While not all risks can be reduced to zero, there have been improvements made. In 2017, OBIM conducted matcher tuning of IDENT's largest fingerprint gallery to increase the accuracy of fingerprint matching within in the system. Currently, OBIM is preparing to work with The National Institute of Standards and Technology (NIST) to increase the quality of its biometrics and the accuracy of OBIM's biometric-based matching. NIST will evaluate how biometric algorithms perform against DHS data in order to assess the quality of biometric data within IDENT. NIST will also assess the strengths and weaknesses that may exist in IDENT's current or future algorithms, suggest updates to relevant biometric industry standards, and recommend best practices for DHS adoption. Finally, the new HART system will enhance matching and sharing capabilities, as well as facilitate faster auditing and refinement of data filtering. All of these efforts are designed to improve the overall accuracy and quality of the data within the system, and by extension, will help mitigate privacy risk areas. OBIM intends to ensure privacy mitigations are built into HART as it is developed, and will publish an updated PIA before the system goes live.

- c. Do you commit to making sure that the OBIM Director regularly conducts PIAs on OBIM's biometric collection practices, identifies privacy risks, and works to mitigate them in a timely manner?

If confirmed, I commit to ensuring OBIM works with the DHS Office of Privacy to conduct PIAs on its biometric collection practices, identify privacy risks, and mitigate any identified risks in a timely manner.

###



**The App Association**

February 12, 2018

The Honorable Ron Johnson  
Chairman  
Committee on Homeland Security and Governmental Affairs  
United States Senate  
Washington, District of Columbia 20510

The Honorable Claire McCaskill  
Ranking Member  
Committee on Homeland Security and Governmental Affairs  
United States Senate  
Washington, District of Columbia 20510

Dear Chairman Johnson and Ranking Member McCaskill,

ACT | The App Association writes to express our strong support for the nomination of Christopher C. Krebs to the position of undersecretary of the National Protection and Programs Directorate (NPPD). The App Association has worked with Mr. Krebs for many years in his roles at the Department of Homeland Security (DHS) and in the private sector. We applaud Mr. Krebs's work on legislative and regulatory efforts to make cybersecurity information sharing possible for small and medium-sized businesses; this work is especially important and deserving of recognition. Mr. Krebs's professionalism is beyond reproach, and he possesses the skills and experience necessary to be successful as the leader of the NPPD.

It is more important to the app economy than ever for the federal government to participate in a responsive, flexible, and comprehensive approach to cybersecurity. Innovations across the technology and content industries depend on the security of critical infrastructure as well as the rapid development of defensive measures informed by streamlined information sharing processes. The App Association encourages the Committee to move expeditiously to confirm Mr. Christopher C. Krebs.

Sincerely,

Morgan Reed  
President  
ACT | The App Association

1401 K Street NW Suite 501  
Washington, DC 20005

📞 202.331.2130

🐦 @ACTonline

🌐 ACTonline.org

📘 /actonline.org



607 14<sup>th</sup> St. NW  
Ste. 660  
Washington, DC 20005  
T +1 800 225-5224  
ca.com

April 26, 2018

The Honorable Ron Johnson  
Chairman  
Committee on Homeland Security  
and Governmental Affairs  
United States Senate  
Washington, DC 20510

The Honorable Claire McCaskill  
Ranking Member  
Committee on Homeland Security  
and Governmental Affairs  
United States Senate  
Washington, DC 20510

Dear Chairman Johnson and Ranking Member McCaskill:

CA Technologies strongly supports the nomination of Christopher C. Krebs to serve as Undersecretary of the National Protection and Programs Directorate at the U.S. Department of Homeland Security.

CA has had the opportunity to work with Mr. Krebs on a range of cybersecurity issues in both his current role as Senior Official Performing the Duties of the Undersecretary and in his former role as Director of Cybersecurity Policy at Microsoft. We believe his experience working on issues of critical infrastructure cybersecurity and his demonstrated ability to work effectively with public and private stakeholders make him an ideal candidate for the Undersecretary position.

CA Technologies urges the Committee to favorably report Mr. Krebs's nomination to the full Senate.

Thank you for your consideration.

With warmest regards,

A handwritten signature in black ink, appearing to read 'B. Peter', written over a horizontal line.

