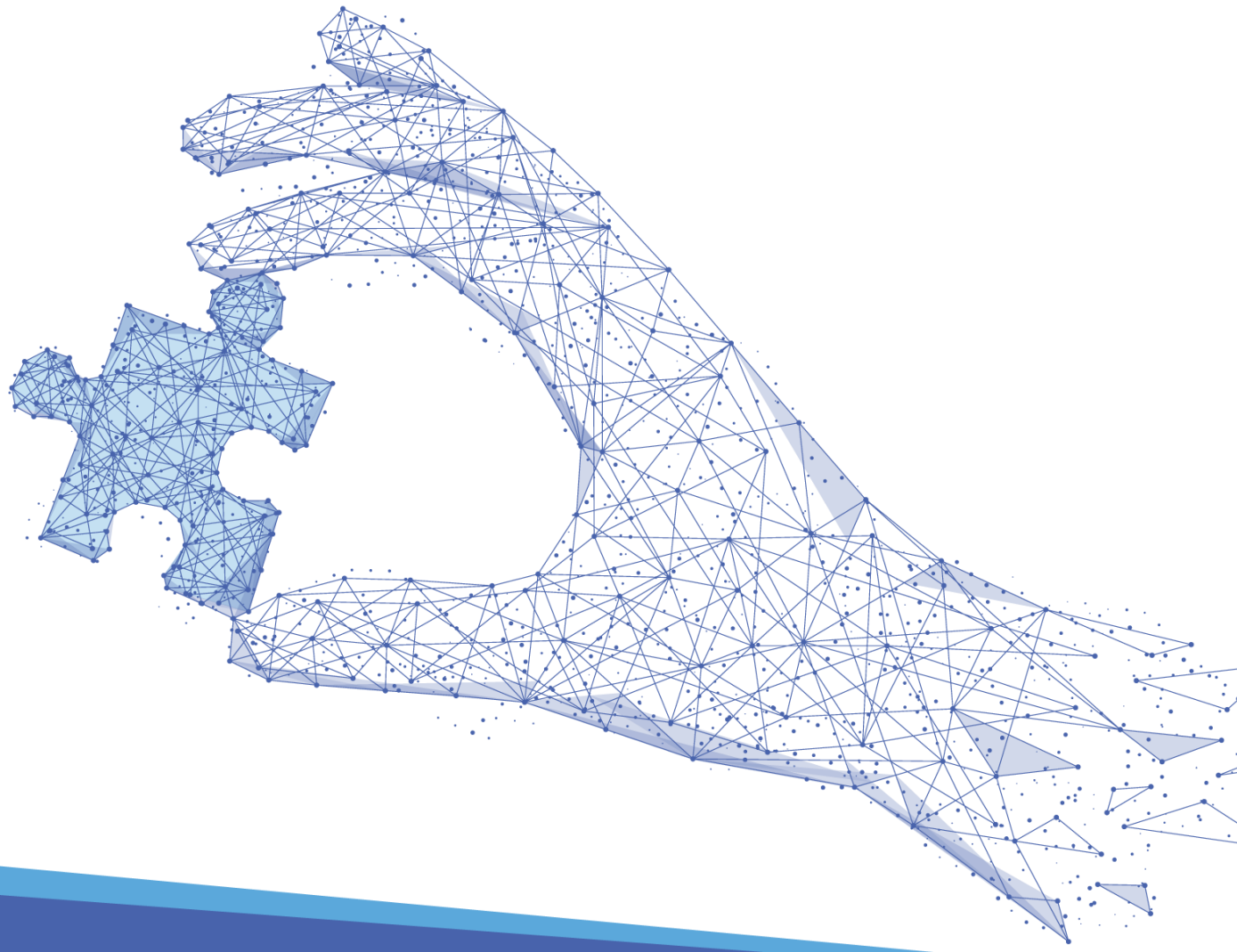


Pentagon's Supplier Network Concern Affects Every Organization

Whitepaper

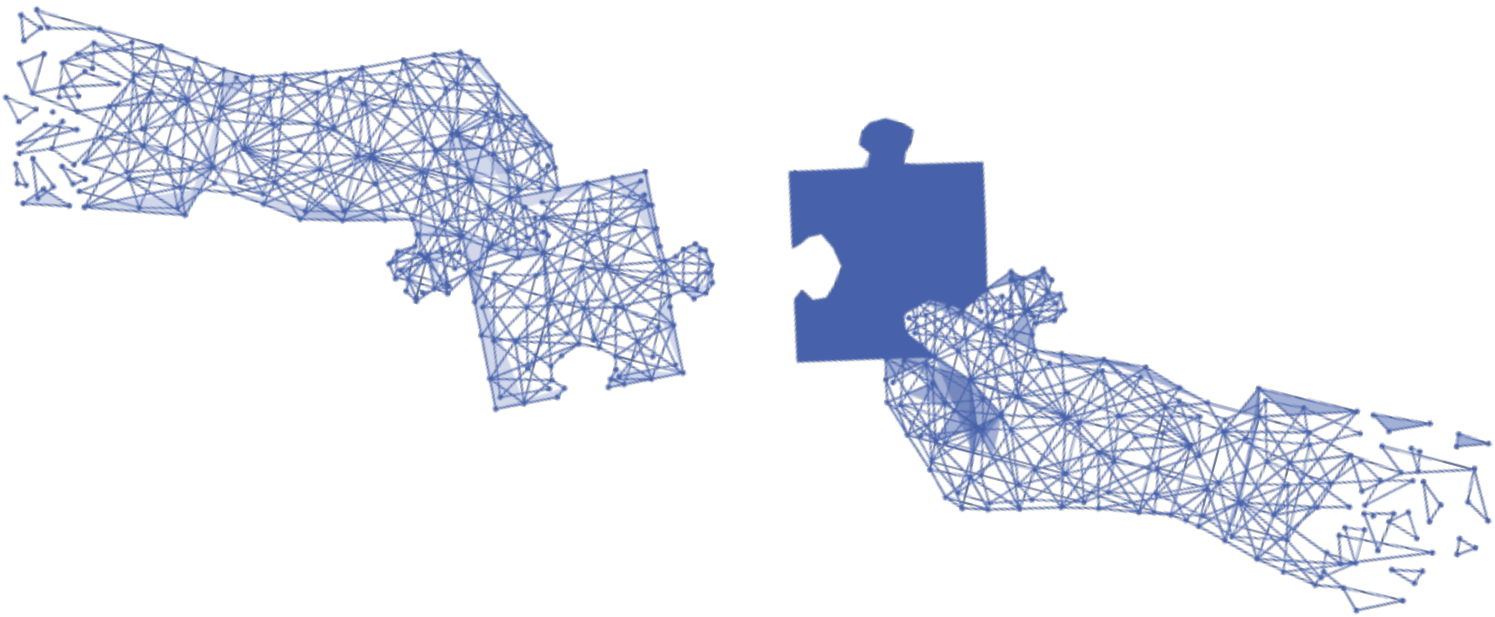
attila SECURITY

What concerns the Pentagon should concern every organization.

The Pentagon is worried about foreign threats to its supply chain. So worried in fact that it's launching a program to do something about it. Called the Trusted Capital Marketplace program, the idea is to strengthen the industrial base against China and other potential adversaries. The program is set to launch in late October or early November, 2019. According to Ellen Lord, undersecretary of defense for acquisition and sustainment, "The idea here is that we don't often look down into the fourth, fifth, sixth, seventh layer of our supply chain to understand where we're sole source or where we're dependent on a foreign entity that might not be a trusted source."

