March 5, 2025

The Honorable Howard Lutnick
Secretary
U.S. Department of Commerce
1401 Constitution Ave., NW
Washington, DC 20230

Re: Strengthening Cybersecurity: The Need for Sustained Support for the National Institute of Standards and Technology's (NIST) Cybersecurity Mission

Dear Secretary Lutnick,

As the US Government seeks opportunities to identify cost savings and efficiencies, the undersigned organizations urge you to protect and prioritize support for NIST's cybersecurity mission. With escalating cybersecurity activity – particularly from the People's Republic of China (PRC), which continues to actively target U.S. critical infrastructure – it is imperative that we safeguard our nation's ability to counter these advanced persistent threats. In addition, we must push back against burdensome international regulatory approaches to cybersecurity, which hamper innovation and undermine U.S. competitiveness. NIST's work is critical to meeting both of these objectives.

The undersigned organizations submit this letter on behalf of our member companies, who represent a broad cross-section of American industry, and support millions of American jobs. Collectively, these companies underpin our nation's private sector efforts to identify, protect, detect, respond, and recover from cyber-attacks by our adversaries.

NIST plays a crucial role in developing cybersecurity standards, guidelines, best practices, and other resources based on internationally recognized standards to support U.S. industry, federal agencies, and the broader public. Its research spans across critical areas including secure communications, artificial intelligence, cryptography, bioscience, electronics, energy, environment, public safety, and transportation, providing U.S. agencies and organizations with both immediate, actionable guidance and long-term research to address emerging threats and technological advancements.

Among NIST's most impactful resources is the Cybersecurity Framework 2.0 (CSF), which helps organizations assess, prioritize, and communicate their cybersecurity efforts without prescribing specific controls. Instead, it connects users to additional resources that provide guidance on best practices to tailor to their specific risk environment. The CSF's widespread adoption—translated

into seven languages and used globally—demonstrates its significance. It is a prime example of American leadership in cyber policy development.

Other key NIST initiatives include the Privacy Framework, the Risk Management Framework, and the NICE Workforce Framework for Cybersecurity, all of which contribute to strengthening cybersecurity resilience across sectors. Furthermore, NIST's leadership on post-quantum cryptography is crucial for national security and forms the foundation to protect against future threats. NIST's critical role in advancing cybersecurity and technological innovation has earned high praise from leaders across government. We were pleased to see you describe NIST as a "central hub of knowledge of the American government" in your Senate confirmation hearing, and emphasize that "the way we've done cybersecurity is the gold standard of the world."

NIST is widely recognized for its strong public-private engagement, actively seeking feedback from industry partners to ensure its resources remain relevant and effective. A key example of NIST's collaborative approach is the National Cybersecurity Center of Excellence (NCCoE), which serves as a hub where industry, government, and academia work together to tackle pressing cybersecurity challenges. By leveraging commercially available solutions based on industry standards, the NCCoE provides practical guidance that strengthens cybersecurity across sectors. NIST also plays a critical role in advancing priority areas such as cryptography, education and workforce development, emerging technologies, risk management, identity and access management, measurements, privacy, and the development of trustworthy networks and platforms.

NIST also fulfills critical cybersecurity responsibilities outlined in federal statutes, executive orders, and policies, including the development of cybersecurity standards and guidelines for federal agencies. It is tasked with enhancing accountability for software and cloud service providers, securing federal communications and identity management systems, and advancing innovative cybersecurity technologies. NIST plays a direct role in operationalizing transparency and security in third-party software supply chains, strengthening federal communications, combating cybercrime and fraud, and promoting security in artificial intelligence. As the government continues to entrust NIST with these critical responsibilities, it is essential that the agency receives the necessary budgetary resources to effectively execute its mission.

In an era of growing cyber threats and evolving technological challenges, NIST's work is more critical than ever. As the government seeks to cut costs and improve efficiency, it is essential to safeguard the agency's ability to fulfill its mission – one that directly impacts national security. NIST's personnel are highly effective and respected within industry, bringing invaluable expertise to the development of cybersecurity standards and research. Without sustained funding, the

agency risks losing its top talent, which would put its ability to provide essential cybersecurity guidance, research, and standards at risk.

We urge you to prioritize NIST's budgetary support and empower its employees to continue its mission: strengthening the nation's cybersecurity resilience, protecting critical infrastructure, and promoting the American approach to cyber policy around the world.

Sincerely,

Better Identity Coalition
Coalition to Reduce Cyber Risk (CR2)
Cyber Risk Institute (CRI)
Cyber Threat Alliance (CTA)
Cyberspace Solarium Commission 2.0
Information Technology Industry Council (ITI)
Partner Nation Cybersecurity Coalition (PNCC)
Telecommunications Industry Association (TIA)