QFR Responses of Jamil N. Jaffer[1]
on
U.S. Cybersecurity Preparedness and H.R. 7331, the National Cyber Director Act
before the
Committee on Oversight and Government Reform
of the
United States House of Representatives

July 15, 2020

Responses for Chairwoman Carolyn B. Maloney (D-NY)

---

1. *In your opinion, what are the greatest cybersecurity threats posed by our State and non-State adversaries today, and what changes are needed at the federal level to better prepare America to confront those threats?*

Thank you for the question Chairwoman Maloney. As you know, for the better part of a decade, and certainly more so in recent years, our nation has been involved in a consistent and ongoing series of conflicts in cyberspace. This state of affairs—whether we call it a war or not (and I believe that we are, in fact, at war in the cyber domain)—has undoubtedly had a huge impact on our nation and its allies. For example, it is estimated that the cyber-enabled economic warfare conducted by China—primarily focused on the U.S. private sector—drains private companies of billions of dollars a year, with total damage estimates running well into the trillions of dollars.[2] Likewise, we've seen the significant threat that both nation-state and criminal actors can pose to key critical infrastructure entities, including those in the financial services, healthcare, and energy sectors, as well as in the government.[3]

---

[1] Jamil N. Jaffer currently serves as Founder & Executive Director of the National Security Institute and as an Assistant Professor of Law and Director, National Security Law & Policy Program at the Antonin Scalia Law School at George Mason University and is affiliated with Stanford University's Center for International Security and Cooperation. Mr. Jaffer also serves as Senior Vice President for Strategy, Partnerships & Corporate Development at IronNet Cybersecurity, a startup technology products company headquartered in the Washington, DC metropolitan area. Among other things, Mr. Jaffer previously served as Chief Counsel & Senior Advisor to the Senate Foreign Relations Committee, Senior Counsel to the House Intelligence Committee, Associate Counsel to President George W. Bush, and Counsel to the Assistant Attorney General for National Security in the U.S. Department of Justice. Mr. Jaffer would like to thank Austin Shaffer, Joe Brambil, Suzanne Schultz, Taylor Nelson, and Jessica Jones for their excellent research and editing assistance in preparing these responses. Mr. Jaffer provides these responses to the Committee in his personal and individual capacity and not on behalf of any organization or entity, including but not limited to any current or former employer.

[2] *See* Jamil N. Jaffer, *Prepared Statement on U.S. Cybersecurity Preparedness and H.R. 7331, the National Cyber Director Act* at 2, n. 3, Committee on Oversight and Government Reform, United States House of Representatives (July 15, 2020), *available online at* <https://docs.house.gov/meetings/GO/GO00/20200715/110895/HHRG-116-GO00-Wstate-JafferJ-20200715.pdf>.

[3] *See id*. at 4-6.

One of the key challenges that our nation faces is the core way in which we think about defending the nation in the cyber domain. Historically, our approach to national-level threats, particularly those brought to bear upon us by foreign nation-states, is that the federal government will confront these threats.[4] And yet today, this historic expectation is flipped on its head. In the modern environment, we expect every company in United States to defend itself against attacks of all size and scope, whether conducted by a nation-state, criminal group, or individual actor.[5]

However, there is little question that the government does not provide an effective, comprehensive defense of the nation today. While we have established U.S. Cyber Command, and provided it with some amount resources, we have not provided it with anywhere near the kind of resources or authorities it would take to truly defend the nation, as a whole, in cyberspace. If the nation expects U.S. Cyber Command—or any other entity within the government—to fully take on such a responsibility, the President and Congress have an obligation, working together, to provide it with appropriate resources and authorities to do so. Of course, one of the critical challenges for our political branches in doing so, is that there may not be a consensus today in our nation on what role the government ought have, if any, in defending our overall national cyber infrastructure. Specifically, while there is little question that the government ought defend itself in the cyber domain, there does not yet appear to be agreement—or really even the national conversation necessary to reach agreement—on whether the government ought put in place the intelligence collection and defensive capabilities necessary to protect the whole of the nation in cyberspace, nor even just critical infrastructure sectors.