In other words, the government's supply chain isn't only wide, it's also deep. And each member of that supply chain ecosystem represents a potential security threat. What wasn't explicitly stated in the program announcement is the fact that what concerns the Pentagon should concern every organization.

> **"The government's supply chain isn't only wide, it's also deep."**

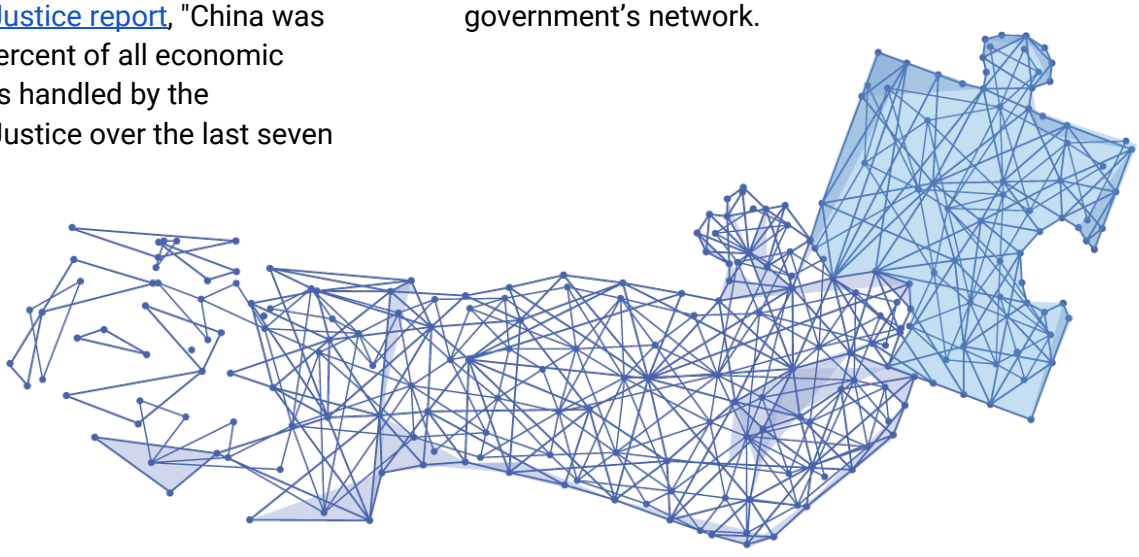


Impetus for the Trusted Capital Marketplace Program

According to National Defense Magazine, "The effort, which the Pentagon announced earlier this year, is in response to growing concerns about foreign nations such as China investing in U.S. companies and how that could affect national security. Particular focus areas for the Defense Department are rare earth elements as well as small unmanned aerial systems."

