Testimony of Kemba E. Walden

Acting National Cyber Director

United States House of Representatives

Committee on Oversight and Accountability

Subcommittee on Cybersecurity, Information Technology, and Government Innovation

Unpacking the White House National Cybersecurity Strategy

March 23, 2023

Washington, D.C.

Chairwoman Mace, Ranking Member Connolly, and distinguished members of the Subcommittee, thank you for the privilege to appear before you today to discuss the Biden-Harris Administration's National Cybersecurity Strategy. I am eager to share with you how the President's strategy will make our digital ecosystem more secure and resilient. The work of this Subcommittee is critical because cybersecurity is essential to the basic functioning of our everyday lives. It is central to our economy, the operation of our critical infrastructure, our national defense, the strength of our democracy and democratic institutions, an innovative future, and the privacy of our data and communications.

An Evolving Strategic Environment

The urgency of the threats we face in cyberspace is real. The world is entering a new phase of deepening digital dependencies. Driven by emerging technologies and ever more complex and interdependent systems, dramatic shifts in the coming decade will unlock new possibilities for human flourishing and prosperity, but also multiply the systemic risks posed by unsecure systems. Too often, we are layering new functionality and technology onto already brittle and intricate systems at the expense of security and resilience. Next-generation interconnectivity is collapsing the boundary between the digital and physical worlds, and

exposing some of our most essential systems to disruption. Today, an attack on one organization, sector, or state can rapidly spill over to other sectors and regions.

Malicious cyber activity has evolved from nuisance defacement to espionage and intellectual property theft, damaging attacks against critical infrastructure, ransomware attacks and cyber-enabled influence campaigns designed to undermine public trust in the foundation of our democracy. The governments of China, Russia, Iran, North Korea, and other autocratic states with hostile intent are aggressively using advanced cyber capabilities to pursue objectives that harm U.S. interests and global peace and security. Their disruptive and destabilizing cyberspace behavior is threatening both U.S. national security and economic prosperity.

Emerging technologies like artificial intelligence, machine learning (AI/ML) and quantum computing are poised to upend the technology landscape and may give malicious actors enhanced capabilities unless we take proactive steps today. While the full implications of these technologies are not yet known, it is clear that they have the potential to significantly impact cyberspace. We must raise our defenses promptly and proactively advance our interests in this domain, instead of belatedly reacting to our adversaries.

A New Strategic Approach

The President's National Cybersecurity Strategy calls for changes to the underlying dynamics of the digital ecosystem, shifting the advantage to its defenders and persistently frustrating the forces that would threaten it. The President's vision is a defensible, resilient digital ecosystem where it is costlier to attack systems than defend them, where sensitive or private information is secure and protected, and where neither incidents nor errors cascade into catastrophic, systemic consequences. In creating these conditions, we can and must seize the opportunity to instill America's values. To achieve this outcome, the strategy calls for two fundamental shifts in how the United States allocates roles, responsibilities, and resources in cyberspace.

First, the most capable and best-positioned actors in cyberspace must be better stewards of the digital ecosystem. Today, end users bear too great a burden for mitigating cybersecurity risks. Individuals, small businesses, local governments, and even many critical infrastructure

operators have limited cyber expertise and resources. Yet, these actors' choices can have a significant impact on our national cybersecurity. Across both the public and private sectors, we must expect more of the most capable and best-positioned actors to make our digital ecosystem secure and resilient. In a free and interconnected society, protecting data and assuring the reliability of critical systems must be the responsibility not only of the owners and operators of the systems that hold our data and make our society function, but also of the technology providers that build and service these systems.

Second, our economy and society must incentivize activity that makes cyberspace more resilient and defensible over the long term. Protecting the systems we have now, while investing in and building toward a future digital ecosystem that is more inherently defensible and resilient are both priorities. The strategy outlines how the Federal Government will use all tools available to reshape incentives and achieve unity of effort in a collaborative, equitable, and mutually beneficial manner. We must ensure that market forces and public programs alike reward security and resilience, build a robust cyber workforce that draws from all parts of our society, embrace security and resilience by design, coordinate research and development investments in cybersecurity strategically, and promote the collaborative stewardship of our digital ecosystem with our allies and partners.

To achieve the President's vision for cyberspace, the strategy lays out objectives organized around five pillars:

Pillar 1: Defend Critical Infrastructure

Defending the systems and assets that constitute our critical infrastructure is vital to our national security, public safety, and economic prosperity. The American people must have confidence in the availability and resilience of this infrastructure and the essential services it provides. We aim to operationalize an enduring and effective model of collaborative defense that equitably distributes risk and responsibility, and delivers a foundational level of security and resilience for our digital ecosystem.