Brendan M. Peter  
Vice President, Global Government Relations



CHAMBER OF COMMERCE  
OF THE  
UNITED STATES OF AMERICA

NEIL L. BRADLEY  
EXECUTIVE VICE PRESIDENT &  
CHIEF POLICY OFFICER

1615 H STREET, NW  
WASHINGTON, DC 20062  
(202) 463-5310

April 25, 2018

The Honorable Ron Johnson  
Chair  
Committee on Homeland Security and  
Governmental Affairs  
United States Senate  
Washington, DC 20510

The Honorable Claire McCaskill  
Ranking Member  
Committee on Homeland Security and  
Governmental Affairs  
United States Senate  
Washington, DC 20510

Dear Chairman Johnson and Ranking Member McCaskill:

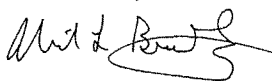
The U.S. Chamber of Commerce supports the nomination of Christopher C. Krebs to be undersecretary of the National Protection and Programs Directorate (NPPD) at the Department of Homeland Security (DHS). NPPD is a central point for interactions between industry and government to defend against threats to the business community that have economic and national security implications.

Mr. Krebs currently serves as the senior official performing duties of the undersecretary for NPPD and oversees the cybersecurity and physical infrastructure security missions of the department. On his second stint at DHS, Mr. Krebs has a deep understanding of cyber and critical infrastructure protection. Mr. Krebs also has relevant private sector experience, including directing cyber policy at Microsoft.

The nominee is a trusted partner among public and private sector professionals. Mr. Krebs has demonstrated a willingness to collaborate with the private sector on an array of issues such as information sharing, chemical security, and supply chain risk management.

The Chamber urges the committee to report Mr. Krebs nomination. We appreciate your consideration.

Sincerely,



Neil L. Bradley

cc: Members of the Senate Committee on Homeland Security and Governmental Affairs



February 25, 2018

Reference: Nomination of Christopher Krebs

Honorable Ron Johnson,

As Chair of Crime Stoppers USA (CSUSA) I would like to support the nomination of Christopher Krebs for the Undersecretary of the Department of Homeland Security's National Programs and Protections Directorate. The announcement of Christopher Krebs as the Undersecretary for the DHS National Programs and Protection Directorate is a positive step in supporting grass roots initiatives such as Crime Stoppers USA in the prevention of violent crimes in our communities. His experience in the realm of infrastructure protection and Cyber Security will serve him well as he leads the effort to keep our communities safe.

Crime Stoppers is a proud and active partner of the Department of Homeland Security and the Nationwide Suspicious Activity Reporting (SAR) Initiative. We value our relationship with the Department and we look forward to working with Chris and NPPD in the future.

Crime Stoppers programs across the country work daily with federal, state and local agencies. We strive to build strong partnerships with government and private sector collaboration as we continue to provide anonymous tip lines for criminal information. I believe under Chris Krebs' direction the collaborative efforts between DHS and CSUSA would thrive.

Sincerely,

A handwritten signature in black ink, appearing to read "Barb Bergin".

Barb Bergin  
Chair Crime Stoppers USA

Crime Stoppers USA, PO Box 64066, Virginia Beach, VA 23467



March 5, 2018

Honorable Ron Johnson  
Chairman  
Senate Committee on Homeland Security and Governmental Affairs  
340 Dirksen Senate Office Building  
Washington, DC 20510

Honorable Claire McCaskill  
Ranking Member  
Senate Committee on Homeland Security and Governmental Affairs  
340 Dirksen Senate Office Building  
Washington, DC 20510

Dear Chairman Johnson and Ranking Member McCaskill:

The Exhibitions and Meetings industry has a \$300 billion dollar impact on our economy, and it is vital we protect all its mass gathering venues around the United States, but more importantly, ensure the safety and security of those millions of people that attend exhibitions, meetings, conferences, and conventions every day.

Our trade associations represent this vital economic engine, and we write to you in strong support of the nomination of Christopher C. Krebs to be the Under Secretary for the National Protection and Programs Directorate (NPPD) in the Department of Homeland Security. We urge the Committee on Homeland Security and Governmental Affairs and the full Senate to act on his nomination quickly to provide DHS, and the Nation, with the full extent of Mr. Krebs' expertise and critical NPPD mission familiarity.

Our industry has been working closely with several components within DHS, including NPPD and the SAFETY Act Office, and created EMSSI (Exhibitions & Meetings Safety and Security Initiative) to develop national safety and security guidelines for convention centers and related venues around the United States. Combined, we have put in over 3,000 work hours dedicated to the development of EMSSI via research, meetings, conference calls, security reviews, industry discussions, and educational forums. We now have over 60 industry organizations supporting this initiative. Our ultimate goal is to have all these venues achieve SAFETY Act Designation and provide this level of certification to elevate the overall safety and security best practices and protocols around

these public assembly structures. Mr. Krebs has made it a priority to enhance the security and coordination for soft targets, and both his NPPD headquarters and regional personnel continue to provide strong support and resources to our industry. In addition, his background as Senior Policy Advisor to the Assistant Secretary for Infrastructure Protection, in addition to his cyber security expertise in the private sector, would be a great asset to our industries' efforts.

The ability to understand both public and private sector infrastructure security needs is a critical responsibility of the Under Secretary for NPPD. The combination of Mr. Krebs' DHS background and experience working on private sector security issues make him uniquely qualified for the position of Under Secretary for the National Protection and Programs Directorate. The International Association of Exhibitions & Events (IAEE), the International Association of Venue Managers (IAVM), and the Exhibition Services & Contractors Association (ESCA) enthusiastically agree that Christopher Krebs would be an outstanding Under Secretary of NPPD, and encourage the Senate to confirm him as quickly as possible. Our country and our industry need his leadership.

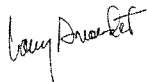
Sincerely,



Brad Mayne, CVE  
President & CEO  
International Association of Venue Managers



David DuBois, CMP, CAE, FASAE, CTA  
President & CEO  
International Association of Exhibitions and Events



Larry Arnaudet  
Executive Director  
Exhibition Services & Contractors Association

April 22, 2018

Honorable Ron Johnson  
Chairman  
Senate Committee on Homeland Security and Governmental Affairs  
340 Dirksen Senate Office Building  
Washington, DC 20510

Honorable Claire McCaskill  
Ranking Member  
Senate Committee on Homeland Security and Governmental Affairs  
340 Dirksen Senate Office Building  
Washington, DC 20510

Dear Chairman Johnson and Ranking Member McCaskill,

As a bipartisan group of former government officials and industry leaders who served or worked closely with the Department of Homeland Security, we write enthusiastically in support of the nomination of Christopher C. Krebs to be the Under Secretary for the National Protection and Programs Directorate (NPPD) in the Department of Homeland Security (DHS). We urge the Committee on Homeland Security and Governmental Affairs and the full Senate to act on his nomination quickly to provide DHS, and the Nation, with the full extent of Mr. Krebs' expertise and critical NPPD mission familiarity.

NPPD is tasked with protecting critical physical and digital infrastructure along with being the first point of federal support for the private sector for cybersecurity crises. With over 3,500 employees and 230 field offices, the men and women of NPPD work around the clock to protect critical infrastructure from digital and physical attacks. The Nation urgently needs a confirmed leader of those dedicated men and women to ensure the safety and security of the Country.

Mr. Krebs first joined the Department of Homeland Security in 2007 as a Senior Policy Advisor to the Assistant Secretary for Infrastructure Protection, a role which he served in for two years. In this position, Mr. Krebs played an intimate role in the implementation of the DHS Chemical Facility Anti-Terrorism Standards regulatory program. Mr. Krebs would also bring substantive private sector knowledge to the role of Under Secretary having served as the Director of Cybersecurity Policy for the Microsoft Corporation. Since rejoining DHS in 2017, Mr. Krebs has played a leadership role and made pivotal contributions to NPPD responses to cyber crises such as the WannaCry ransomware attacks and the federal response to the Meltdown and Spectre vulnerabilities. Mr. Krebs' cybersecurity expertise is particularly needed in the Under Secretary role given the increasing number of severe cyber attacks on our Nation.

Mr. Krebs will bring this extensive industry knowledge and insight to the role of Under Secretary for NPPD, a role which Mr. Krebs has already been fulfilling as the acting Under Secretary since August of 2017. In this capacity, Mr. Krebs has advised DHS leadership on cybersecurity, critical infrastructure protection and recently oversaw the expansion of election infrastructure into a new critical infrastructure subsector within NPPD. Given his strong track record as the

Acting Under Secretary, the Senate has unique visibility now on Mr. Krebs' proven ability to effectively lead in this critical role.

The ability to understand both public and private sector infrastructure security needs is a critical responsibility of the Under Secretary for NPPD. The combination of Mr. Krebs' DHS background and his experience working on private sector security issues makes him uniquely qualified for the position of Under Secretary for the National Protection and Programs Directorate. We are united in agreement that Christopher Krebs will be an outstanding Under Secretary of NPPD, and we urge the Senate to confirm him as soon as possible.

