

COMPSEC DIRECT

706 CRAWFORDS KNOLL CT, ODENTON, MD, 21113 443-345-0503 INFO@COMPSECDIRECT.COM

This letter is in reference to the Wassenaar Arrangement (WA) 2013 request for comments via the Bureau of Industry and Security (BIS) BIS-2015-0011. Our company is deeply concerned with the vocabulary and intent that the proposed modifications to WA includes in these revisions. We are a small company comprised of security experts and researchers. Our staff includes personnel that conducted some form of vulnerability analysis and cyber operations within the Department of Defense under the rules of regulations of the United States (US) government. Based on our experience with Federal regulations, we feel the proposed revisions to WA essentially creates numerous foreseeable problems to individuals inside the Information Security community domestically and abroad since the WA already includes numerous problems.

As a computer security company, we understand the need for some form of restriction for items already covered within WA; such as weapons and other tangible assets. Using WA to control encryption created or funded by the US government or US companies was inevitably doomed to fail as society became more interconnected and sharing previously guarded cryptologic controls covered under WA became impractical and impossible to effectively enforce. The WA revisions represent a noble, yet flawed attempt by US lawmakers and policy decision makers to attempt to rein in this uncontrollable problem (ECCN 5A001.j, 4A005, 4D004). Encryption, as opposed to destructive devices and weapons, is intangible and simpler to conceal than before. Using WA between countries seems more like a gentleman's agreement to respect each other's intellectual property as a matter of convenience. The revisions to WA propose licensing fees and dues which creates a market place of elitism where only well financed corporations in the Information Security industry can play (ECCN 4D001). These revisions, as they are currently worded, will limit innovation and the development of small companies within the US (§ 742.6(b)). The ENC Encryption Request Coordinator cannot feasibly accomplish this undertaking in our opinion.

We are aware that the US government does not want companies either US based or incorporated within the US to simply export encryption to countries with strained diplomatic ties; however this is already covered in the current WA as it is written. The revisions attempt to include a broad range of security applications, programs and high level concepts. In this case, the vocabulary is generalized and is the equivalent of attempting to regulate the dissemination of a tool (ECCN 4A005). As an Information Security professional, many of the terms placed into restriction via WA 2013 are the tools we use to help grow and secure our customers networks. These revisions are similar to attempting to regulate a carpenter's hammer and nails and a plumber's solder torch. The WA revisions also serve as a punitive basis when we notify customers in the private and public sector of potential vulnerabilities and data breach. Instead of allowing Information Security companies, Information Security professionals and Information Security students the ability to notify and help and organizations improve current security controls and practices; you are creating a legal basis which companies and organizations can leverage against individuals under the guise of protecting the priorities of the few while violating the constitutional right of freedom of speech (ECCN 5A001.j, ECCNs 4A005, 4D004, 4E001, 5A001, 5A002, 5D002 and 5E002). Encryption, and the ability to decrypt, is now commonly found in many of the security tools the WA 2013 revisions attempts to limit. This also limits the effectiveness of how well future Information Security professionals and companies conduct business.

If individuals and companies like us cannot divulge or notify companies that their customer and financial information can be exposed or is exposed, where will it end? Will the use of common security tools and techniques inside the Information Security community be impacted by the current draft of WA 2013? Yes, it will. Because of this, the BIS needs to revise the broad vocabulary used and listen to the overwhelming voices of reason that have taken a stand against the current draft of WA 2013.

Attentively,

Jose Fernandez
President CompSec Direct
Information Security Researcher