October 28, 2015

Lisa Aguirre
DTAG Alternate DFO
Directorate of Defense Trade Controls
Bureau of Political-Military Affairs
U.S. Department of State
Washington, DC 20522-0112

Via Email and Fax: DTAG@state.gov / (202) 261-8199

Statement to the DTAG Pursuant to Public Notice: 9281 of September 23, 2015 Defense Trade Advisory Group; Notice of Open Meeting

The Electronic Frontier Foundation and Access Now submit the following comments to the Defense Trade Advisory Group (DTAG) in advance of its upcoming open meeting. The agenda for the meeting includes a discussion of export control reform, specifically a review of "cyber products" and recommendations for which products, if any, should be included on the U.S. Munitions List (USML), and the potential impact on cyber products resulting from such export controls.

About the Electronic Frontier Foundation: EFF is a nonprofit, member-supported civil liberties organization working to protect privacy and free expression in technology, law, policy, and standards in the information society. EFF actively encourages and challenges the executive and judiciary to support privacy and safeguard individual rights as emerging technologies become more prevalent in society. With over 22,000 dues-paying members and over 280,000 mailing-list subscribers, EFF is a leading voice in the global and national effort to ensure that fundamental liberties are respected in the digital environment.

About Access Now: Access Now is an international, non-profit organization that defends and extends the digital rights of users at risk around the world. By combining innovative policy, user engagement, and direct technical support, we fight for open and secure communications for all.

Recommendations

We recommend against adding "cyber products" to the USML. DTAG should be cautious in suggesting that cybersecurity-related devices or services should be export controlled. While we oppose the use of technology in contravention of human rights, the challenge of narrowly and precisely defining "cyber products" risks chilling cybersecurity research and the licit use of cybersecurity devices and services. Furthermore, limitations on the sale of cybersecurity software implicates speech protected by the First Amendment and international freedom of expression standards.

Adding “cyber products” to the USML could limit the development and use of research and tools critical to the security of the Internet. Creating clear definitions for the “cyber products” to be listed on the USML would be a nearly impossible task, given the general purpose nature of software. DTAG should look to the Department of Commerce’s Bureau of Industry and Security’s difficulty defining “intrusion software” for control under the EAR as an illustration[1] of the difficulty of creating clear definitions in this space. Any ambiguity in the definition would risk extreme chilling effects on the computer security industry. If, for example, the USML could be read to control the vulnerability market, it would create undue pressure on independent security researchers, who would be unsure of whether their work would be controlled.

Export controls on software, besides being extremely difficult to define, have in the past had serious unintended consequences. Previous export controls on software have resulted in widespread risk to all Internet users. For example, the inclusion of encryption technology on the USML led to deployment of an “export grade” standard to avoid the USML definition. As it turned out, that persistent “export grade” standard, even 20 years after encryption controls were lifted, left millions of users susceptible to the “FREAK” attack[2] used to monitor and modify website browsing data.

In addition to the security risk that will inevitably result from developers having to engineer their software around the USML “cyber products” definition, any restrictions (intended or otherwise) on the sharing of vulnerability research and security tools raise freedom of expression questions and would need to be evaluated on domestic and international legal standards. In the U.S, the Ninth Circuit Court of Appeals has ruled that software source code is speech protected by the First Amendment.[3] The United Nations Special Rapporteur for Freedom of Opinion and Expression has reported[4] that prohibitions on the use of encryption unnecessarily and disproportionately restrict freedom of expression, and rules controlling its import and export may constitute a ban.

Finally, we note that the ongoing process of implementing the Wassenaar Arrangement 2013 plenary agreements on intrusion software, surveillance systems, and other items in the United States has been a highly contentious process. Adding “cyber products” to the USML at this time may conflict with the Wassenaar Arrangement implementation, and would certainly risk confusing and dividing the already-limited stakeholder engagement in this important discussion.

Export controls must comply with domestic protections and international human rights law without chilling research and the promotion of cybersecurity. Given the above considerations, and the practical impossibility of defining the control list with enough specificity to avoid severe chilling effects on the computer security industry, we strongly

---

[1] https://www.bis.doc.gov/index.php/policy-guidance/faqs

[2] https://freakattack.com/

[3] *Bernstein v. United States*, 176 F.3d 1132 (9th Cir. 1999).

[4] https://www.eff.org/deeplinks/2015/06/un-special-rapporteur-calls-upon-states-protect-encryption-and-anonymity-online

recommend that DTAG not advise the State Department to add “cyber products” to the USML. We further urge DTAG to exercise caution before implementing export controls on any cybersecurity-related devices or services.

Sincerely,

Nate Cardozo
Staff Attorney

Eva Galperin
Senior Global Policy Analyst

for the
Electronic Frontier Foundation

Amie Stepanovich
U.S. Policy Manager

Drew Mitnick
Policy Counsel

for
Access Now