Likewise, to the extent that we expect the government to take action to deter threat actors in cyberspace, we must provide organizations like U.S. Cyber Command with additional authorities and resources to do so. Congress took strong action to do so in the FY 2019 National Defense Authorization Act[6] alongside reported action by the President in National Security Presidential Memorandum 13.[7] These are important initial steps and have permitted the Department of Defense to "defend forward" and conduct "persistent engagement" abroad, but our nation certainly can and should do more. First, we must encourage and fund more forward-leaning efforts by the government to overtly impose substantive costs on our cyber adversaries for their malign actions in cyberspace. It is only through such clear, public, and attributable action can we possibly expect to effectuate real deterrence in the cyber area.[8]

Second, we must recognize that the current state of affairs leaves the private sector, including those organizations critical to the functioning of our nation and its economy, extremely

---

[4] *Id*. at 7-8 & n. 30.

[5] *Id*. at 8 & n. 32.

[6] See John S. McCain National Defense Authorization Act for Fiscal Year 2019, P.L. 115-232 §§ 1632, 1636, 1642 available online at <https://www.congress.gov/115/plaws/publ232/PLAW-115publ232.pdf>.

[7] *See* Mark Pomerlau, *New Authorities Mean Lots of New Missions at Cyber Command*, Fifth Domain (May 8, 2019), available online at <https://www.fifthdomain.com/dod/cybercom/2019/05/08/new-authorities-mean-lots-of-new-missions-at-cyber-command/>.

[8] *See* Keith B. Alexander and Jamil N. Jaffer, *Iran's Coming Response: Increased Terrorism and Cyber Attacks?*, The Hill (May 15, 2019) ("While some have suggested that deterrence doesn't work in the cyber domain, the reality is that if an attacked party is willing to deliver real consequences and is seen to do so, deterrence can in fact work.")

vulnerable both to nation-state threats, as well as advanced criminal actors, who increasingly have nation-state like capabilities. Given our nation's reliance on cyber-enabled systems to function daily, as well as the fundamentally innovation-focused nature of our new economy, the government must take action to support private sector defensive efforts. Specifically, as the Cyberspace Solarium Commission has recommended, we must work to establish true collective defense in cyberspace.[9] One key step the government ought take immediately in line with this effort would be to begin using our national intelligence collection capabilities to obtain and share with industry actionable cyber threat intelligence about foreign efforts directed at the U.S. private sector.[10] This will require providing significantly more high-level security clearances to organizations and individuals in the private sector, an effort we should ramp up quickly.[11] Finally, the government must not stop at information sharing and creating shared situational awareness, but should take the next step and actively collaborate with the private sector, particularly critical infrastructure entities, to better protect them from significant foreign cyber threats.[12]

2. *H.R. 7331 would enable the National Cyber Director to engage internationally on cybersecurity coordination, specifically by participating in international meetings or conferences on cybersecurity.*

    a. *What agencies, departments, and officials currently represent the U.S. at such events?*

Currently, the United States is represented at such events by a wide range of primary action agencies, including but not limited to: the Department of State's Office of the Coordinator for Cyber Issues; the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA); the Department of Defense's U.S. Cyber Command (USCYBERCOM), National Security Agency (NSA), and the Office of the Deputy Assistant Secretary of Defense for Cyber Policy; the Department of Justice's National Security Division (NSD) and Federal Bureau of Investigation (FBI); and the Office of the Director of National Intelligence (ODNI), to name just a few.

---

[9] *See* Cyberspace Solarium Commission, *Commission Report* (March 2020), at 96, 101-102, *available online at* <https://www.solarium.gov/report> ("The U.S. government and industry … must arrive at a new social contract of shared responsibility to secure the nation in cyberspace….This 'collective defense' in cyberspace requires that the public and private sectors work from a place of truly shared situational awareness and that each leverages its unique comparative advantages for the common defense.…While the U.S. government has taken a number of steps to develop situational awareness in cyberspace, there continue to be significant limitations on its ability to develop a comprehensive picture of the threat…the data or information is not routinely shared or cross-correlated at the speed and scale necessary for rapid detection and identification.")

[10] *See* Jaffer, *Prepared Statement on U.S. Cybersecurity Preparedness*, *supra* n. 2 at 9.

[11] *See* Jenny Menna, Critical Access: *Enhancing the Value of Private Sector Security Clearances to Protect Critical Infrastructure* at 6-10, National Security Institute (Sept. 2019), *available online at* <https://nationalsecurity.gmu.edu/2019/09/menna-critical-access/>.