Sincerely,

Michael Chertoff  
Former Secretary  
Department of Homeland Security

Valerie Abend  
Former Deputy Assistant Secretary for Critical Infrastructure Protection & Compliance Policy,  
Department of the Treasury

Jayson Ahern  
Former Commissioner (Acting), Customs and Border Protection

W. Ross Ashley, III  
Former Assistant Administrator, Federal Emergency Management Agency

Thomas Atkin  
Rear Admiral, U.S. Coast Guard (Retired)  
Former Acting Assistant Secretary of Defense for Homeland Defense and Global Security

Stewart A. Baker  
Former Assistant Secretary for Policy, Department of Homeland Security

Michael Balboni  
Former New York State Deputy Secretary for Public Safety  
Former New York State Senator

John Banghart  
Former Director for Federal Cybersecurity, National Security Council

Jeremy Bash  
Former Chief of Staff, Central Intelligence Agency  
Former Chief of Staff, Department of Defense

Ralph Basham  
Former Commissioner, Customs and Border Protection

Rand Beers  
Former Under Secretary of Homeland Security for National Protection and Programs  
Directorate, Department of Homeland Security

Frank Cilluffo  
Former Special Assistant to the President, Department of Homeland Security

Alan Cohn  
Former Assistant Secretary for Strategy, Planning, Analysis & Risk, Department of Homeland  
Security

Jacob Crisp  
Former Deputy Staff Director for National Security, House Homeland Security Committee

Chris Cumiskey  
Former Acting Under Secretary of Management, Department of Homeland Security

Michael Daniel  
Former Special Assistant to the President and Cybersecurity Coordinator

Brian de Vallance  
Former Assistant Secretary for Legislative Affairs, Department of Homeland Security

Caitlin Durkovich  
Former Assistant Secretary for Infrastructure Protection, Department of Homeland Security

Chris Finan  
Former Director of Cybersecurity Legislation and Policy, National Security Council

William F. Flynn  
Former Principal Deputy Assistant Secretary, Office of Infrastructure Protection, Department of  
Homeland Security

Michael E. Garcia  
Former Senior Cybersecurity Strategist, National Protection and Programs Directorate,  
Department of Homeland Security

Deborah Gill  
Former Deputy Chief of Staff, National Protection and Programs Directorate, Department of  
Homeland Security

Jeremy Grant  
Former Director, National Strategy for Trusted Identities in Cyberspace, National Institute of Standards and Technology

Andy Grotto  
Former Senior Director for Cybersecurity Policy, National Security Council

Adam Isles  
Former Deputy Chief of Staff, Department of Homeland Security

Robert D. Jamison  
Former Under Secretary, National Protection and Programs Directorate, Department of Homeland Security

Rob Knake  
Former Director for Cybersecurity Policy, National Security Council  
Special Counselor, National Protection and Programs Directorate, Department of Homeland Security

Andrew J.P. Levy  
Former Deputy General Counsel, Department of Homeland Security

James M. Loy  
Admiral, U.S. Coast Guard (Retired)  
Former Deputy Secretary, Department of Homeland Security

Meghan Ludtke  
Former Chief of Staff, Office of the General Counsel, Department of Homeland Security

Jane Holl Lute  
Former Deputy Secretary, Department of Homeland Security

Bruce McConnell  
Former Deputy Under Secretary for Cybersecurity, Department of Homeland Security

Mike McNerney  
Cyber Policy Advisor, Office of the Secretary, Department of Defense

Michael Neifach  
Former Principal Legal Advisor, Immigration and Customs Enforcement

Dr. Andy Ozment  
Former Assistant Secretary for Cybersecurity, Department of Homeland Security



Philip R. Reitingger  
Former Deputy Under Secretary, National Protection and Programs Directorate, Department of Homeland Security

W. Price Roe  
Former Counselor to the Secretary, Department of Homeland Security

Paul Rosenzweig  
Former Deputy Assistant Secretary for Policy, Department of Homeland Security

Phyllis Schneck  
Former Deputy Under Secretary for Cybersecurity and Communications for the National Protection and Programs Directorate, Department of Homeland Security

Ari Schwartz  
Former Special Assistant to the President and Senior Director for Cybersecurity, National Security Council

Suzanne Spaulding  
Former Under Secretary, National Protection and Programs Directorate, Department of Homeland Security

Chad Sweet  
Former Chief of Staff, Department of Homeland Security

Francis X. Taylor  
Former Under Secretary, Office of Intelligence and Analysis, Department of Homeland Security

Pamela J. Turner  
Former Assistant Secretary for Legislative Affairs, Department of Homeland Security

C. Stewart Verdery, Jr.  
Former Assistant Secretary for Border and Transportation Security Policy and Planning  
Department of Homeland Security

