CISA Task Force Makes Progress in Supply Chain Security

Partnerships and collaborations will be priorities in advancing supply chain security for information and communications tech.

Melissa Harris
Thu, 10/17/2019 - 15:19

A Cybersecurity and Infrastructure Security Agency task force aimed at identifying and developing strategies to improve information communications technology supply chain security is emphasizing public-private partnerships and international collaboration with allies as key steps to risk management.
The group, called Information and Communications Technology Supply Chain Risk Management Task Force comprising 20 federal partners and 40 industry members, highlighted its findings and recommendations in its first interim report released last month.

The report, which the task force’s co-chairs presented before the House Homeland Security Committee Wednesday, details two key takeaways: information-sharing between federal and industry partners remains a priority, and the global supply chain threat landscape is diverse.

“We want something in place to encourage private-sector firms to share information about things they might not have trusted based on due diligence work they do,” said Bob Kolasky, assistant director of CISA’s National Risk Management Center and task force co-chair. “We want to expand our ability within the federal government to give it in the hands of the procurement officials within the federal government” by gaining more information from industry in return.

In looking at the size and scope of the supply chain threat landscape, the task force compiled nearly 200 supplier-related threats and categorized them into nine categories, including cybersecurity, economic and legal factors, which requires equally broad and deep threat analysis, said task force Co-Chair John Miller, who also serves as senior vice president of policy and senior counsel at Information Technology Industry Council.

“This work illustrates how adequately managing supply chain risk requires a fact-based and contextual analysis of multiple identifiable threats and potential mitigation,” Miller said.

Based on its findings, the task force issued three key recommendations for lawmakers to consider in strengthening national ICT supply chain security.

First, lawmakers should continue to use the task force as a key resource for public-private collaboration on supply chain risk management to help inform respective policy efforts and collaborate with the Federal Acquisition Security Council to help build both partnerships between agencies and industry and the rules to implement the Secure Technology Act.
The second is to target future supply chain measures to identity gaps.

“The task force realized early on that conducting an inventory of public-sector supply chain activities would be useful for helping the task force and other stakeholders identify what tasks weren’t being done and to prioritize those that were most important,” Miller said. “Once complete, we should share the task force inventory results with key stakeholders and leverage those results to inform supply chain policymaking across the board.”

The final recommendation calls for the U.S. government to continue working with international partners to pursue coordinated and globally scalable solutions to ICT security.

With 5G security one priority for CISA, according to the agency’s strategic intent document, the multiple layers of collaboration and partnerships between government and industry, as well as between agencies, are critical, Kolasky said.

“We can’t do this work without the partnership with industry and across the interagency,” he said. “The task force can be a model for a range of public-private partnership activities in this space and beyond.”

The task force has aided CISA in addressing Executive Order 13873, which calls for the agency to identify supply chain vulnerabilities in the U.S., Kolasky said. CISA deconstructed the ICT supply chain into 61 elements, including hardware, software and services that collectively make up the ICT ecosystem, and relied on the task force to complete its assessments.

“Among the elements that CISA designated as critical for focusing supply chain risk reduction efforts were home subscriber services, mobile switching centers and sensitive system software, to include software-defined networking,” Kolasky said about CISA’s findings.

The future goals of the task force are to push further on guidance around a qualified bidder list and qualified manufacturer list and to continue information-sharing threat evaluation work — particularly in coming back to the committee with “tangible recommendations” on that matter, Kolasky said.
The task force in the next year will look to connect its work with other critical infrastructure areas and with the Federal Acquisition Security Council to help it form its strategic plan, Kolasky added.

The interim report further details that four working groups within the task force will divide this work by focusing on information-sharing, threat evaluation, qualified bidder and manufacturer lists, and policy recommendations to incentivize the procurement of ICT from authorized resellers and original equipment manufacturers.