[12] *See* Jaffer, *Prepared Statement on U.S. Cybersecurity Preparedness*, *supra* n. 2 at 9.

b. *Do you think sending a National Cyber Director to these events on behalf of the United States would be more effective at conveying a cohesive, whole-of-government approach to cybersecurity to our allies and partners?*

Given the wide range of agencies that play a role in the government's offensive and defensive cybersecurity missions, there is every reason to believe that strong, centralized policy leadership in the White House will help accomplish certain cybersecurity goals more quickly than without such a strategic position. Coordination is critical if the government is to achieve unity of any effort. At the same time, there is significant expertise across various parts of the government, including, in particular, at the Department of State when it comes to international relationships in the cyber area. Given this fact, focusing, by statute, the representation of the United States in a single White House official and requiring them to be Senate confirmed, may be unwise. It may be more useful to provide the President with the necessary authority to create such an office and responsibility if he or she chooses to do so, as well as the flexibility to assign certain responsibilities, including lead authority, to another agency, whether that be the State Department or elsewhere.

3. *Do you think establishing a National Cyber Director would signal the seriousness with which we confront the cyber threat to our allies and partners, as well as our adversaries?*

Certainly having a key strategic leader that is well-respected in government and industry and has substantive coordinating (and perhaps, where appropriate, directive) authority at the White House could help signal the seriousness with which we confront cyber threats from our adversaries. At the same time, it is not clear that Senate confirmation of such a position or a massive staff is necessary to establishing such strategic leadership within the White House Office. Indeed, given the likely resistance of any White House to such an effort, creating such a position in statute could potentially have the opposite effect with the President simply choosing not to nominate someone for that position.

4. *Are there any benefits to our national security to not having a statutorily empowered central authority coordinating our nation's whole-of-government cybersecurity operations in the Executive Office of the President?*

There are a number of reasons that Congress may wish to proceed with caution in considering whether it ought statutorily create a new position in the Executive Office of the President, particularly one that is Senate-confirmed, and which may have a significantly large staff and expenditures. First, because of the President's constitutionally assigned role as Commander-in-Chief, Congress has historically seen fit to leave the designation and appointment of senior national security officials in the White House to the sole discretion of the President. This is true from the most senior levels, including the Assistant to the President for National Security Affairs all the way to lower level policy advising staff.

While it is true that a small handful White House officials with responsibilities related to national security are Senate-confirmed and have significantly-sized staff, including the Director of the Office of Management and Budget and the United States Trade Representative, this is generally the exception to the rule, and there are far more core-national security focused leaders

that are appointed by the President at his or her sole discretion. Given the critical national security importance of cybersecurity matters, it may make sense to leave this authority with the principal constitutionally-assigned official, in this case, the President of the United States and permit such an official to report to the President either directly or through the National Security Advisor, as the President sees fit. Such an allocation of authority would reflect historical understandings and would avoid the creation of significant tension between the President and Congress, as well as the potential for mission-creep associated with a large leadership staff footprint inside the White House.

5. *In the hearing, you stated:*

> *"...Today in our country, we expect [large companies and small businesses alike] to defend themselves against nation-states like Russia, China, Iran, [and] North Korea that have virtually unlimited human and monetary resources to throw at this problem. It's an unwinnable battle. We've got to get those companies to come together with one another to create a collective defense structure with multiple industries working with one another, and the Government, frankly, takes all this intelligence it collects and provides it back to industry in an actual form to help them defend themselves. If we're going to put them on the front lines, we owe them better, and we're not doing that right now."*

   a. *Can you provide additional detail on this idea? Should this "collective defense structure" be set up by the federal government, and if so, what form should it take?*

There are two principal ways in which collective defense might effectively work and where Congress could help move the ball forward. First, there is collective defense that takes place purely within the private sector. That is, a defense structure in which companies are sharing threat intelligence at speed and scale with one another both within and across industries and also collaborating in real-time over that threat data. In this space, there are certain things that Congress might do to build on the important work it did in passing the Cybersecurity Information Sharing Act of 2015 (CISA 2015).[13] First, Congress might clear out some of the additional legal barriers to sharing that it had identified during consideration of CISA 2015 and its predecessor legislation, the Cybersecurity Information Sharing and Protection Act of 2012 (CISPA) but which didn't make the final cut.[14] Specifically, Congress might consider expanding the liability protection offered for cyber threat information sharing beyond just the act of sharing itself to the decisions made by companies in receipt of shared information.[15] Such an expansion could serve—perhaps alongside other financial measures, like tax credits for investments in

---

[13] *See* Consolidated Appropriations Act of 2015, P.L. 114-113, 129 Stat. 2242 ("CISA 2015"); *see also* Cybersecurity Information Sharing Act of 2015, S. 754, 114th Cong. (as passed by the Senate on Oct. 27, 2015).

