Testimony of:

The Honorable Jim Langevin,
The Honorable Mike Gallagher, and
Ms. Suzanne Spaulding

Commissioners of the
Cyber Space Solarium Commission

Before the United States House Committee on Oversight and Reform

"U. S. Cybersecurity Preparedness and H.R. 7331, the National Cyber Director Act"

July 15, 2020

I. INTRODUCTION - INTENT OF THE COMMISSION[1]

The Cyberspace Solarium Commission (CSC) was established in the John S. McCain National Defense Authorization Act for Fiscal Year 2019 to "develop a consensus on a strategic approach to defending the United States in cyberspace against cyberattacks of significant consequences."

The Commission consists of fourteen Commissioners, including four serving legislators, four Executive Branch leaders and six recognized experts with backgrounds in industry, academia, and government service, and Senator Angus King and Representative Mike Gallagher serve as Co-Chairmen. The Commissioners spent the past eleven months studying the issue, investigating solutions, deliberating courses of action, and producing a comprehensive report. The Commission met 30 times as a body, and the staff conducted more than 400 interviews with industry, federal, state and local governments, academia, non-governmental organizations, and international partners. The Commission stress tested its findings and red teamed different policy options in an effort to distill the optimal approach to protecting the United States in cyberspace.

The Commission concluded a strategic approach of layered cyber deterrence will ensure the country can defeat emerging threats in this domain; Commissioners also identified 82 specific policy or legislative actions the Federal government can take to implement the strategic approach. The legislative recommendations were subsequently turned into 54 legislative proposals that have been shared with the appropriate Senate and House committees. The finished report was presented to the public on March 11, 2020.

Throughout this process the Commission always considered the Congress as its “customer”. Through the NDAA, the Congress tasked the Commission to investigate the issue of cyber threats that undermine American power and to determine an appropriate strategic approach to protect the nation in cyberspace and identify policy and legislative solutions that protect the nation in cyberspace. We three Commissioners are here today to tell you what we learned, advocate for our recommendations and work with you to assist in any way we can in reducing the very real risks we face in cyberspace.

A. Overall Focus of Commission Effort

Cyber defense and resilience of the Homeland forms the foundation of the Commission’s strategy. Critical infrastructure - the systems, assets, and entities that underpin our national security, economic security, and public health and safety – is increasingly threatened by malicious cyber actors. Effectively securing critical infrastructure and providing for its resilience

[1] We would like to acknowledge the work of the Commission staff, and particularly our Executive Director, Mark Montgomery, for their tireless efforts over the past year and for their assistance in preparing this testimony.

requires reducing the consequences of its disruption, minimizing its vulnerability, and disrupting adversary operations that seek to hold it at risk.

First and foremost, the Executive Branch must establish a National Cyber Director to centralize and coordinate the cybersecurity mission at the national level. The National Cyber Director would work among Federal departments and agencies to bring coherence in both in the development of cybersecurity policy and strategy and in its execution. The position would provide clear leadership in the White House and signal cybersecurity is an enduring priority in U.S. national security strategy.

Second, the government must continue to improve the resourcing, authorities and organization of the Cybersecurity and Infrastructure Security Agency (CISA) in its role as the primary Federal agency responsible for critical infrastructure protection, security, and resilience. We recommend empowering CISA with greater tools to strengthen public-private partnership, including a Joint Collaborative Environment for real-time information exchange and analysis, an Integrated Cyber Center for person-to-person collaboration, and a Joint Cyber Planning Office for public-private planning that can be rapidly actioned in a crisis. These changes will forge the type of public-private operational collaboration necessary to quickly detect, mitigate, and respond and recover from a significant cyber incident.

Third, the United States must take immediate steps to ensure our critical infrastructure can withstand and quickly respond and recover from a significant cyber incident. Resilience against attack is critical in reducing benefits that our adversaries can expect from their operations - whether disruption, intellectual property theft, or espionage. The Commission recommends codifying Sector-Specific Agencies as Sector Risk Management Agencies and strengthening their ability to aid critical infrastructure sectors in identifying and managing the risks they face. This work will be critical in establishing a Continuity of the Economy Plan, government-wide and public-private contingency planning to rapidly restart our economy after a major disruption. In addition, we recommend establishing a Cyber State of Distress tied to a Cyber Response and Recovery Fund, giving the government greater flexibility to scale up and augment its own capacity to aid the private sector when a significant cyber incident occurs. These changes will ensure the infrastructure that supports our most critical national functions can continue to operate amidst disruption or crisis.