Mark Weatherford  
Former Deputy Under Secretary, National Protection and Programs Directorate, Department of Homeland Security

Honorable Joe D. Whitley  
Former First General Counsel, Department of Homeland Security

Thomas S. Winkowski  
Former Commissioner (Acting), Customs and Border Protection

SECRETARY OF STATE  
STATE OF INDIANA



CONNIE LAWSON  
SECRETARY OF STATE

April 25, 2018

U.S. Senate Homeland Security and Governmental Affairs Committee  
340 Dirksen Senate Office Building  
Washington, DC 20510

Members of the Committee:

I write today to offer my support for Christopher C. Krebs, who has been nominated by President Trump as Under Secretary of Homeland Security for National Protection and Programs.

In his current post, Mr. Krebs has played an integral role in fostering the partnership between states and the Department of Homeland Security. His knowledge, resourcefulness, and insight are invaluable and I am supremely confident of his qualification for this post.

Mr. Krebs brings a wealth of cyber and physical security experience to the table and I am pleased to support his nomination.

Sincerely,

A handwritten signature in cursive script that reads "Connie Lawson".

Connie Lawson  
Indiana Secretary of State



# SECURE COMMUNITY NETWORK

25 BROADWAY, NEW YORK, NEW YORK 10004 | 212.284.6940 | [WWW.SECURECOMMUNITYNETWORK.ORG](http://WWW.SECURECOMMUNITYNETWORK.ORG)

MICHAEL MASTERS  
NATIONAL DIRECTOR | CEO

HAROLD GERNSBACHER  
BOARD CHAIRMAN

February 16, 2018

Honorable Ron Johnson  
Chairman  
Senate Committee on Homeland Security and Governmental Affairs  
340 Dirksen Senate Office Building  
Washington, DC 20510

Honorable Claire McCaskill  
Ranking Member  
Senate Committee on Homeland Security and Governmental Affairs  
340 Dirksen Senate Office Building  
Washington, DC 20510

Dear Senator Johnson and Senator McCaskill:

Please accept this letter of support for the nomination of Mr. Chris Krebs to be Under Secretary of the United States Department of Homeland Security's (DHS) National Protection and Programs Directorate (NPPD), on behalf of the Secure Community Network, the official organization charged with addressing homeland security and safety issues for the American Jewish community, representing 148 Jewish Federations and 300 independent communities across the United States and North America as well as the 50 major national American Jewish organizations.

Since 2004, SCN – on behalf of the Jewish Federations of North America and the Conference of Presidents of Major American Jewish Organizations – has worked with the federal government, and DHS as well as the Federal Bureau of Investigation, in particular, to address threats, undertake assessments, provide training and serve as a resource to the Jewish community. As such, we have developed best practice programs while strengthening the relationships between our community and government.

Through our interactions with Mr. Krebs, it is clear that he is acutely aware of the challenges as well as risks faced by faith-based communities; he has demonstrated strong support to our community on behalf of DHS and the federal government, to include on both a strategic and a programmatic level, as well as –critically – during periods of heightened threat.

The Department's engagement and handling of nearly 150 bomb threats targeting over 100 Jewish community centers and other organizations in early 2017, in which Mr. Krebs was intimately involved, was an impactful recognition of the role of faith-based and community organizations as critical stakeholders, as well as Mr. Krebs' commitment to the same.

Currently leading the DHS effort to enhance security and coordination for soft targets, his inclusion of faith-based organizations as a component of the Administration's effort is a further demonstration of both his leadership as well as his strategic approach to outreach and engagement.

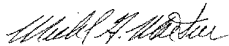
Mr. Krebs has also been a critical leader and leading advocate for ensuring that a priority focus is placed on the convergence of physical and cybersecurity programs, which are inextricably intertwined in today's complex and dynamic threat environment. We are grateful to his leadership, as we work with DHS on a cyber-security related initiative for our community.

Mr. Krebs has been a steady force, reliable advocate and trusted partner within the Department during its transition over the past year who brings unique qualifications to the mission of protecting the Homeland. We are confident that, should Mr. Krebs be confirmed as Under Secretary, he will continue the strong outreach efforts that he has directed, previously. As such, we strongly support his nomination for Under Secretary.

Respectfully,



Harold Gernsbacher  
Chairman of the Board  
Secure Community Network



Michael Masters  
National Director and CEO

Cc: Jerry Silverman  
Chief Executive Officer  
Jewish Federations of North America

Malcolm Hoenlein  
Executive Vice Chairman  
Conference of Presidents of Major American Jewish Organizations