Supply Chain Security:
Principles for a Strategic Review

The tech sector shares policymakers' concerns regarding threats to global ICT supply chains, which implicate not only cybersecurity, national security and economic security policy objectives but also U.S. competitiveness. Over the past several years, however, uncoordinated approaches by the U.S. federal government to ICT supply chain risk management have resulted in a patchwork of overlapping, inconsistent and, in some cases, conflicting measures, including Executive Orders, agency actions, regulations and legislation. The net result has been a confusing supply chain security policy terrain that is increasingly difficult for companies to navigate, and which in many respects has not achieved the intended goal of improved supply chain security across the U.S. federal enterprise, critical infrastructure, and global private sector ICT supply chains. Perhaps the most notable example of a well-intentioned supply chain policy measure that is not carefully calibrated to both address supply chain security risks and minimize broad, unintended commercial and economic impacts is the *Executive Order on Securing the ICTS Supply Chain* (ICTS EO) and subsequent Commerce Department rulemakings.

The change in administrations offers the opportunity for a strategic review of U.S. supply chain security policy, consistent with the holistic assessment of the ICT supply chain called for by the new *Executive Order on America's Supply Chains.* As evidenced by the inventory developed by the soon-to-be published ICT Supply Chain Risk Management Task Force, there are upwards of 30 supply chain security measures currently being contemplated and/or in force. Therefore, as a departure point, we encourage the Biden Administration to **undertake a strategic review of ICT supply chain security policy as part of the assessment called for by the new EO to develop a more coherent, streamlined and effective long-term approach**. In doing so, the Administration should consider how to address legitimate national security issues in a *coordinated* and *holistic* manner. Short-term, piecemeal approaches should be avoided. Below, we offer our perspective on best practices to inform and develop a more coherent, streamlined and strategic approach to supply chain security policy.

- ✔ **To ensure the development of a coherent supply chain security policy, the U.S. Government should designate a lead supply chain security risk management agency and empower the National Cyber Director to coordinate these efforts,** as ITI referenced in our Competitiveness Agenda[1]. Doing so will help to avoid duplication of efforts and help ensure that efforts to address both federal and commercial supply chain security risks are complementary.

- ✔ **Approaches to supply chain security must be risk- based and evidence-driven, and facilitate transparency and predictability for private actors to the greatest extent possible.** The approach to supply chain security over the last several years has primarily focused on country-of-origin, particularly China, which has led to an over-reliance on this attribute and short-circuited the risk analysis. While country-of-origin is one risk factor, it should not be the sole and dispositive factor animating U.S. supply chain policy for all technologies. It is noteworthy that the ICT SCRM Task Force working group on Threat Assessment catalogued a total of 188 supplier-related threats, with country of origin being just one. A successful supply chain security strategy must widen the aperture to consider a full array of relevant threats and address identifiable, material, concrete national security risks directly tied to actionable threats articulated in U.S. government intelligence or vulnerability assessments.

- **The U.S. government should leverage the existing ICT Supply Chain Risk Management Task Force as a focal point for public-private collaboration on supply chain security.** Policymakers should work with Task Force leadership to develop a strategic plan to establish long-term support for the Task Force as a venue to co-develop solutions with industry to the nation's most pressing supply chain security challenges, including to establish the Task Force as a coordination point for ICT supply chain input pursuant to the new EO. The Task Force has brought together subject matter experts from the private sector and from across the U.S. government and has produced several actionable tools and other work products that can be used by industry and government to address supply chain security challenges, including related to information-sharing, threat modeling, procurement, and vendor attestation. Addressing supply chain security threats requires a holistic approach and the Administration should look first to this established public-private mechanism for creative, actionable solutions, and should prioritize implementing and operationalizing Task Force products across the U.S. government and incentivizing their promotion and uptake across the critical infrastructure community.

- **The U.S. government should view supply chain risk management through the lens of trustworthiness, which has many dimensions.** We urge the U.S. government, in conjunction with industry, to continue to work to develop consistent criteria that would assist in evaluating the risk-level that transactions, suppliers, or other activities may pose. The Task Force has done a significant amount of work already to develop such criteria, which should include both technical and non-technical considerations, be grounded in industry-driven, consensus-based international standards, including the ISO 9000 series, take into account the geopolitical implications of manufacturing locations, localization and sourcing requirements, government interference where the rule of law and effective judicial redress are not present, responsible corporate behavior and existing legal protections, and the criticality of the component to the security and continuity of the supply chain. Another important facet to consider is the availiability of alternate sources, including domestic availability, of critical goods and assessing the costs and benefits of shifting suppliers.

- **Bi-directional information-sharing should also be a key tenet in any supply chain security approach.** Increased information-sharing regarding risks related to suppliers and other aspects of the ICT supply chain can help both the government and the ICT industry to identify and mitigate supply chain risks. Currently, companies face challenges in sharing supplier risk information. This includes the legal risk of sharing potentially derogatory information about a supplier, the administrative barriers for federal personnel to share detailed, actionable information with individuals who don't hold clearances, and instances where the Federal government withholds vulnerability disclosures for offensive purposes.[2] The Task Force is currently working on developing a legislative proposal that would provide liability protections for companies that share threat information in good faith. In considering a comprehensive approach to supply chain security, we urge the Administration to design an approach to information-sharing that improves the flow and uptake of information about risks, threats, and vulnerabilities. It is worth leveraging and sharing exclusionary decisions made by the Federal Acquisition Security Council in this context as well.

- **Any measures that the U.S. government designs should be used to advance and protect U.S. national security objectives without putting American competitiveness at risk.** Lack of clarity in scope and process in any rulemaking, legislation, or other policy mechanism makes for an uncertain business environment and threatens the ability of companies to compete with foreign companies not subject to U.S. or similar foreign conditions. Overbroad policy approaches or approaches that duplicate or conflict with existing mechansims, such as those embodied in the ICTS EO, stifle U.S. innovation, technological leadership, and competitiveness. U.S. policymakers should seize the opportunity to advance supply chain security policy approaches that are not only compatible with but drive global policymaking norms. Any approach should focus on addressing acute national security risks to the United States and *should not* be used to advance trade or economic policy goals.

[1] *https://www.itic.org/advocacy/us-competitiveness-agenda*
[2] *https://www.cisa.gov/sites/default/files/publications/ict-scrm-task-force-threat-scenarios-report_0.pdf*