Coalition for Responsible Cybersecurity

Preventing harmful export control rules for cybersecurity products and services

BIS ETRAC Meeting
October 15, 2015

Presentation of the Coalition for Responsible Cybersecurity

Presented by:

Meredith Rathbone – Steptoe & Johnson LLP

Ryan Speers – Ionic Security Inc.

Bill Wright – Symantec Corporation

Mario Palacios – Intel Corporation

Overview of Concerns

- The Coalition believes that, while the intended purpose of the rule was worthy, the controls proposed by BIS will have a devastating impact not only on the U.S. cybersecurity industry, but on cybersecurity itself
  - Overbroad: lack of technical distinction between legitimate cybersecurity items and malicious items
  - Ineffective: unlikely to deter bad actors
  - Counterproductive: would result in mostly collateral damage by hindering law-abiding companies' ability to protect us, while achieving a small policy benefit that could be accomplished through other means

*The Coalition for Responsible Cybersecurity represents a broad cross-section of U.S. cybersecurity companies, including Symantec, Ionic Security, Intel, FireEye, Synack, Raytheon, Global Velocity, WhiteHat, and Trail of Bits

Unique Industry

- Not a typical corporate supply chain
  - Application of traditional CCL-based export controls is an exercise in fitting a square peg into a round hole
  - Must respond to real threats in real time: minutes and hours, not weeks and months
    - Those who rely on this industry to protect them would be harmed
  - Cybersecurity industry relies heavily on real-time collaboration
    - Often informal
    - With other companies/individuals
    - Within the United States and around the world
    - Many of which cannot be identified before the threat is discovered

Examples of Unintended Consequences

- Legitimate cybersecurity software/technology – often indistinguishable from malicious products – caught by proposed controls:
  - (1) specially designed or modified to avoid detection by monitoring tools or to defeat protective countermeasures, and
  - (2) extraction of data, modification of system or user data, or modification of the standard execution path of a program or process in order to allow the execution of externally provided instructions
- Ionic's products
- Rescue tools
- Software innovation
- Third party updates and patching

Examples of Unintended Consequences (cont.)

- Legitimate cybersecurity software/technology caught by proposed controls (cont.):
  - Penetration testing
    - The ability to conduct unfettered research into vulnerabilities, including zero days, is critical
  - Threat information sharing
    - Uncertainty about the scope of export controls could cause law-abiding researchers to refrain from sharing critical information about threats
  - Reverse engineering of cyber threats

Recommendations

- Return to Wassenaar to address problems with current language
- The same products & techniques can be used for either malicious purposes or beneficial cybersecurity purposes, depending on the intent of the actor – focus on mechanisms better tailored to distinguish based on intent:
  - Criminal law enforcement
  - Prohibited end use/end users