Testimony of the National Cyber Director

J. Chris Inglis,

United States Senate

Committee on Homeland Security and Governmental Affairs

September 23, 2021

Chairman Peters, Ranking Member Portman, distinguished members of the Committee, and your staff – thank you for the privilege to appear before you today, and the honor to appear alongside Director Easterly and Mr. DeRusha. I am eager to update you on the Biden-Harris Administration's progress in standing up the new Office of the National Cyber Director and discuss the Administration's approach to cybersecurity. The President's commitment to cybersecurity as a matter of national security is evident both by the positions he has created and appointments he has made, as well as the unmatched speed with which the Administration has acted to modernize our defenses and bolster our security in nine short months.

But first, I wanted to recognize the history of this particular moment. I am appearing before you as the first National Cyber Director, a position that you created just last year, and then confirmed me for following my nomination by President Biden. I am grateful for the confidence that the President and Congress have placed in me in this role, as well as for the cybersecurity and critical infrastructure resilience investments that you are endeavoring to make in in the proposed Infrastructure Investment and Jobs Act and elsewhere. I remain committed to engaging with you as we take on these critical, shared imperatives.

To that end, I am pleased to tell you that our new office is making progress in standing up as a full-fledged contributor in those imperatives. Cyber talent is in high demand everywhere, but I will continue working with Congress to secure the resources we need to bring on key staff. While we continue to work with the Office of Management and Budget (OMB) and Congress on funding amounts, organizational planning, and timelines, we are determining how our office and limited team can begin helping the Administration confront the critical challenges facing us.

And as the ONCD organizes for that purpose, I see those responsibilities falling into a few major areas of emphasis to bolster the President's cybersecurity agenda:

- Informing and helping develop policy and strategy around cybersecurity, technology supply chains, and, the resilience of the cyber ecosystem across the people, processes, and technology that constitute cyberspace.
- Ensuring accountability and follow-through on implementation and providing recommendations on agency investments in cybersecurity to ensure they align with national strategy and priorities;
- Engaging with the private sector and our international partners, in collaboration with the rest of government, to find opportunities for greater integration and collaboration;
- Coordinating with OMB and the Cybersecurity Infrastructure Security Agency (CISA) on security and resilience of the Federal civilian network enterprise; and,
- Ensuring defense cyber operations and planning have the policies, plans, procedures, and coordination mechanisms necessary to be successful.

None of this work occurs in a vacuum, and much of the credit for progress in developing these themes and in the work of putting them into practice must go to my partners at the National Security Council, my colleagues sitting alongside me – Director Easterly and Mr. DeRusha – and many others serving in the Federal cyber ecosystem.

Cyberspace is attractive to our adversaries and frustrating to our allies because of how difficult it is for any one country or entity to have the benefit of a complete picture of actions and actors across the shared spaces of cyberspace. Cyberspace allows a global reach and efficiency of scale unrivaled in any other domain, meaning that our geopolitical competitors can have global reach and strategic effect and criminals and extremists can have wield an unprecedented level of impact and coercion. Malign actors big and small often believe they can evade consequence for acts and crimes that in most other realms would provoke swift and severe responses.

The complexities of holding actors accountable applies not only to malign actors, but also to our friends and partners. This is true in both the positive and negative sense; across the public and private sectors alike, there are rarely clear lines defining what it means to "do the right thing" when preparing or responding to a cyber incident. And the reward for success can be even more elusive, as it is hard to quantify and even harder to celebrate an attack avoided. Conversely, the consequences for failing to take appropriate security steps are not always clear, even for those who knew (or should have known) how to secure their systems and who had the

resources to do so, yet still chose not to do it. We have the good fortune of having two domestic agencies at the forefront of cyber incident preparation and response—CISA and FBI—whose roles complement one another and who, working together, strengthen our defense of cyberspace in ways that could not happen if they were in competition or isolation. The more we can support these agencies' synchronized efforts and partnerships, with each other and the private sector, the greater the return on our investment will be for the American people.