Since the release of a 2018 report: *Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States*, the Pentagon has focused on investing in areas that strengthen its supply chain. However, much of its time has been spent intervening and attempting to block foreign acquisitions of U.S. tech companies that play an important role in national defense. The reality the United States government has had to face is that foreign suppliers represent a threat, with China being the most significant. According to a Department of Justice report, "China was involved in 90 percent of all economic espionage cases handled by the Department of Justice over the last seven years."

According to the Cox Report, "The Chinese government is accused of stealing trade secrets and technology, often from companies in the United States, to help support its long-term military and commercial development. China has been accused of using a number of methods to obtain US technology (using U.S. law to avoid prosecution), including espionage, exploitation of commercial entities and a network of scientific, academic and business contacts." It becomes even more egregious. According to testimony before a House subcommittee, "In addition to traditional espionage, China partners civilian Chinese companies with American businesses to acquire technology and economic data and uses cyber spying to penetrate the computer networks of US businesses and government agencies." And, espionage isn't the only threat. The computer systems of suppliers (both foreign and domestic) are often insecure, and thereby bring infections into the government's network.



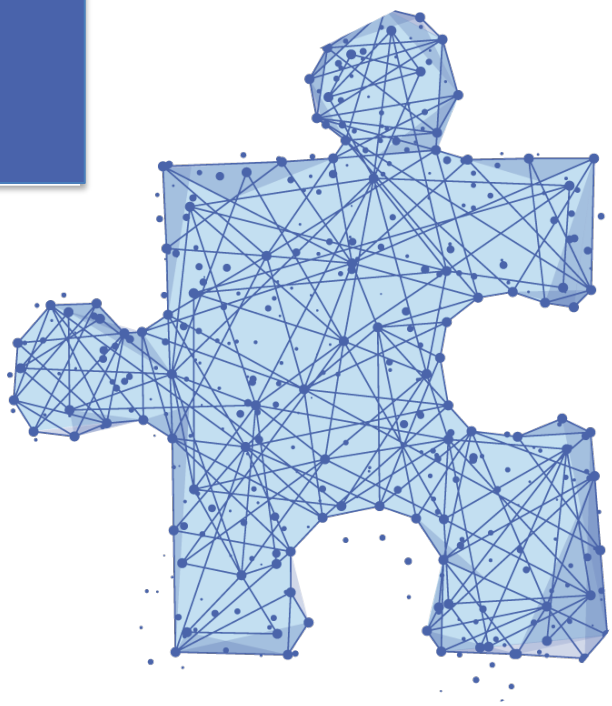
Impact of New Legislation on Private Sector Companies

What concerns the government should concern every organization, whether public or private. There are many, many links in a supply chain, and nearly every organization has at least one foreign supplier, perhaps even one from China. Risk travels up and down the supply chain, and in general cyber vulnerabilities and the threat of industrial espionage both increase along with the complexity of the supply chain. In some regards, industrial espionage is more of a threat than typical cyber exploits like malware and ransomware.

How bad can industrial espionage get? In one example, China-based Sinovel Wind Group Company was convicted for stealing wind turbine technology from a U.S. company resulting in a loss of over 700 jobs (over half the company's global workforce) and more than $1 billion in shareholder equity.

No Easy Solution for Network Insecurities

The Pentagon's approach to addressing its network insecurities probably isn't practical for most private sector organizations. National Defense reported that the DoD's approach "is to get secure sources of capital together with typically small, innovative companies that have technology and early-stage products in the sectors that we identified to try to get investment in areas that the Department of Defense thinks are critical."



So, what can private sector companies do to protect their organizations from foreign adversaries? Since it isn't feasible to try to recreate or control the entire supply chain ecosystem, the best alternative is to establish secure business relationships with all first line suppliers.

A sound business relationship may begin by vetting a supplier, but it is also critical to establish a means for secure communications and data transmission. One way in which this may be achieved is by mandating the use of a virtual private network (VPN) for all communications. VPNs establish a secure point-to-point “tunnel” for data transmission, encrypt the data, filter internet and data traffic and deny unsolicited data requests. Those VPNs that are CSfC (Commercial Solutions for Classified) certified may even be used for the transmission of classified data. A VPN not only secures supplier-government communications from unknown attackers, it also secures it from the rest of the supply chain ecosystem. In essence, a VPN deepens an organization's security with respect to its supply chain.

There is no easy solution to the problem the Pentagon has identified regarding network insecurities. There are only incremental steps. Still, all public enterprises must take these small initial steps to improve their own security profiles. The stakes are high, and the adversaries aren't going away.

.