[14] *See* Cyber Intelligence Sharing and Protection Act, H.R. 3523, 112th Cong. (as passed by the House on Apr. 26, 2012) ("CISPA").

[15] *See* Jamil N. Jaffer, *Carrots and Sticks in Cyberspace: Addressing Key Issues in the Cybersecurity Information Sharing Act of 2015*, 67 Univ. S. Car. L. Rev. 585, 595-97 (2016), *available online at* <https://nationalsecurity.gmu.edu/wp-content/uploads/2017/01/Carrots-and-Sticks-in-Cyberspace.pdf>.

cybersecurity information sharing and collaboration effort—to incentivize more robust private-to-private sharing.[16]

Second, there is collective defense that takes place between the government and the private sector. As noted above, this where the government makes an active effort to collect actionable threat intelligence on threats aimed at the private sector, shares that intelligence at speed and scale with the private sector, collaborates in real-time with the private sector over such threat data, and takes action to deter further activities by threat actors, in particular other nation-states. In this portion of the collective defense framework, industry also has a critical role to play, sharing information about threats it is seeing likewise at speed and scale with the government, potentially on a fully anonymized basis. In order to help encourage such sharing, beyond the measures described above for private-to-private sharing which would also promote bidirectional public-to-government sharing, the government might also consider additional measures to promote the latter efforts. Specifically, the government could: (1) bar the use of any information shared by the private sector for any regulatory purposes;[17] (2) shift the burden of minimization away from private actors to the government as it does in other contexts;[18] and (3) certify additional routes for sharing with the government other than the single route authorized in the text of CISA 2015.[19]

In addition, Congress could consider taking up and implementing key recommendations made by the Commission related to collective defense, threat intelligence sharing, and operationalizing cyber collaboration between the public and private sectors, including but not limited to the recommendations that Congress should: (1) establish and fund a joint collaborative environment to share and fuse threat intelligence both within the federal government and between the public and private sectors;[20] (2) establish a joint public-private cyber planning (and operational) organization;[21] (3) institutionalize the role of the Department of Defense in public-private defensive efforts and ensure collaboration between DOD and the information and communications technology sector;[22] (4) strengthen the government's integrated public-private cyber sharing programs;[23] and (5) as needed, clarify authorities related to government intelligence support for the private sector and ensure that such support meets private sector needs and priorities.[24]

---

[16] *Id*.; *see also* Jamil N. Jaffer, *Prepared Statement on Foreign Cyber Threats: Small Business, Big Target* at 12, Committee on Small Business, United States House of Representatives (July 6, 2016), *available online at* <https://nationalsecurity.gmu.edu/foreign-cyber-threats-small-business-big-target/>.

[17] *See* Jamil N. Jaffer, *Carrots and Sticks*, *supra* n. 15 at 594-95

[18] *Id*. at 590-91.

[19] *Id*. at 592-94.

[20] *See* Cyberspace Solarium Commission, *Report of the Cyberspace Solarium Commission*, at 101-103 (Mar. 2020), *available online at* <https://www.solarium.gov/report>.

[21] *Id*. at 107-08

[22] Id. at 109.

[23] *Id*. at 105-07.

[24] *Id.* at 99-100.

b. *How should existing federal agencies fit into this structure, and what new authorities or entities are needed to make it successful?*

As a general matter, large policy decisions on national-level cybersecurity should flow through the normal national security decision making process, including at the highest level through the National Security Council at the White House. At the same time, key operational authority can and should be delegated down as far as reasonably feasible, including to key operations leaders withing DOD, NSA, U.S. Cyber Command, and DHS CISA, to name a few.

Consideration and implementation of the policy recommendations provided above regarding potential modifications to the authorities provided in CISA 2015, as well as the recommendations of the Cyberspace Solarium Commission described above, would be a strong next step in provide the necessary authorities and direction to federal agencies and other organizations playing key roles in national-level cyber defense.

c. *Should this be included in the National Cyber Strategy required by H.R. 7331?*

Absolutely, the concept of collective defense and steps to operationalize it, including but not limited to those described above should be included in the Strategy required by H.R. 7331.

