April 12, 2021

The Honorable Alejandro Mayorkas
Secretary of Homeland Security
Department of Homeland Security
300 7th St., SW
Washington, DC 20024

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

Dear Secretary Mayorkas and Secretary Raimondo:

The undersigned associations congratulate you on your confirmations and welcome the opportunity to work with you on the critical challenges and opportunities facing the information communications technology ("ICT") sector. Chief among these are global efforts to enhance the security of the ICT ecosystem and maintain U.S. private sector leadership in international standards development. The undersigned organizations are deeply committed to partnering with the government and look forward to helping you pursue these goals. The ICT sector has engaged across federal agencies to promote a consistent approach to supply chain risk management (SCRM). In 2020, the ICT sector intensified its efforts across multiple workstreams to address challenges related to the COVID-19 pandemic.

Of critical importance now is maintaining the United States' longstanding commitment to industry-led technical standards and best practices to address cybersecurity, supply chain, and other global challenges. Such standards are a bedrock of federal trade, technology, and security policy, so it is imperative that your respective Departments champion them. The federal government should not attempt to create its own technical demands, nor should it try to supplant private sector leadership in standards bodies.

In the wake of recently revealed, widespread compromises through software vectors like SolarWinds, government and industry face a renewed call to arms to address threats from foreign adversaries. The government has a vital interest in preventing suppliers that pose a national security threat from exploiting U.S. networks or undermining critical functions. However, policymakers should reconsider which tools are best suited to address particular aspects of this challenge and which kinds of approaches will deliver optimal security outcomes. Some recent policies deserve special review.

For example, we recognize the Administration's view that national security emergencies may warrant the use of extraordinary measures like the previous administration's Executive Order 13873, "Securing the Information and Communications Technology and Services Supply Chain," however, such actions should be more tailored. In the long term, the nation is best served by pragmatic approaches that are designed to address specific risks.

Critically, the United States should prioritize and champion industry-led standards and best practices that raise the bar for security across the ecosystem, increasing the cost of supply chain attacks for bad actors, and encouraging forward-thinking security risk management. Such consensus-based standards are developed by myriad organizations in the technology sector. The United States government can and does play an important role in third party standards development, and appropriate agencies should continue to be an active convener and supporter of these venues. Voluntary and transparent standards can promote much needed international cybersecurity norms, enable more effective communication across stakeholders sharing the security responsibility, and create incentives for companies to innovate and adopt security technologies that are more adaptable to the evolving nature of cybersecurity threats.

As the Biden/Harris Administration takes the reins and embarks on its review of these issues, we urge the Administration to take a close look at the full spectrum of legal and policy tools available to address threats facing U.S. networks. In refining the recently released Interim Final Rules that implement aspects of E.O. 13873, the Department of Commerce has an opportunity to undertake a more effective approach to supply chain security. In doing so, Commerce should leverage the DHS and private sector-led ICT Supply Chain Risk Management Task force as the key mechanism for public-private collaboration, tailor intervention actions to where they are most necessary, and place greater focus on industry-led standards and best practices that provide a positive model for nations working to build a secure, resilient, and innovative connected ecosystem now and in the future.

We look forward to ongoing collaboration on these issues and welcome the opportunity to discuss this important issue in further detail with you or your staff.

Sincerely,

CCA
CTA
CTIA
ITI
NAB
NTCA
TIA
USTelecom
WIA