Testimony of the National Cyber Director

J. Chris Inglis,

United States House of Representatives

Committee on Homeland Security

November 3, 2021

Chairman Thompson, Ranking Member Katko, 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. I am eager to update you on the Biden-Harris Administration's progress in standing up the new Office of the National Cyber Director (ONCD) and to 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 created and appointments he made, as well as the unmatched speed with which the Administration continues to act to modernize our defenses and bolster our security in eleven 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 (NCD), a position the Congress 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 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 as a full-fledged leader in those imperatives. On Thursday, October 28, I released the NCD's first *Strategic Intent Statement*, which outlines at a high level the strategic approach and scope of work I expect my office to undertake. At the same time, I announced the designation of Chris DeRusha as a Deputy National Cyber Director for Federal Cybersecurity, a dual-hatted title he will hold along with his current role as Federal Chief Information Security Officer, creating unity of effort and unity of purpose in our shared mission to ensure the security of Federal networks. Both of these announcements lay the groundwork for the ONCD's approach but are certainly not the sum total of our endeavors. We will continue to build out our leadership team and our strategic intent will soon be followed by a more concrete, comprehensive description of our priorities and strategic objectives that will guide our work for years to come.

While we will continue working with Congress to secure the resources we need to bring on key staff, I am pleased to inform the Committee that we have built a robust pipeline of talent and expect to reach a total of 25 personnel on board by the end of December. Additionally, with limited funds from the President's Unanticipated Needs Fund, we have procured an office suite for the Office of the National Cyber Director at the 716 Jackson Place Townhome within the White House complex. I would emphasize, however, that without appropriations, we remain limited in our ability to hire key staff members, make necessary procurement and acquisitions, and find permanent office space for our future, full complement of staff. More fundamentally, the lack of appropriations inhibits our ability to plan and delays our ability to quickly and fully realize the role of the NCD.

As I have testified previously to the Senate Homeland Security and Government Affairs Committee, the ONCD looks to four key outcomes as its benchmark of success. Given the foundations these priorities establish for ONCD accountability, I will comment on them here.

- First, the ONCD will drive coherence across the Federal cyber enterprise – from coordinating with NIST in standards and guideline development, harmonizing our approach to supply-chain risk management, supporting the Cybersecurity and Infrastructure Security Agency (CISA) in providing operational support to federal agencies, and working in partnership with OMB to resource these key cybersecurity initiatives. This means ensuring that the government is speaking with one voice, moving in the same direction, and, to the greatest extent practicable, sharing common priorities by which we can organize our collective efforts for maximum possible effect. Acting with unity of purpose and effort in the defense of our digital infrastructure is an absolute imperative.
- Second, the ONCD will ensure the continued improvement of public-private collaboration in cybersecurity. We will work closely with Director Easterly, CISA , the National Institute of Standards and Technology (NIST), and Sector Risk Management Agencies and seek to expand engagement and partnership across sectoral lines to new levels – because tackling the cyber challenges we face demands nothing less. The new Joint Cyber Defense Collaborative (JCDC), hosted by CISA and leveraging authorities, capabilities, and talents of the federal cyber ecosystem in partnership with industry, will

play an important role in this effort, and I look forward to working with the JCDC and other associated initiatives to ensure synergy across the Federal government.

- Third, we will ensure that the US government is aligning our cyber resources to our aspirations and accounting for the execution of cyber resources entrusted to our 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 warrant an increase and those that may not be having the intended impact or effect. The ONCD intends to work with and through OMB in assessing and evaluating the performance of these investments and advising departments and agencies on recommended changes and updates in alignment with Administration priorities.
- Finally, the Office will work to increase present and future resilience of technology, people, and doctrine, not only within the Federal government, but also across the American digital ecosystem. We expect to do this by identifying common, emerging priorities in partnership with relevant departments and agencies and planning strategic, government-wide initiatives to address them. 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, technologies, and our structures and organizations are not only fit for purpose today, but are prepared for the challenges of tomorrow.

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 colleague sitting alongside me – Director Easterly – and many others serving in the Federal cyber ecosystem.

Attempting to subvert this cyber ecosystem 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 its shared spaces. Cyberspace allows a reach and efficiency of scale unrivaled in any other domain, meaning that our geopolitical competitors can have global reach and strategic effect; criminals and malicious actors can wield an unprecedented level of influence, impact, and coercion.

The general strategic imperatives emerging in response to these threats includes ensuring our digital infrastructure is resilient by design, proactively defended by collaborative coalitions, and backstopped by a doctrine that delivers benefits for good behavior and costs for bad. For the

Committee's consideration, I submit there are three categories of threat that are systemic, enduring, and globally diffuse in nature and warrant continued effort and attention.