Finally, the Commission recommends two relevant initiatives to reshape the cyber ecosystem. The first, the creation of a National Cybersecurity Certification and Labeling Authority, would help create standards and transparency that, over time, will allow purchasers of technology products and services – whether businesses or consumers - to use the power of their purses and demand more security and less vulnerability in the technologies they buy. The second line of effort, the creation of a Bureau of Cyber Statistics, focuses on collecting better data regarding cyber incidents and deriving insights from those data to improve the security behavior of individuals and organizations, driving down the human vulnerability that pervades the ecosystem. A fully functioning Bureau of Cyber Statistics would help provide private companies, the public, and government policymakers with an empirical evaluation of what does and does

not work in cybersecurity and publish cybersecurity data to allow for further research to inform public policy and cybersecurity investments in the public and private sectors.

II. SPECIFIC RECOMMENDATION FOR A NATIONAL CYBER DIRECTOR

For the past 20 years, commissions, initiatives, studies, and even four Presidential Administrations have been challenged to define and establish an effective national-level mechanism for coordinating cyber strategy, policy, and operations. Emerging technology empowered by stronger and more capable digital networks is being infused into every part of our government, economy, and life. How we navigate the resulting opportunities and challenges will determine the effectiveness of the nation to deal with future cyber-driven, or cyber-enabled, contingencies. It is imperative that the Executive Branch have a strong, stable, and expert-led cyber office and leader within the White House. To fill this gap, our report recommends the creation of a National Cyber Director. Situated within the Executive Office of the President, the Senate-confirmed National Cyber Director would be supported by the Office of the National Cyber Director and fill several important roles:

1. Act as the President's principal advisor on cybersecurity and associated emerging technology issues and lead development of a National Cyber Strategy and associated policies;
2. Ensure the implementation of the National Cyber Strategy across departments and agencies to include the effective integration of interagency efforts, and providing for the review of designated department and agency cybersecurity budgets.
3. Oversee and coordinate Federal government activities to defend against adversary cyber operations inside the United States, to include coordination with private sector and state, local, tribal, and territorial (SLTT) entities;
4. With concurrence from the National Security Advisor or the National Economic Advisor, convene and coordinate Cabinet-level or National Security Council (NSC) Principals Committee–level meetings and associated preparatory meetings.

III. RECOMMENDATION DEVELOPMENT

Looking at the history and the current structure of the Executive Branch, four clear institutional challenges emerge. First, the Federal government lacks consistent, institutionalized leadership in the White House on cybersecurity strategy and policy. Second, due to the absence of a consistent advocate, cybersecurity is inconsistently prioritized in the context of national security. Third, the United States lacks a coordinated, cohesive, and clear strategic vision for cyber.[2] Fourth, the lack of centralized Executive Branch leadership complicates and prevents effective congressional oversight. In the March 2020 Commission report, the Commission recognized the need for a single individual at the highest level in the Federal government to take on these responsibilities. The Commission began by exploring the country's needs in the current dynamic

[2] The Commission's first recommendation is "Issue an Updated National Cyber Strategy" to address precisely this point.

cyber environment and envisioning potential Executive Branch structures to address these needs in preparation for future challenges.

Early in this process, Commissioners identified the need to create a leadership position that would be the strategic focal point to coordinate and execute on national cyber issues. When approaching this issue, the Commission was faced with three key decision points: (1) how to address the gap in national leadership, coordination, and consistent prioritization, (2) whether to recommend Senate confirmation for the coordination and leadership position, and (3) the size, structure, and scope of authorities for the coordinator and leadership office.