Responses for Ranking Member James Comer (R-KY)

July 15, 2020, Hearing: "U.S. Cybersecurity Preparedness and H.R. 7331, the National Cyber Director Act."

---

1. *Is a Homeland Security Advisor in the White House, tasked by Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, with reporting to the President directly on an assessment of cyber readiness, capable of operating as the primary voice to the President on cybersecurity matters?*

    a. *Could a president restructure this position to do what is envisioned by an NCD?*

    Thank you for the question, Ranking Member Comer. The answer to your question is yes. The President has plenary authority to restructure any position created by an Executive Order and could do so here to ensure that the Homeland Security Advisor has the relevant authority to undertake much, if not all, of the responsibilities that Congress is contemplating providing to the National Cyber Director (NCD). It is this very flexibility that Congress should consider working to preserve to the extent that it seeks to legislate in this area. Specifically, even if Congress chooses to codify an NCD, it could provide the President with the authority to add additional responsibilities to the NCD, as well as to delegate the NCD's statutory authorities to others.

    b. *What authorities would the Cyber Director have over intelligence community and Defense Department led offensive and incident response activities? Would the NCD office be a peer coordinating entity or would it have any actual ability to influence the activities of the nation's intelligence and defense functions?*

    While the Cyberspace Solarium Commission's Report indicates that the NCD "would not direct or manage day-to-day cybersecurity policy or the operations of any one federal agency, but instead will be responsible for the integration of cybersecurity policy and operations across the executive branch,"[25] the proposed statute, including H.R. 7331, is less clear. Specifically, H.R. 7331 provides that the NCD would "lead joint interagency planning for the Federal Government's integrated response to cyberattacks and cyber campaigns of significant consequence," including "coordinating with relevant Federal departments and agencies in the development of, for the approval of the President, joint, integrated operational plans…for incident response that feature…support for the integration…with offensive cyber plans and capabilities…and updating these operational plans…as needed in coordination with ongoing offensive cyber plans and operations."[26] In addition, H.R. 7331 provides that

---

[25] *See* Cyberspace Solarium Commission, *Report of the Cyberspace Solarium Commission*, at 37 (Mar. 2020), *available online at* <https://www.solarium.gov/report>.

[26] *See* H.R. 7331, National Cyber Director Act § 2(D), *available online at* <https://www.congress.gov/bill/116th-congress/house-bill/7331/text?r=7&s=1>.

the NCD would "direct the Federal Government's response to cyberattacks and cyber campaigns of significant consequence, to include…developing for the approval of the President….operational priorities, requirements, and tasks."[27]

These provisions, as written, have the potential to hamper offensive, defensive, and incident response operations of the Defense Department and Intelligence Community that, by their very nature, must be agile and flexible. Congress, of course, can choose to codify such responsibilities but ought be cautious to ensure that the President has the ability to carry out operations consistent with his or her constitutionally authorized role as Commander-in-Chief. This includes the ability to hold operational planning and execution authorities in the White House with a Presidentially-appointed official or to delegate those authorities as far down the line as the President determines is appropriate to ensure operation flexibility and success while maintaining appropriate supervision and oversight.

2. *The National Security Council (NSC) has traditionally operated as the hub for coordinating the nation's cybersecurity response. Should Congress instead be supporting the NSC in this mission rather than splintering the authorities of the NSC yet again, following removal of various mission areas like drug coordination and trade coordination from its ambit?*

   Yes. Congress should support the role of the National Security Council as the primary hub for the coordination of cybersecurity response from a policy perspective. Operational decisions, as a general matter, should be delegated to the relevant operational components with specific operations being elevated to the NSC process in appropriate circumstances, including but not limited to when such operations raise novel policy or legal questions or when there is expected to be significant national security or foreign policy consequences to a given operation.