Collaboration to address advanced threats will be effective only if owners and operators of critical infrastructure have cybersecurity protections in place to make it harder for adversaries to disrupt them. This Administration is committed to constructing consistent regulatory frameworks for cybersecurity tailored for each sector's risk profile, and harmonized to reduce duplication complementary to public-private collaboration and cognizant of the cost of implementation. In the last two years, the Administration has made significant progress in this area, establishing new cybersecurity requirements in key sectors such as oil and natural gas pipelines, aviation, rail, and water.

We must build new and innovative capabilities that allow owners and operators of critical infrastructure, Federal agencies, product vendors and service providers, and other stakeholders to effectively collaborate with each other at speed and scale. Federal agencies that support critical infrastructure providers must enhance their own capabilities and their ability to collaborate with other Federal entities. When incidents occur, Federal response efforts must be coordinated and tightly integrated with private sector and State, local, Tribal, and territorial (SLTT) partners. Following major incidents, we will also ensure that the cybersecurity community benefits from lessons learned through the Cyber Safety Review Board (CSRB). The Board's public-private review will generate insights and provide recommendations for improving the Nation's cybersecurity posture.

Additionally, the Federal Government can better support the defense of critical infrastructure by making its own systems more defensible and resilient. This Administration is committed to improving Federal cybersecurity through long-term efforts to implement its Zero Trust Architecture (ZTA) Strategy and modernize both information technology and operational technology infrastructure. In doing so, Federal cybersecurity can be a model for critical infrastructure across the United States for how to successfully build and operate secure and resilient systems. As this Subcommittee understands well, replacing legacy systems with more secure technology, including through accelerating migration to secure cloud-based services, will improve the cybersecurity posture of agencies across the Federal Government, and in turn, improve the security and resilience of the digital services it provides to the American people.

Among the strategic objectives in this pillar is 1.3: Integrating Federal Cybersecurity Centers. Federal Cybersecurity Centers serve as collaborative nodes that fuse together whole-of-

government capabilities across homeland defense, law enforcement, intelligence, diplomatic, economic, and military missions, including to protect critical infrastructure. The strategy commits the Administration to better integrating the centers and new collaboration initiatives like Cybersecurity and Infrastructure Security Agency's (CISA) Joint Cyber Defense Collaborative (JCDC) and the National Security Agency's Cybersecurity Collaboration Center. Leveraging these centers will allow the government to better coordinate defensive and disruptive operations while providing opportunities to enable timely, actionable, and relevant information sharing directly with private sector partners. My office, the Office of the National Cyber Director (ONCD), will lead the Administration's effort to enhance the integration of these centers, identify gaps in capabilities, and develop an implementation plan to enable collaboration at speed and scale.

Pillar 2: Disrupt and Dismantle Threat Actors

The United States will use all instruments of national power to disrupt and dismantle threat actors whose actions threaten our interests. These efforts may integrate diplomatic, information, military (both kinetic and cyber), financial, intelligence, and law enforcement capabilities. Our goal is to make malicious actors incapable of mounting sustained cyber-enabled campaigns that would threaten the national security or public safety of the United States.

Coordinated efforts by Federal and non-Federal entities have proven effective in frustrating the malicious cyber activity of foreign government, criminal, and other threat actors. The Federal Government has increased its capacity to respond to cybersecurity incidents; arrested and successfully prosecuted transnational cybercriminals and state-sponsored actors; imposed sanctions on malicious cyber actors, including bans on travel and denying access to the U.S. financial system; and deprived threat actors of access to digital infrastructure and victim networks. The Federal Government has also targeted financial infrastructure used for illicit activity; established new diplomatic initiatives attributing disruptive, destructive, or otherwise destabilizing cyber activities to hold actors accountable for their malicious behavior; and recovered billions of dollars' worth of ill-gotten assets.

We will build upon these successes to enable more sustained and effective disruption of adversaries. Our efforts will require greater collaboration by public and private sector partners to improve intelligence sharing, execute disruption campaigns at scale, deny adversaries use of U.S.-based infrastructure, and thwart global ransomware campaigns.

Among the strategic objectives in this pillar is 2.5: Counter Cybercrime, Defeat Ransomware. Ransomware is a threat to national security, public safety, and economic prosperity. The Administration sees ransomware as a threat to national security, not just a criminal justice issue and is committed to bringing all elements of national power to confront the threat and working with international partners to do the same. The Joint Ransomware Task Force, co-chaired by CISA and the Federal Bureau of Investigation (FBI) and chartered as part of the Cyber Incident Reporting for Critical Infrastructure Act, will coordinate, deconflict, and synchronize agency efforts to disrupt ransomware operations and provide support to SLTT and private sector partners to protect against ransomware. We will also continue our efforts to prevent criminals from profiting from their nefarious deeds by continuing to sanction malign actors, including illicit cryptocurrency operations, and by supporting international partners to implement anti-money laundering efforts countering the financing of terrorism controls, know-your-customer requirements, for cryptocurrency and related service providers.