On the issue of whether to recommend the creation of new Executive Branch structures, or strengthen the existing structures, the Commission explored several different options. These models included the creation of a new cabinet department for cyber led by a Secretary, an independent agency for cyber led by a Director reporting to an existing cabinet department, an equivalent to a Homeland Security Advisor for cyber within the National Security Council, or a new office within the White House Executive Office of the President (EOP) led by a Director. Ultimately, the Commission decided that the Federal government would be better served by strengthening existing department and agency efforts in cybersecurity, including strengthening CISA and Sector-Specific Agencies, rather than the creation of a new department. While the creation of a new cabinet department or independent agency would give the position gravitas, the Commission recognized the protracted development of a new department would prevent, or even eliminate, much-needed near-term progress.

However, in doing so, the Commission recognized that the current structure, even with strengthened departments and agencies,[3] would still lack institutionalized leadership, coordination, and a consistent advocate for the appropriate prioritization of cybersecurity as a national security issue. With this insight, the Commission deemed the institutionalization of a cyber coordinator position in the White House to be essential. To date, the existence of national cyber leadership has been a matter of Executive Branch policy. The prominence, and attendant influence, of the role has fluctuated across administrations, with some declining, at times, to fill the position at all. These changes have prevented the persistence and consistency needed to establish enduring policy and strategy. The Commission therefore determined the position and office would need a high level of prominence within the EOP to effectively coordinate national strategy and provide much needed leadership internationally, with SLTT organizations, and with the private sector.

With the Commission's decision to recommend creating a National Cyber Director in the EOP, the second decision point was how best to institutionalize the position and ensure cybersecurity and emerging technology are consistent priorities in national security affairs. In contemplating the stature of the position, the Commission determined that requiring the National Cyber Director to be Senate confirmed would not only signal Congress's commitment to cyber issues,

[3] Strengthening CISA in particular is a major emphasis of Commission recommendations 1.4, 3.1, 3.3, 5.2, 5.3, and 5.4.

but also afford them a level of political support that bipartisan endorsement would bring. The position would also ensure that Congress has the ability to conduct comprehensive oversight of cyber and cyber-related issues, which would help address competing and conflicting priorities among Federal departments and agencies and corresponding issues playing out in Congressional committees. Placing the central cyber leadership position within the EOP would mean the individual serves at the discretion of the President, and making the role Senate-confirmed would provide greater permanence by institutionalizing the position's existence and ensuring the role would endure through Presidential transitions. Senate-confirmation of EOP leadership is not without precedent. The heads of the Office of Management and Budget (OMB), the Council of Economic Advisers, the Office of the National Drug Control Policy (ONDCP), the Office of Science and Technology Policy (OSTP), and the Office of the United States Trade Representative (USTR) are all Senate-confirmed. Similarly, having a Senate-confirmed position involved in national-security decision-making is not unique; the Secretary of Defense, the Secretary of Homeland Security, the USTR and others are routinely involved in sensitive discussions with the President on national security affairs, and are able to testify on the Hill without risking violating executive privilege.

The final outstanding decision point for the Commission regarded recommendations on the scope of responsibilities for the National Cyber Director and whether to create an office to support the National Cyber Director. The Commission determined that the National Cyber Director should have a national and strategic focus. That individual should have the ability to ensure strategic coordination of roles and responsibilities and be responsible for assessing performance against the national cyber strategy. To this end, the Director's focus must be on creating and implementing national strategy, which further instilled the Commission's conviction that the National Cyber Director must sit apart from departments and agencies, both of which focus on the day-to-day responsibilities of their given mission set. The scope of responsibilities and characteristics of the leadership position the Commission felt were most important naturally lent themselves to the creation of a new office within the EOP led by a National Cyber Director.

