ETRAC Meeting Presentation

BIS Implementation of the 2013 Wassenaar Arrangement

By: Iain Mulholland

October 15, 2015

VMware Background

- 4th Largest Software company in the world; and the fastest growing
- Global company, 18,000 employees in 140 countries worldwide
- VMware has more than 500,00 customers and 75,000 partners, including 100 percent of the Fortune 100
- VMware serves all sectors of the U.S. Government; including the Department of Defense, the Civilian agencies, and the Intelligence Community; as well as state and local government
- Our software installed in 90 percent of all federal datacenters
- VMware builds core infrastructure software behind cloud computing
- Makes considerable investments in building and maintaining customer trust
- VMware maintains a large, dedicated internal global team focused on ensuring product security

Iain Mulholland : Bio

- Vice President, Engineering Trust & Assurance
  - Established VMware Product Security Group in 2011
  - 15+ years in Product Security field
  - Founding member of Microsoft Trustworthy Computing Group in 2002
  - Leading expert in Product Security Incident Response

VMware Statement

Based in Palo, Alto, California, VMware is a global software company with 18,000 employees in 140 countries worldwide. Like other global software companies, VMware regularly exchanges security-related information across borders to conduct research and development, for security testing against our own global software infrastructure, or to resolve and prevent any network breaches for our business clients.

The draft BIS proposal to implement the 2013 Wassenaar Arrangement would severely undermine VMware's ability to secure not only our networks but that of the technology security ecosystem as a whole.

Moving forward, we encourage BIS to revisit its original proposal to implement the 2013 Wassenaar Arraignment. We also strongly support BIS and the Administration to return to Wassenaar to renegotiate the export control rules given the global nature of cybersecurity threats from both inside the U.S. and oversees.

Summary of Concerns

- The need to apply for export licenses for every security related instance is not workable and could open U.S. companies and the cybersecurity ecosystem to a greater number of network vulnerabilities

- It is important for BIS and the Commerce Department to advocate for a bilateral solution; fixing U.S. policy only solves part of the problem

- Duality is impossible to separate at a practical level – exploits are the ‘scientific proof’ often required by defenders to accurately identify and remediate security issues

Specific Examples where current proposed rules lead to product insecurity

- Recent publicly reported Critical security vulnerability in VMware vCenter management product
- Internal global use of exploit code in automated testing, developer education programs
- Software Industry real-time sharing of threat information, including exploits and vulnerability detection code

Recommendations

- VMware believes that BIS and the Department of Commerce should revisit its original proposal to implement the 2013 Wassenaar Arrangment.

- VMware strongly supports BIS, the Commerce Department and other federal agencies to returning to Wassenaar to renegotiate the 2013 Arrangement.

- Create a “Working Group” at the upcoming Wassenaar meeting in December. This could help facilitate a renewed dialogue with other Wassenaar signatories to help resolve some of the challenging issues relating to the export control component of the 2013 Wassenaar Arrangement