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 expect 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 determines 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 Council (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