Pillar 3: Shape Market Forces to Drive Security and Resilience

To build the secure and resilient future Americans want, we must shape market forces to place responsibility on those within our digital ecosystem that are best positioned to reduce risk. That requires shifting the consequences of poor cybersecurity away from the most vulnerable so that our digital ecosystem is more worthy of trust. In this effort, we will channel market forces productively toward keeping our country resilient and secure. Our goal is a modern digital economy that promotes practices that enhance the security and resilience of our digital ecosystem, while preserving innovation and competition.

Continued disruptions of critical infrastructure and thefts of personal data make clear that market forces alone have not been enough to drive broad adoption of best practices in cybersecurity and resilience. In too many cases, organizations that choose not to invest in

cybersecurity negatively and unfairly impact those that do, often disproportionately affecting small businesses and our most vulnerable communities. While market forces remain the first, best route to agile and effective innovation, they have not adequately mobilized industry to prioritize our core economic and national security interests.

To address these challenges, the Administration will shape the long-term security and resilience of the digital ecosystem, against both today's threats and tomorrow's challenges. We will use Federal purchasing power and grant-making to incentivize security. We will explore how the government can stabilize insurance markets against catastrophic risk to drive better cybersecurity practices and to provide market certainty when catastrophic events do occur.

Among the Strategic Objectives in this pillar is 3.4: Use Federal Grants and Other Incentives to Build in Security. Federal grant programs offer strategic opportunities to make investments in critical infrastructure that are designed, developed, fielded, and maintained with cybersecurity and all-hazards resilience in mind. Through programs funded by the Bipartisan Infrastructure Law, the Inflation Reduction Act, the CHIPS and Science Act, and the State and Local Cybersecurity Grant Program, the Administration will collaborate with SLTT entities, the private sector, and other partners to balance cybersecurity requirements for applicants with technical assistance and other forms of support.

Pillar 4: Invest in a Resilient Future

A durable and flourishing digital future begins with investments made today. We can build a more secure, resilient, privacy-preserving, and equitable digital ecosystem through strategic investments and coordinated, collaborative action. In doing so, the United States will maintain its leading role as the world's foremost innovator in secure next-generation technologies and infrastructure.

Foundational elements of our digital ecosystem, like the Internet, are products of sustained and mutually-supporting investments by both public and private sector entities. However, public and private investments in cybersecurity have long trailed the threats and challenges we face. As we build a new generation of digital infrastructure, from next-generation telecommunications and Internet of Things (IoT) to distributed energy resources, and prepare for

revolutionary changes in our technology landscape brought by artificial intelligence and quantum computing, the need to address this investment gap has grown more urgent.

Decades of adversaries and malicious actors weaponizing our technology and innovation against us—to steal our intellectual property, interfere in or influence our electoral process, and undercut our national defenses—has demonstrated that leadership in innovation without security is not enough. We will complement our efforts to out-innovate other countries with focused, coordinated action to optimize critical and emerging technologies for cybersecurity as they are developed and deployed.

Among the Strategic Objectives in this pillar is 4.6: Develop a National Strategy to Strengthen Our Cyber Workforce. We must make the investments in people necessary to realize a future digital ecosystem that is secure, resilient, and furthers American prosperity and national security. To that end, ONCD is currently developing a national cyber workforce and education strategy. The workforce and education strategy will recognize that the dynamism of our technological environment will place ever-changing demands on our cyber workforce. The workforce and education strategy also must address concerns that the American people have that the jobs of today will be erased by technology – our future success requires good-paying jobs and building an economy from the bottom up and the middle out, while ensuring that we have the best and brightest – from all walks of life – contributing to our collective defense. The United States has a tremendous opportunity to engage, employ, and develop a more inclusive and diverse workforce in good jobs that enable workers to thrive and their communities to prosper. We will take a whole-of-nation approach to create a strong and diverse cyber workforce and fully address cyber training and education to ensure we are not only opening career pathways to fill hundreds of thousands of openings for cybersecurity jobs, but also equipping and upskilling everyone with knowledge to secure their own digital lives while contributing to systemic cybersecurity.

Pillar 5: Forge International Partnerships to Pursue Shared Goals

The United States seeks a world where responsible state behavior in cyberspace is expected and rewarded and where irresponsible behavior is isolating and costly. To achieve this

goal, we will continue to engage with countries working in opposition to our larger agenda on common problems while we build a broad coalition of nations working to maintain an open, free, global, interoperable, reliable, and secure Internet.

