United States Senate

COMMITTEE ON COMMERCE, SCIENCE,
AND TRANSPORTATION

WASHINGTON, DC 20510–6125

WEBSITE: https://commerce.senate.gov

July 28, 2021

The Honorable Gina Raimondo
Secretary
Department of Commerce
1401 Constitution Avenue NW
Washington, DC 20230

Dear Madam Secretary,

As a world leader in the digital economy, the United States—including its economic and national security—depends on secure and consistent access to information systems. Digital and connected technologies support individual and institutional financial transactions, enable critical infrastructure, underlie the navigation and communications systems in our vehicles and our phones, and provide Americans with direct access to their government. These digital systems convey significant amounts of data, including personally identifiable information and proprietary information, making their protection crucial to security and privacy. The nation's reliance on cyber-enabled systems demands that the Department of Commerce (DOC), including the National Institute of Standards and Technology (NIST), deepen its critical role in protecting the nation from cybersecurity threats and vulnerabilities with funding that matches the seriousness of the threat. The President's Budget Request to level-fund NIST cybersecurity programs, while requesting significant increases across the agency, is insufficient to meet the need.

Reliance on cyber-enabled systems provides an attractive target for U.S. adversaries and cybercriminals. Separate threat assessments by the Director of National Intelligence and the Department of Homeland Security ranked cyberattacks as an acute threat to government at all levels as well as to the private sector. Recent events highlight these risks and the importance of cybersecurity risk management. The SolarWinds attack, which infiltrated systems at multiple government agencies, exploited vulnerabilities in the software development supply chain. Ransomware attacks—which have this year impacted U.S. beef production and fuel distribution—have increased by an estimated 300% this year, with the ongoing Kayesa attack affecting up to 1,500 businesses worldwide. As reemphasized at a Senate Commerce, Science, and Transportation Committee hearing this week, a ransomware attack on Colonial Pipeline, one of the nation's largest pipeline operators, led to gas shortages and panic buying in Washington D.C. and the Southeast United States. This attack not only impacted passenger drivers and freight haulers, but also threatened airlines and mass transit.

The Administration has correctly called for action, with the Department of Homeland Security issuing new requirements for U.S. pipeline operators and the Department of Justice moving to identify foreign hackers. DOC must also be part of the solution, given its already significant

responsibilities. In September 2020, the U.S. Government Accountability Office identified the DOC as the lead agency for 49 of the 191 activities outlined in the 2018 National Cyber Strategy, more than any other federal agency. Among these activities, the NIST cybersecurity and privacy frameworks support the adoption of standards and best practices by industry, academia, and government institutions. In addition, NIST's National Initiative for Cybersecurity Education supports universities, major corporations, the federal government, and others to develop the cybersecurity workforce of the future.

Recent actions by the Administration and Congress, including legislation led by the Senate Commerce Committee, have further entrusted DOC with high-priority cybersecurity initiatives. In January, the Fiscal Year (FY) 2021 National Defense Authorization Act (NDAA) (P.L. 116-283) directed DOC to grow the cybersecurity workforce and to hold cybersecurity-relevant prize competitions. In May, the President's Executive Order (E.O.) on Improving the Nation's Cybersecurity (E.O. 14028) directed NIST to publish software supply chain security guidelines and take other actions to make the nation more cybersecure. In June, the Senate passed the United States Innovation and Competition Act (S. 1260), which would require DOC to address supply chain resiliency; offset small manufacturers' cybersecurity protection costs via the Manufacturing Extension Partnership; help universities improve their cyber posture to promote research security; and incentivize domestic semiconductor manufacturing, which could support the availability of secure hardware.

Given these emerging responsibilities, we were encouraged by your commitment to build on NIST cybersecurity efforts, as expressed during your confirmation process before the Senate Commerce Committee. We urge you to take swift action on this important work and to ensure that the full range of NIST cybersecurity activities is appropriately resourced, with a particular focus on the following areas:

(1) **Developing the Cybersecurity Workforce**. As of 2019, there were 300,000 unfilled cybersecurity jobs in the United States. DOC should swiftly and fully implement the cybersecurity workforce provisions from the HACKED Act, which passed as part of the FY 2021 NDAA after careful consideration within our committee. The HACKED Act directed DOC to carry out the Regional Alliances and Multistakeholder Partnerships to Stimulate (RAMPS) program, an effort to attract and retain cybersecurity personnel through cooperation between educational institutions and industry. DOC should also continue its existing cybersecurity workforce activities performed via the National Initiative for Cybersecurity Education.

(2) **Demonstrating New and Existing Cyber Capabilities**. DOC should swiftly and fully implement the cybersecurity prize competitions directed by the CYBER LEAP Act, passed in FY 2021 NDAA after careful consideration within our committee. These challenges will demonstrate the potential for systems that make cyberattacks economically unattractive, improve federal agency response to cyberattacks, and increase the privacy, security, and safety on individuals while online. DOC should also continue to support the National Cybersecurity Center of Excellence—a public-private partnership to create practical cybersecurity solutions.

(3) **Ensuring Resilient Supply Chains.** Consistent with the E.O. 14028, DOC should continue addressing cybersecurity supply chain risk, including by updating and, as appropriate, encouraging the adoption of software supply chain best practices. Actions should include a prompt update to NIST Special Publication 800-161, *Cyber Supply Chain Risk Management Practices for Systems and Organizations*, and continued work on advancing trustworthy networks and infrastructure, including zero trust architectures. Further, DOC should leverage its supply chain resilience activities—such as the sectoral reviews under E.O. 14017, the new supply chain task force, and the semiconductor incentives under the FY 2021 NDAA, as appropriate—to promote the availability of measurably secure hardware and software.

(4) **Addressing Emerging Technology.** DOC should leverage its significant research experience to address the cybersecurity challenges and opportunities from emerging technologies such as artificial intelligence, quantum technology, advanced communications, and the Internet of Things. DOC should continue to support research within the Applied Cybersecurity Division, the Computer Science Division, and the Information Technology Laboratory, while expanding research in emerging areas, including interdisciplinary research and research between offices, to better prepare the United States for the effects of these technologies.

Cybersecurity threats are growing and evolving, so the federal response must do so as well. To ensure the safety and security of the American people and economy, DOC and NIST must be part of the solution. We appreciate your shared interest in this critical mission.

Sincerely,

Maria Cantwell
Chair

Roger F. Wicker
Ranking Member