IV. DETAILED RECOMMENDATION

A. The Director's Role as Principal Advisor on Cybersecurity

1. Structure and Size of Office

The National Cyber Director should oversee and manage the Office of the National Cyber Director and be assisted in their duties by two Deputy National Cyber Directors: the Deputy National Cyber Director for Strategy, Capabilities, and Budget and the Deputy National Cyber Director for Plans and Operations. The Commission recommends that the President consider designating an operational position within a department or agency of the Federal government to serve concurrently as the Deputy National Cyber Director for Plans and Operations to enable the National Cyber Director's execution of their responsibilities in the planning and coordination of operational responses. To fulfill the full range of functions and responsibilities envisioned in the recommendation, the Commission recommends the Office of the National Cyber Director be

staffed with approximately 75 to 100 full-time employees,[4] a size similar to that of existing, comparable EOP organizations. It is expected that the National Cyber Director's staff would maintain a significant number of rotating detailees from other Federal departments and agencies to complement a core group of direct-hire, full-time employees of the office. The inclusion of detailees from departments and agencies, besides being a standard practice for other, comparable White House offices, would be critical, as deep cyber expertise and direct, first-hand knowledge of department and agency leadership, personnel, programs, budgeting, and operations would be essential in conducting the full range of the office's responsibilities.

B. Policy and Strategy Development and Coordination

The National Cyber Director should be an Assistant to the President and the primary advisor on issues involving cyber, cybersecurity, federal information security, and associated emerging technologies. As such, the National Cyber Director would be responsible for policy and strategy development relevant to these issues, in coordination with other appropriate offices within the Executive Office of the President, including the National Security Council, the National Economic Council, the Homeland Security Council, and the Office of Science and Technology Policy. To ensure that the National Cyber Director is fully empowered in their ability to advise the President on these issues, and to ensure policymaking fully benefits from the expertise of the National Cyber Director and their staff, the Commission recommends that the National Cyber Director be made a statutory member of the National Security Council. The Director should additionally be empowered to convene National Security Council, Homeland Security Council (if being utilized), and National Economic Council meetings with the concurrence of the National Security Advisor, Homeland Security Advisor, or Director of the National Economic Council, as appropriate.

1. Development and Implementation of the National Cyber Strategy

The development of a National Cyber Strategy would be one of the key responsibilities of the National Cyber Director. The strategy would establish a clear vision, priorities, and objectives to advance the cybersecurity posture of the United States through: improved Federal programs and policies; enhanced integration of Federal departments and agencies; and the establishment of a robust public-private collaboration that reflects private sector and SLTT priorities and concerns. This responsibility and authority are modeled after that granted to the Director of the Office of National Drug Control Policy, who similarly crafts a unified, cohesive national strategy around which department and agency programs, budget, and priorities align. In the development of the National Cyber Strategy and in the policy changes relevant to its implementation, the National Cyber Director should coordinate among all relevant Federal departments and agencies and consult with the private sector and SLTT entities, as appropriate.

A key responsibility of the National Cyber Director is ensuring the effective implementation of the National Cyber Strategy across Federal departments and agencies. The National Cyber

[4] While the Commission's March 2020 report recommended the Office of the National Cyber Director to be staffed by 50 persons, follow-up interviews with various experts consistently and strongly supported increasing the staff number to 75 to 100.

Director would not direct or manage day-to-day implementation of the strategy by any one Federal agency, but instead would be responsible for the overall integration and execution of the strategy across the Executive Branch through policy, operations, and budget. The numerous Federal departments and agencies, with different responsibilities for and interests in securing cyberspace, often compete for resources and authorities, sometimes resulting in efforts that are conflicting or carried out at cross-purposes. The National Cyber Director will be responsible for harmonizing the Executive Branch's policies and efforts in cyberspace and overseeing the implementation of strategy guidance from the President. All of this is done in order to achieve coherence in the planning, resourcing, and employing of government cyber resources to improve the cybersecurity posture of the United States.

2. Coordination with White House Policy Councils on Cyber Issues

If implemented as envisioned, the National Cyber Director's primary responsibility for cyber and associated emerging technology-related policy and strategy development is not expected to limit or constrain the ability of other White House principals, such as the National Security Advisor, Homeland Security Advisor, or the National Economic Advisor, to address similar issues. However, as a statutory member of the National Security Council and as an Assistant to the President, the National Cyber Director would likely participate in Principals Committee meetings with the President where these issues are under consideration. Given this reality, the Commission recommends that White House offices avail themselves of the expertise, participation, and guidance of the National Cyber Director (and their staff) early and throughout their respective policymaking processes for issues within or related to the National Cyber Director's remit. This should serve to reduce uncoordinated, parallel processes that could undermine the overall aim of a unified, cohesive cyber strategy.

