Defense Industry Companies Launch Supply Chain Cybersecurity Task Force

WASHINGTON, D.C., USA, April 3, 2019 /EINPresswire.com/ -- The Defense Industrial Base Sector Coordinating Council (DIB SCC) announced today the chartering of the Supply Chain Cybersecurity Industry Task Force to identify, prioritize, oversee and drive adoption of implementable solutions to protect controlled unclassified information throughout the supply chain. Mike Gordon, Chief Information Security Officer (CISO) for Lockheed Martin, chairs the DIB SCC. Gordon explained, "This task force will use the DIB SCC construct to serve as a focal point for industry collaboration across the supply chain, leveraging input and efforts from small to large companies. Our objective is to help identify and implement adversarial-focused solutions that enhance the cyber posture of companies throughout the multi-tier supply chain."

"We recognize that nation states and other attackers are aggressively targeting suppliers at all tiers of the DIB supply chain in an effort to steal or alter intellectual property and DoD information residing on company networks," said J.C. Dodson, Vice President, Cybersecurity and Global CISO, for BAE Systems. "This task force will help to ensure the appropriate level of collaboration to eliminate vulnerabilities and protect critical national security information."

The formation of this task force marks the continued evolution of information sharing and collaboration within the defense industry, but sharply focuses on supply chain cyber security activities and will serve as an on-going mechanism to drive change to improve the resilience of the DIB. "By creating a focused construct for repeatable idea generation, and a trial and execution engine under the DIB SCC, industry will better be able to coordinate and partner with DoD task forces and agencies focused on the same problem," said Dr. Michael Papay, Vice President and CISO for Northrop Grumman Corporation (NGC).

Initial focus areas for the task force include evolving requirements to focus on advanced persistent threat (APT) tactics, enhancing oversight and accountability, driving implementation of paradigm changing approaches and establishing enduring partnerships across industry and with the DoD. Jeff Brown, Vice President and CISO, Raytheon Company, observed, "There is no one single solution that can secure the supply chain. We need to bridge potential technical solutions and multi-tier implementation approaches to enhance protections throughout the supply chain."

Task Force members are comprised of small, medium and large companies who form the DIB SCC. Founding members of Task Force are BAE Systems, Boeing, Lockheed Martin, Northrop Grumman and Raytheon. "The importance of working together to address this issue cannot be understated, input from companies of all sizes is important to ensuring proposed approaches will actually work" said Scott Regalado, Sr. Director, Information Security and Boeing Sr. leadership representative, Boeing Company.

Steve Shirley, Executive Director, National Defense Information Sharing and Analysis Center (NDISAC) explained that US national policy for critical infrastructure protection encourages the creation of sector coordinating councils (SCCs) and counterpart US Government coordinating councils (GCCs). Shirley, who is also SCC Vice Chairman, noted the underlying policy affords an exemption to the Federal Advisory Committee Act, and is a means to conduct iterative dialogs to drive collaborative solutions between Government and Industry. "There's a higher potential for an optimal outcome when there is a collaborative process," Shirley emphasized. The DIB SCC is

nested within the NDISAC for administrative and staff support.

About the DIB SCC
The Defense Industrial Base (DIB) Sector Coordinating Council (DIB SCC) serves as the primary private sector policy coordination and planning entity for the DIB to discuss cybersecurity, physical security, insider threat and issues that affect the resiliency of the DIB. The DIB SCC sustains the security, resilience, and critical infrastructure protection advances of the U.S. Defense Industry, both as an industry coordinating body within the DIB sector, and in partnership with the Department of Defense (DoD) as the designated Sector Specific Agency (SSA) for the DIB. The DoD's counterpart to the SCC is the DIB Government Coordinating Council (DIB GCC).

Operating under the auspices of the DHS Critical Infrastructure Partnership Advisory Council (CIPAC) framework, the DIB SCC was established by the Secretary of Homeland Security pursuant to the authority of section 871 of the Homeland Security Act of 2002 (6 U.S.C. §451). The DIB SCC provides a single point of contact for internal coordination on a wide range of sector specific infrastructure protection activities and issues. It further provides a recurring forum for the DoD and the DIB to facilitate information sharing, discuss areas of mutual interest, to synergistically leverage activities, to eliminate duplicative processes, and to collaborate on measures necessary to ensure the DIB sector mission performance.

The DIB SCC maintains relevant coordination with operational activities of the Federal government and other operational organizations via the National Defense Information Sharing and Analysis Center (National Defense ISAC) which supports the DIB SCC as the sector's information sharing, analysis, and operational mechanism.

NDISAC
National Defense ISAC
+1 202-888-2724
email us here