For decades, we have worked through international institutions to define and advance responsible state behavior in cyberspace. We have used multilateral processes such as the United Nations (UN) Group of Governmental Experts and Open-Ended Working Group to develop a framework that includes a set of peacetime norms and confidence-building measures, which all UN member states have affirmed in the UN General Assembly. We have supported the expansion of the Budapest Convention on Cybercrime and other global efforts to make cyberspace more secure. We will continue these efforts while recognizing the need to work with partners to thwart the dark vision for the future of the Internet that the People's Republic of China and other autocratic governments promote. We will do so by demonstrating to economies and societies the value of openness and by jointly imposing consequences for behavior that runs counter to agreed norms of state behavior.

To counter common threats, preserve and reinforce global Internet freedom, protect against transnational digital repression, and build toward a shared digital ecosystem that is more inherently resilient and defensible, the United States will work to scale the emerging model of collaboration by national cybersecurity stakeholders to cooperate with the international community. We will expand coalitions, collaboratively disrupt transnational criminals and other malicious cyber actors, build the capacity of our international allies and partners, reinforce the applicability of existing international law to state behavior in cyberspace, uphold globally accepted and voluntary norms of responsible state behavior in peacetime, and punish those that engage in disruptive, destructive, or destabilizing malicious cyber activity.

Among the Strategic Objectives in this pillar is 5.3: Expand U.S. Ability to Assist Allies and Partners. As recent cyberattacks against Costa Rica, Albania, and Montenegro have demonstrated, allies and partners who fall victim to a significant cyberattack may seek support from the United States. The Administration will establish policies for determining when it is in the national interest to provide such support, develop mechanisms for identifying and deploying department and agency resources in such efforts, and, where needed, rapidly seek to remove existing financial and procedural barriers to provide such operational support.

Implementation

The strategic objectives outlined in the strategy will require a strong focus on implementation. In implementing the strategy, the Federal Government will take a data-driven approach and will measure investments made, progress, and the outcomes and effectiveness of these efforts. The Federal Government will lead by ensuring that its networks have implemented security measures. Implementation of the strategy will involve close collaboration with Congress, interagency partners, and the broader cybersecurity community to ensure accountability, secure needed resources and new authorities where necessary, and continuously evaluate our performance and opportunities to integrate lessons learned. The Administration looks forward to engaging with public and private stakeholders on the implementation of the strategy and efforts are already underway to put the strategy into action. The ONCD, in coordination with the National Security Council staff, Office of Management and Budget, and departments and agencies, will assess the effectiveness of the strategy and report annually to the President and Congress on the effectiveness of the strategy, associated policies, and follow-on actions in achieving its goals.

Strategy Development Process

It is important to address briefly how the strategy developed. Last year, ONCD led a highly collaborative drafting process for a new National Cybersecurity Strategy. Throughout that process, ONCD engaged extensively with interagency partners, Congress and non-Federal stakeholders, including representatives from civil society, academia, industry, and the international community. The strategy, importantly, also built on the work of several prior administrations and strategies including the 2018 National Cyber Strategy and 2016 Cybersecurity National Action Plan.

The strategy was developed alongside the Biden-Harris Administration's National Security Strategy and National Defense Strategy by a broad interagency team and through a months-long consultation process with the private sector and civil society. It is informed by and implements the values of the Declaration for the Future of the Internet, the Freedom Online Coalition, and other long-standing efforts to realize a democratic vision for our digital

ecosystem. It carries forward the foundational direction of Executive Order (EO) 14028, "Improving the Nation's Cybersecurity," National Security Memorandum (NSM) 5, "Improving Cybersecurity for Critical Infrastructure Control Systems," NSM 8, "Improving the Cybersecurity of National Security, Department of Defense (DoD), and Intelligence Community Systems," and other executive actions.

The robust, collaborative, and iterative development process ensured that the strategy was not created in a vacuum, and the resulting final product is both one that a broad array of stakeholders can see their contributions in and one that reflects the President's clear vision for America in this decisive decade—committing to creating a more equitable economy for all Americans, rebuilding our national infrastructure, strengthening our democracy, accelerating our clean energy transition, and making the nation's workforce more competitive. The success of each of these initiatives depends on the willful contributions of all of us, and is enhanced by a secure and resilient cyberspace.

Conclusion

The President's strategy lays out how the United States is prepared to meet the challenges in cyberspace from a position of strength, leading in lockstep with our closest allies, and working with partners everywhere who share our vision for a brighter digital future. Thank you for the opportunity to testify before you today, and I look forward to your questions.

*****END*****