3. Participation in Interagency Councils and Committees

Interagency councils and committees play a significant role in implementing the policies, strategies, and priorities of the President, and a number directly relate to or intersect with the purview of the National Cyber Director. To ensure that the National Cyber Director can fully implement the National Cyber Strategy, and to ensure interagency councils and committees fully benefit from the expertise of the National Cyber Director and their staff, the Commission recommends that the National Cyber Director be included as a member in interagency councils and committees that relate to or are within their remit. If the legislation establishing the National Cyber Director is signed into law, the Commission recommends the President invoke their authority to appoint the National Cyber Director to the Committee on Foreign Investment in the United States (CFIUS) and the Federal Acquisition Security Council (FASC). Additionally, the Commission recommends that the Executive Branch update relevant executive orders to include the National Cyber Director as a member in the Federal Chief Information Officer (CIO) Council, the Federal Senior Leadership Council (FSLC), the Equities Review Board (ERB), the National Science and Technology Council (NSTC), the National Infrastructure Advisory Committee (NIAC), and the National Security Telecommunications Advisory Committee (NSTAC).

4. Budget and Oversight Authorities and Responsibilities

While the policy coordination authorities and responsibilities outlined above are sufficient to empower the National Cyber Director in developing a National Cyber Strategy and implementing its relevant policy changes, they alone would have limited effectiveness in driving implementation through department and agency budgetary and programmatic priorities. Additionally, the lack of any oversight authority for performance, programs, and budget would significantly limit the National Cyber Director's ability to negotiate compromises among departments and agencies, forge consensus, and drive the President's agenda. The Commission recommends that the National Cyber Director be granted, in coordination with the Office of Management and Budget, budget and oversight responsibilities in the implementation of a National Cyber Strategy, to include an annual assessment and report to Congress and the President on departments and agencies' implementation of the strategy and its relevant policies and programs.

The National Cyber Director should have the authority to act as a certifier for department and agency budgets. This authority would grant the National Cyber Director the power to review the annual budget proposal for each Federal department or agency and certify to heads of these organizations and the Director of the Office of Management and Budget whether the department or agency proposal is consistent with the National Cyber Strategy. It is expected that the National Cyber Director and the relevant examiners in the Office of Management and Budget would work closely together early and throughout the entire budgetary process to identify inconsistencies, gaps, and redundancies in budget and programs and negotiate a resolution with relevant departments and agencies. Additionally, the Director should have the authority to review department and agency transfer or reprogramming requests to the Office of Management and Budget that would increase or decrease funding for cybersecurity programs, projects, or activities by more than five percent. This authority would allow the Director to ensure transfer and reprogramming actions are also consistent with the National Cyber Strategy.

C. Defensive Cyber Operations Planning, Coordination, and Execution

The National Cyber Director should lead the coordination and integration of U.S. government defensive cyber activities, including Federal government response to significant cyber incidents affecting the U.S. homeland and "defensive cyber campaigns", or whole-of-government efforts designed to deter, defend against, mitigate, or limit the scope of an identified malicious cyber campaign. The National Cyber Director should act primarily as a convening authority in planning and coordinating these operations, ensuring that they are fully integrated, taking full advantage of participating department and agency authorities and capabilities, and reflecting the President's priorities. Day-to-day execution of cybersecurity responsibilities should be carried-out by appropriate Federal departments and agencies, such as CISA, the Federal Bureau of Investigation (FBI), the Department of Defense (DoD), Sector Specific Agencies (SSAs), and others as appropriate. The National Cyber Director is not intended to override or interfere with the authorities and responsibilities of departments and agencies in their cyber missions, but to ensure that they are appropriately and effectively deconflicted, integrated, and mutually-supporting in their approaches and that they receive necessary support in furtherance of broader government-wide efforts. The National Cyber Director should be granted sufficient

latitude to coordinate operational responses, as necessary and appropriate, beyond the scope of previously established plans when required by evolving threats and exigent circumstances. The National Cyber Director should also carry out these responsibilities, to the greatest extent practicable, in coordination with the private sector and SLTT entities.