These are just some of the challenges that President Biden sought to address in Executive Order 14028, Improving the Nation's Cybersecurity (signed May 12, 2021). The President took bold, aggressive action to transform Federal government cybersecurity for the better, and through that, to improve the security of critical infrastructure for all Americans. Since the President signed the Order, OMB, CISA, NIST, and others in the interagency have worked tirelessly to ensure its successful implementation. This includes developing contracting requirements, implementation guidance, cybersecurity expectations, information sharing improvements, and incident notification. Our hope is that the federal government's purchasing power is great enough that these requirements will echo throughout industry, even outside of direct contractual relationships with the government.

The President has also taken aggressive action to secure the Nation's Critical Infrastructure. His Industrial Control Systems Cybersecurity Initiative has already driven improvements in the electricity and pipeline subsectors and will soon expand to other areas. And on July 28, he signed a National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems, which among other things directed CISA and NIST to develop performance goals for critical infrastructure cybersecurity. Director Easterly can give you more details about the terrific progress CISA and NIST have made in this area.

Steps like these are critical to ensuring that critical infrastructure owners, whether public or private sector, implement necessary security measures and become more accountable for their responsibility to the broader economic and digital ecosystem in which they reside. The importance of this dynamic has been reinforced by recent ransomware attacks against critical infrastructure entities. The Colonial Pipeline attack was a stark illustration of how the increasingly digitized nature of every part of our commercial ecosystem can create cascading, physical consequences. We hope that seeing this real-world example will catalyze stakeholders

across the public and private sectors to implement security controls commensurate with the importance of their operations.

The Office of the National Cyber Director will build on this momentum, fill in gaps and seams in the government's current approach, and bring a unique perspective and direction by focusing on the following priorities:

- First, the Office will champion coherence across the Federal cyber enterprise – from coordinating with NIST in standards and guideline development, supporting CISA in providing operational support to federal agencies, and working in partnership with OMB to resource these key cybersecurity initiatives. That means ensuring that we are speaking with one voice and moving in the same direction, particularly in areas like common standards and guidelines in hardware and software, in propagating best practices, acting with unity of purpose and effort in the actual defense of our digital infrastructure, and ensuring that the good work Sector Risk Management Agencies are doing is not only improving their respective sectors, but also adding value across the Federal enterprise.
- Second, the Office will highlight the importance of improving public-private collaboration. We will work closely with Director Easterly and Mr. DeRusha and seek to expand engagement and partnership across this sectoral line to new level – because tackling the cyber challenges we face requires nothing less. The new Joint Cyber Defense Collaborative, hosted by CISA and leveraging authorities, capabilities, and talents of the federal cyber ecosystem in partnership with industry, can play an important role in this effort, and I look forward to working with the JCDC and other associated initiatives across the Federal government.
- Third, we will ensure that the US government is aligning their resources to their aspirations and accounting for the execution of cyber resources entrusted to their care. We are in close discussions with OMB on how best to exercise the National Cyber Director's budget review and recommendations authority to identify investments that are not being made or those that are not quite singing from the same general sheet of Federal music.
- Finally, the Office will work to increase present and future resilience, not only within the Federal government, but also across the American digital ecosystem. That is a big task for which we will start by exercising our incident response and planning processes, and

we hope to soon be working to ensure our workforce, or technologies, and our very structures and organizations are not only fit for purpose today, but are future-proofed for tomorrow.

These are daunting undertakings, but with the support of this Congress, we are excited to undertake them.

Finally, I'd like to draw the Committee's attention to our cyber workforce. Your investment in education, training, and workforce programs like the National Initiative for Cybersecurity Education at NIST, CyberCorps: Scholarship for Service, and the special hiring authorities afforded to the Department of Defense and CISA have made very real progress in ensuring the U.S. Government can attract and retain the talent it needs. In the months and years ahead, we will need to ensure that all portions of the Federal government that have a strong, central role in our collective cyber defense also benefit from the best recruitment and retention tools we have to offer. The ultimate purpose should be to create a shared, interoperable community of interest that operates with unity of effort and unity of purpose across the U.S. Government.

These are all important undertakings. The Office of the National Cyber Director is a young and still small office, but once funding is in place and with the partners we have today, and with the confidence and support of this Congress, it will be in a strong position to succeed. Thank you for the opportunity to testify before you today, and I look forward to your questions.