

Critical Infrastructure Colleagues and Partners

Today, the [Cybersecurity and Infrastructure Security Agency \(CISA\)](#) and government and industry members of the Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force released an analysis report on the impact of COVID-19 on global supply chains. *Building A More Resilient ICT Supply Chain: Lessons Learned During The COVID-19 Pandemic* examines how ICT supply chains have been logistically impacted by the pandemic and provides practical recommendations to increase supply chain resiliency from future risks.

The COVID-19 global pandemic caused profound disruptions to global supply chains, including those in the Information Technology (IT) and Communication sectors. In an effort to understand and document the disruptions, the Task Force formed the COVID-19 Impact Study Working Group which studied how key supply chain operational areas, such as inventory management, supply chain mapping/transparency, and supply chain diversity, were impacted by the shocks of the pandemic.

Findings from the group identified three major stress points on ICT supply chains during the pandemic. It exposed how some manufacturing companies were unprepared because of their reliance on lean inventory models. It underscored the difficulties that companies faced in understanding who their junior tier suppliers are and where they are located. It also acknowledged the need for an approach that was already underway over the last six years: diversifying supply chains to a broader array of locations and away from single source/single region suppliers. Recommendations from the study include refining supply-chain risk-management approaches, mapping out detailed supply chains and developing standardized approaches to doing so, encouraging dual-sourcing from multiple or lower-risk regions, holding buffer inventories, and planning alternatives for potential transportation and logistical bottlenecks.

Moving forward, the task force will aim to highlight these recommendations, and others made over the past two years with the goal of securing the ICT supply chain. With the interconnectedness between the sectors and the scale of supply chain risks faced by both government and industry, private-public coordination is essential to enhance the ICT supply chain resilience.

For more information and resources about ICT supply chain, visit cisa.gov/ict-scrm-task-force.

Thank you,

Sector Partnership

Cybersecurity and Infrastructure Security Agency

Department of Homeland Security

Sector.Partnership@CISA.DHS.GOV