- First is the vulnerability of our software supply chains. As we saw with the SolarWinds intrusion, sophisticated malicious actors are exploiting security and quality control seams among software service providers and software development pipelines, affording those actors the ability to rapidly "scale up" the reach and depth of their malicious activities across our digital ecosystem.
- Second is the pervasive vulnerability of the products and devices that enable opportunistic cyber attacks typified by ransomware actors and more sophisticated actors alike. Poor security practices, insecure design, short-sighted approaches to doctrine, and a lack of cyber talent among the workforce remain widespread, even in the face of known flaws, shortcomings, and vulnerabilities. Propagating best practices – including enforcing accountability for those who do not adhere to those practices – will be critical to righting the ship.
- Finally, we must remain laser-focused on maintaining the integrity of our information and telecommunications infrastructure against high-risk actors. Large portions of the hardware supply chain underpinning our most critical such technologies are located in countries that could leverage it for intelligence gathering or disruption at global scale.

These threats are serious and are receiving urgent and aggressive attention from the Biden-Harris Administration. The Administration is also, however, looking beyond these immediate threats and toward how to shape the future of cyberspace so that such threats are systemically blunted or mitigated. This requires not only a thorough understanding of the nature of the threats, but also a clear vision for our digital ecosystem and what we want that ecosystem to achieve. With such a vision , we can pursue the fundamental, systemic changes necessary to realize the digital future in which we want to live. Such changes require *clarity of accountability* and *depth of collaboration*.

Accountability must flow in both positive and negative directions. It is rarely clear what it means to "do the right thing" when preparing or responding to a cyber incident, and harder yet to celebrate the benefits of 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. A key priority for the ONCD will be examining roles and responsibilities between the public and private sectors so as to make the required clarity of responsibility more actionable. It is an oft-cited statistic that 85% of our critical infrastructure is owned and operated by the private sector, and that privately-owned critical infrastructure is increasingly core to the government's imperative to protect and provide for national security. Shared defense is not a choice, but an imperative.

Incorporating these lessons into a modern social contract will also require us to consider which stakeholders in the digital ecosystem should be held accountable for what magnitude of responsibilities. As I articulated in our office's first *Strategic Intent Statement*, the complexity of our challenges in cyberspace has too often resulted in responsibility for systemic cyber risk being devolved onto the smallest, least-sophisticated actors: individuals, small businesses, and local governments. The potential consequences of one key individual's password being compromised are simply too grave; tools like multifactor authentication are a critical means to stanch the bleeding, but are not in and of themselves a systemic remedy. It is unreasonable to ask everyday Americans to maintain constant digital vigilance without also looking to key stakeholders to shoulder a greater share of this ecosystem-wide burden, especially those firms charged with operating and securing our information and communications systems and networks. How and where this burden reallocation should happen will be one of our preeminent objectives.

To achieve these and other objectives, it is clear that more routine and explicit statements of priorities and guidance on a year-to-year basis will support Departments and Agencies in their efforts to set their own planning and operational priorities. The Federal government undertakes a vast array of actions and programs to support and defend the private sector in cyberspace; ensuring coherence across these lines of effort will be key in ensuring these initiatives are always mutually supporting and never redundant. Realizing this unity of effort and unity of purpose will continue to be a core guiding principle in all that we do. We have the good fortune of having a number of capable agencies at the forefront of securing and defending cyberspace—CISA, FBI, Department of Defense, the National Security Agency, Department of Energy, and NIST, among others—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.

The Biden-Harris Administration has already made progress in addressing these issues and countering the threats we face in cyberspace -- most recently during last month's thirty-nation summit on ransomware. On May 12, 2021, President Biden issued Executive Order 14028, Improving the Nation's Cybersecurity, taking 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 requirements. Our expectation is that the federal government's purchasing power is great enough that the requirements in the Executive Order will drive improvements 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. 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 this real-world example will catalyze stakeholders across the public and private sectors to implement security controls commensurate with the importance of their operations.

These are daunting undertakings, and overcoming them will require realizing a digital ecosystem that is resilient by design, a policy and commercial environment that aligns actions to consequences, and ensuring public and private sectors are postured to proactively, decisively collaborate. Although the Office of the National Cyber Director is a young and still small office, we have made significant progress, and are building robust relationships with our interagency partners. When funding is in place, and with the continued confidence and support of this Congress, ONCD will be in a strong position to lead in enhancing the security and resilience of our Nation's cyber ecosystem. Thank you for the opportunity to testify before you today, and I look forward to your questions.