3. *President Trump recently signed an executive order declaring foreign threats to the nation's energy infrastructure a national emergency. Under the executive order, the Secretary of Energy will lead a task force to ensure that power systems are protected against foreign intrusion and attack. The Secretary of Defense, Secretary of Homeland Security and the Director of National Intelligence will also be members of the task force.*

   a. *Is this task force model potentially a better way of dealing with sector-specific cyber threats rather than a specified individual who is expected to handle such a diverse range of cyber threats?*

      Certainly a task force like the one established by the President to address energy sector threats is a reasonable approach to handle a sector-specific set of cyber threats confronting the nation, particularly given that it is likely to be focused on some key operational decisions to best protect the energy critical infrastructure systems and given that it involves the participation of nearly all of the key agencies. Likewise,

[27] *Id*. at § 2(E).

assigning a single individual to handle all manner of cyber threats at an operational level from the White House may present a significant challenge given the diverse range of threats as well ensuring appropriate operational direction to as the various organizations involved. That being said, there is a significant benefit to policy coordination and direction from the White House, and at times in specific circumstances, even operational leadership from the top. As a result, having a strong, well-qualified individual in a senior position in the White House office to handle such cyber related issues is critical. Such a position could provide the necessary leadership to guide the operational activities contemplated by future task forces that parallel the energy infrastructure task force.

b. *What other federal agencies would need a seat at such a task force and why?*

The agencies covered by the Executive Order, which include the Departments of Defense, Homeland Security, Commerce, Interior, and the Office of the Director of National Intelligence and the Office of Management and Budget, are all relevant to this effort.[28] Other agencies that ought be considered for inclusion are the Departments of Justice, Treasury, and State, given their particularly important roles in national-level cybersecurity matters.

4. *The Foreign Intelligence Surveillance Act (FISA) authorizes DOJ to seek orders to surveil individuals acting as agents of foreign powers.*

a. *Is FISA a tool for investigating foreign cyber intrusions?*

Yes. Given the role that foreign powers, including nation-states, play in threating our public and private systems in cyberspace, including critical infrastructure, the Foreign Intelligence Surveillance Act of 1978, as amended (FISA), can and does play a critically important role in investigating foreign cyber intrusions and more.

Keeping FISA vibrant and strong protects our nation and its people in myriad ways, including by obtaining highly valuable intelligence against some of the most important threats to American national security, including those related to terrorism, cyber attacks, foreign spying, and our broader national security and foreign policy priorities.

Having served in the Justice Department's National Security Division during the Bush Administration, and having worked on high priority intelligence collection matters before the FISA, including those related to terrorism and cyber threats, I can assure the members of the Committee that there are few more important intelligence collection authorities for our national security than those provided in FISA.

[28] *See* The White House, *Executive Order on Securing the United States Bulk-Power System* (May 1, 2020), *available online at* <https://www.whitehouse.gov/presidential-actions/executive-order-securing-united-states-bulk-power-system/>.

b. *Are there gaps in FISA which, if filled, would assist investigators and prosecutors in combatting foreign cyber-attacks?*

Yes. The continuing expiration of key portions of FISA, as amended to better protect our nation and its citizens in the aftermath of the September 11, 2001 terrorist attacks, presents a significant, ongoing danger to our nation. The authorities that are no longer available to the federal government, including the roving wiretap authority, are important not only to counterterrorism matters but also to certain cyber investigations as well. Leaving these authorities expired for even one week—and it has now been many, many months—makes our nation significantly less safe, as it requires federal national security officials to rely on existing authorizations that may be inflexible and will eventually be unusable, as well as to rely on laws as they existed before the September 11 attacks.

In my view, leaving these provisions expired is unconscionable and puts the nation and our people at significant risk, including with respect to certain threats in the cyber arena. Congress should consider taking action to reauthorize these authorities as soon as possible.

In addition, other modifications to FISA might be made to clarify the authorities of the government to collect and rapidly disseminate actionable threat intelligence, including highly classified information, as appropriate, to key parts of the private sector, including critical infrastructure organizations and those that support them.

5. *Why shouldn't we take more time to study this matter and further evaluate the need for creation of a new office, something the Senate companion legislation ponders?*

Certainly Congress could take more time to study the question whether a National Cyber Director is needed in the White House Office and, if so, whether that position must be Senate-confirmed and have scores of staff assigned to it. At the same time, there is certainly value in strong, centralized policy leadership in the White House that can help accomplish certain cybersecurity goals. This can be achieved through direct Presidential appointments, as has historically been the case for the White House Office, or Congress could choose to play or more directive role, whether now or after further consideration. Of course, if and when Congress does choose to act, Congress could consider whether requiring Senate confirmation is a critical core component or whether it is more important to provide a future President with flexibility to restructure the role as needed to address a rapidly evolving cybersecurity environment. The Committee may also wish to consider whether it is important to ensure that the staff component of any such office is kept to a fiscally prudent size.