Coalition for Responsible Cybersecurity

Preventing harmful export control rules for cybersecurity products and services

Coalition for Responsible Cybersecurity Asks For Deletion of Intrusion Software Controls

WASHINGTON, DC – March 23, 2016 — Presenting before the Regulations and Procedures Technical Advisory Committee (RPTAC), an advisory board of the US Department of Commerce Bureau of Industry and Security, the Coalition for Responsible Cybersecurity again asked for the complete removal of the Wassenaar Arrangement controls on intrusion software. This approach would not only remove the controls on technology but also on hardware systems and software products.

The Coalition supports the US Government's decision to return the issue to Wassenaar and seek renegotiation of the language. However, the US Government cannot eliminate controls only on technology. A more comprehensive approach is necessary to address the flaws in Wassenaar.

"We appreciate and support the US Government's proposal to eliminate controls on technology at the upcoming Wassenaar meeting. It is a good first step, but it needs to go further," said Cheri McGuire, Vice President of Global Government Affairs and Cybersecurity Policy at Symantec. "The hardware and software controls also should be eliminated, as they would continue to hinder the ability of global companies to fully protect their own networks and customers and to stay ahead of future threats."

During the 2013 Wassenaar Arrangement plenary session, the member nations agreed to export controls for software, hardware, and technology that generate, operate, deliver or communicate with "intrusion software. The purpose of was worthy, but the agreed-to controls are deeply flawed, controlling not only malicious "intrusion" software, but virtually any type of software, hardware, and technology designed to counter "intrusion" software. The controls have also been ineffective in actually reaching their intended purpose, and international implementation of the controls has been wildly divergent.

"We appreciate the opportunity to again go on record about the dangers of the proposed rule," said Adam Ghetti, Founder and Chief Technology Officer of Ionic Security. "It is important everyone understands that U.S. cybersecurity would be dramatically harmed if the intrusion software controls are not removed in full."

The Coalition was formed to ensure that US export control regulations do not negatively impact US cybersecurity effectiveness. It educates US government policymakers on the dangers of using export control regulations in this way and advocates for alternatives.

The Coalition for Responsible Cybersecurity represents a broad cross-section of cybersecurity companies, including Symantec, Ionic Security, Intel, Microsoft, FireEye, Raytheon and others.

Contacts

Steptoe & Johnson LLP
Alan Cohn, 202-429-6283
acohn@steptoe.com