Report on Supply Chain Compliance Volume 3, Number 12. June 11, 2020

DARPA working on security solutions for next-gen chips

By Sascha Matuszak

The United States Defense Advanced Research Projects Agency (DARPA) is working to create automated security engines for integrated circuit (IC) chips. The automated engines are meant to close a security gap in the IC chip supply chain that threatens to compromise the vast emerging smart appliance market. In order to enable the Internet of Things, DARPA has enlisted two teams of private and academic organizations to develop security solutions that can be embedded into the new generation of IC chips.

The DARPA initiative is known as the Automatic Implementation of Secure Silicon[1] (AISS) program. The goal of the program, according to a DARPA news release, is to "automate the process of incorporating scalable defense mechanisms into chip designs, while allowing designers to explore chip economics versus security trade-offs based on the expected application and intent while maximizing designer productivity."

AISS has chosen two teams to conduct research that addresses four distinct security risks: side channel attacks; hardware Trojans; reverse engineering; and supply chain attacks, such as counterfeiting, recycling, re-marking, cloning and overproduction. The two teams consist of: