The Software Alliance

BSA

The Wassenaar Arrangement

Overview

BSA urges members of Congress to sign the Langevin-McCaul letter that cautions against implementing recent updates to the Wassenaar Arrangement (a 41-country, voluntary export control agreement) in a manner that would undermine the United States' national security by regulating access to fundamental cybersecurity technologies.

ISSUE DISCUSSION

The Administration is in the process of implementing recent updates to the Wassenaar Arrangement pertaining to "intrusion software." These well-intentioned provisions are meant to prevent rogue governments from obtaining sophisticated intrusion and surveillance technologies to spy on their own citizens. Although we strongly support this objective, the Administration's flawed proposal for implementing the Wassenaar provisions would undermine US national security while having no impact on the spread of surveillance technologies.

Background and Concerns:

- The Wassenaar Arrangement is a 41-country, voluntary export control agreement. In 2013, members of the Wassenaar Arrangement agreed to impose export controls on hardware and software specially designed or modified for the "generation, operation or delivery of, or communication with" "intrusion software."

- The controls were proposed by the UK government, and were intended to apply to sophisticated spyware/surveillance systems — such as those sold by FinFisher, a UK company, after it became public that these products had been exported to the Governments of Bahrain and Turkmenistan to spy on political dissidents and other activists.

- Unfortunately, the negotiators of these provisions lacked technical expertise and defined "intrusion software" far too broadly. As a result, the Wassenaar Arrangement provisions require export licenses for virtually any defensive cybersecurity technology.

- In May, the Commerce Department issued a Proposed Rule to implement the Wassenaar Arrangement. This Proposed Rule exacerbates the problems associated with Wassenaar's overly broad definition by imposing an unnecessarily strict control policy. Under the Proposed Rule, an export license would be required for virtually any transaction involving cybersecurity technologies or services. Because export licenses can take months to obtain, the Proposed Rule is a serious threat to the ability of US companies to defend themselves against cyber-attacks.
    - Access to legitimate cybersecurity tools would be restricted, as the export of cybersecurity technologies and testing tools would be constrained, even to overseas subsidiaries of US companies.
    - Research into cybersecurity vulnerabilities would be curtailed, as researchers would be hindered from testing networks and sharing technical information across borders.

- Collaboration on cybersecurity risks would be harmed both within cybersecurity companies and with customers and industry partners, as information would be deemed "exported" if it is shared with non-US persons, even if they are physically located in the US.

- In response to the Commerce Department's request for comments, more than 250 stakeholders from across the cybersecurity ecosystem warned that fundamental flaws in the Proposed Rule would: (1) weaken US cyber defenses by imposing burdensome licensing requirements on many commonly used security products, technologies, and techniques; (2) undermine the competitiveness of the US cybersecurity industry; and, (3) increase network susceptibility and risk to the very intrusion and surveillance technologies the Wassenaar Arrangement was intended to thwart.

- In the face of significant pushback from industry, the security research community and public interest organizations, the Commerce Department rescinded the Proposed Rule but has indicated that it will develop a revised rule that it will open for a second round of public comments in early 2016. Despite this pledge, BSA is concerned that the Administration is continuing to overlook the concerns.

BSA POSITION

- **The Administration failed to give sufficient consideration to the unintended national security impacts of the Proposed Rule.** As the Administration works to develop a revised rule, Congress should send a clear message that implementation of the Wassenaar Arrangement's "intrusion software" provisions must be consistent with the United States' broader cybersecurity strategy.

- **Securing our nation's critical networks and infrastructure against malicious intrusions requires real-time testing and remediation actions.** To combat the rapidly evolving threat landscape, cybersecurity professionals must be able to freely share information about threat indicators and solutions with large networks of experts around the world.

- **Congress should therefore encourage the Administration to reject any approach to implementing the Wassenaar Arrangement that would hamper the efforts of cybersecurity professionals by imposing delays and restricting the use of the best available cybersecurity technologies.** The Administration should likewise reject any proposal that is inconsistent with President Obama's Executive Order 13691, which recognizes the necessity of ensuring that all players within the cyber ecosystem are "able to share information related to cybersecurity risks and incidents and collaborate to respond in as close to real time as possible."

- **Signing on to the Langevin-McCaul letter will help ensure that these cybersecurity equities are considered** as the Administration revises its approach to implementing the Wassenaar Arrangement provisions.