To ensure the National Cyber Director is fully empowered in their ability to coordinate and integrate government cybersecurity and defensive cyber efforts, the Commission recommends that the National Cyber Director convene and coordinate the Cyber Response Group (CRG) and any Cyber Unified Coordination Groups (Cyber UCGs), the primary mechanisms by which the U.S. government organizes, plans, and coordinates cybersecurity efforts and its response to significant cyber incidents, respectively. Additionally, the Commission recommends that the Executive Branch revisit and amend PPD-41 and any other relevant executive orders to account for the above changes if the legislation establishing the National Cyber Director is signed into law.

1. **Scope of Authority for Planning and Coordination**

The National Cyber Director's scope of authority for planning and coordination should be limited to leading planning for tactical or strategically defensive cyber operations and activities conducted in defense of the homeland, and exclude directing intelligence and offensive operations conducted daily pursuant to collection requirements and warfighting plans. However, the intelligence community agencies and the Department of Defense do undertake defensive cyber activities for the homeland and contribute significantly to whole-of-government cyber efforts to defend the homeland. It is the Commission's recommendation that such activities undertaken by these agencies, to include counter-cyber operations, be included in the National Cyber Director's scope of responsibility for the planning and coordination of defensive cyber campaigns.

2. **Scope of Responsibility for Emergency Response and Disaster Response**

The Department of Homeland Security, and the Homeland Security Advisor, play leading roles in executing and coordinating government responses for emergencies and disasters, with the National Cyber Director playing a subordinate role in these instances. The National Cyber Director would lead the whole-of-government response only in the case of cyber-focused significant cyber incidents. Where emergencies or disasters are a result of a significant cyber incident, or have caused cyber- or cybersecurity-related consequences of their own, the National Cyber Director would support and coordinate with the Department of Homeland Security and the Homeland Security Advisor within the scope of their authorities and responsibilities.

3. **Defensive Cyber Campaign and Operations Planning**

The National Cyber Director should coordinate and set priorities for interagency planning in support of the U.S. government-led response to a significant cyber incident or a defensive cyber campaign. The National Cyber Director should be responsible for establishing consensus on priorities, scenarios, and frameworks around which the interagency shall orient their respective planning efforts. It is expected that the National Cyber Director would convene meetings of the

National Security Council (and appropriate subordinate meetings) as necessary and with the concurrence of the National Security Advisor, to approve planning documents, select courses of action, and plans when a significant cyber incident occurs or an adversary malicious cyber campaign has been identified. The National Cyber Director would focus on developing and coordinating joint, integrated operational plans, processes, and playbooks for defensive cyber operations that: a) feature clear lines of authority and lines of effort across the Federal government, b) feature authorities that have been delegated to an appropriate level to facilitate effective operational responses, c) reflect integration of defensive cyber plans and capabilities with offensive cyber plans and capabilities, as appropriate, and d) reflect integration and understanding of private sector and SLTT capabilities and requirements, as appropriate and necessary.

The National Cyber Director should work in conjunction with and complement another Commission recommendation, the creation of a Joint Cyber Planning Office (JCPO) within the Cybersecurity and Infrastructure Security Agency. The JCPO would be charged with drafting and coordinating plans and playbooks across departments and agencies at the working level under the guidance, processes, and priorities set by the National Cyber Director. The National Cyber Director would ensure that the JCPO receives the buy-in and resources from other relevant departments and agencies necessary to fulfill its mission and carry out its work. The Commission intended for the National Cyber Director to benefit from more robust cyber- and cybersecurity-related planning capabilities within departments and agencies—to include the JCPO. However, in the event these resources do not materialize, or legislation establishing the JCPO is not signed into law, the National Cyber Director would still be expected to play a central role in developing and coordinating plans but would be significantly limited in the breadth and depth of contingencies for which they could reliably account and prepare. The National Cyber Director would also work with all relevant departments and agencies for the preparation, coordination, and execution of interagency cybersecurity tabletop exercises, including national-level table top exercises, in order to exercise and test elements of plans and playbooks and ensure appropriate participation of private sector, SLTT, and international partners.

4. Visibility into Title 10 and Title 50 Cyber Operations

The Commission recommends that the National Cyber Director be kept apprised of cyber-related Title 10 and Title 50 operations to ensure appropriate coordination and deconfliction with defensive activities. Given the complexity of cyber operations, the need for comprehensive situational awareness, and the potential for retaliation in ways that could affect the homeland, the National Cyber Director should be made aware of relevant U.S. operations in order to plan, coordinate, and balance preparatory defensive efforts with such offensive operations. Furthermore, it is expected that, as a constituent member of the National Security Council, the director would participate in any Principals Committee meeting where offensive cyber operations are under consideration and provide recommendations as appropriate.

D. Coordination with the Private Sector and International Partners

The National Cyber Director would be the foremost spokesperson for the U.S. government for cybersecurity and emerging technology issues. As an Assistant to the President and the senior-

most official in the government focused on cyber and cybersecurity, the National Cyber Director would speak with the President's voice and represent the President's priorities in engagement with the general public, the private sector, and the international community. This role does not require the National Cyber Director to be endowed with any special authorities, as those would be intrinsic to the position by virtue of its proximity to the President and stature in White House leadership. The National Cyber Director is not intended to overstep or interfere with the traditional roles played by the State Department, the Department of Defense, the Department of Commerce, the Cybersecurity and Infrastructure Security Agency, the Federal Bureau of Investigation, elements of the Intelligence Community, and others. In any activity where the National Cyber Director engages with the private sector, SLTT leaders, foreign countries, or the general public, it is expected the National Cyber Director would coordinate the efforts of the relevant departments and agencies.

1. Private Sector Engagement and Coordination

The National Cyber Director, and their office, would serve as the principal touchpoint within the White House for engaging senior private sector leadership on cyber, cybersecurity, and related emerging technology issues. CISA would remain the coordination mechanism for continuous cybersecurity-focused private industry interaction with the Federal government. The National Cyber Director would complement and coordinate with CISA in developing and building an effective public-private partnership. The Commission recommends that CISA, and other agencies as applicable, include and coordinate with the National Cyber Director in senior-level meetings of sector coordinating councils, cross-sector coordinating councils, and other meetings of the Critical Infrastructure Partnership Advisory Council. The National Cyber Director would not replace existing agency relationships.

2. International Engagement and Coordination

It is expected that the National Cyber Director, in coordination with the National Security Advisor and the National Economic Advisor as appropriate, would participate in meetings with international allies and partners on topics of cybersecurity and emerging technologies to implement the National Cyber Strategy and advance the President's international priorities. The National Cyber Director would be expected to coordinate closely with relevant offices within the State Department and the National Institute of Standards and Technology at the Department of Commerce in participating in international cyber- and cybersecurity-related initiatives, international agreements, standards-setting bodies, and capacity-building efforts. The Commission recommends that the National Cyber Director be included as a participant in preparations for and, if appropriate, execution of cybersecurity summits and other international meetings at which cybersecurity or related emerging technologies are a major topic.

V. CONCLUSION

The recommendations put forward by the Commission are an important first step to denying adversaries the ability to hold America hostage in cyberspace and will be critical to our efforts to re-establish deterrence in cyberspace. We believe that deterrence is an enduring American strategy, but it must be adapted to address how adversaries leverage new technology and

connectivity to attack the U.S. To achieve this, it is imperative that the Executive Branch have a strong, stable and expert-led cyber office and leader. To fill this gap, the Commission recommended the creation of a National Cyber Director, situated within the Executive Office of the President, who would: act as the President's principal advisor on cybersecurity and associated emerging technology issues and lead development of a National Cyber Strategy and associated policies; ensure the implementation of the strategy across departments and agencies to include the effective integration of interagency efforts, to include the review of cybersecurity budgets; and, oversee and coordinate Federal government activities to defend against adversary cyber operations inside the United States, to include coordination with the private sector and SLTT entities.