Wassenaar Arrangement Control Implementation: Intrusion and Surveillance Items

Bob Rarog
Bureau of Industry and Security

Robert.Rarog@bis.doc.gov

U.S. DEPARTMENT OF COMMERCE
BUREAU OF INDUSTRY AND SECURITY

Overview of FR Notice

- Wassenaar Arrangement – 41 member multilateral export control regime
- Notice would implement control language agreed to in the December, 2013, Wassenaar Plenary.
- Two product classes affected: network intrusion and network surveillance
- Controls have been in effect in some member states for a year or more.
- Published as a proposed rule on May 20 with a 60 day comment period
- Unrelated to other Administration initiatives in cybersecurity (e.g. EO 13691 on private sector cybersecurity information sharing, or EO 13694 on sanctions for individuals involved in cybercrime)

Network Intrusion

- Controls would apply to commodities, software and technology for command and delivery platforms – software designed to launch malware capable of extracting or modifying data on a network, or that can modify the standard execution path of a computer program.

Platforms vs. Intrusion Software

- Controls would **not** apply to intrusion software itself (e.g., exploits, rootkits, backdoors, viruses, other malicious code).
- Controls would apply only to systems that generate, operate, deliver and communicate with intrusion software.
- Products designed for penetration testing are included.
- Commonly used software sharing some of the functions of command and delivery platforms (e.g., hypervisors, Digital Rights Management Software) are explicitly excluded.

Technology Controls

- Controls would apply both to technology for the development and production of command and delivery platforms, and to technology required for the development of intrusion software.
- "Intrusion software" is software:
  - Specially designed to avoid detection by monitoring tools or to defeat protective countermeasures;
  - That is capable of extracting or modifying data or modifying the standard execution path of software in order to allow the execution of externally provided instructions.

Examples of Technical Data Captured by the Proposal

- Information on developing, testing, refining and evaluating intrusion software in order, for example, to see what the intrusion software can do, and whether it can be run reliably and predictably
- Information on how to prepare the exploit for delivery, or integrate it into a command and delivery platform
- Development or production of the command and delivery platform itself

Data Not Caught by the Proposal

- Information on how to discover a vulnerability in a system
- Information about the vulnerability, including causes
- Information on testing the vulnerability, including trying different inputs to determine what happens.

EAR Exclusions

The EAR does not control:

- Fundamental research
- Publicly available data
- Open source software

U.S. DEPARTMENT OF COMMERCE
BUREAU OF INDUSTRY AND SECURITY

Network Surveillance

- Proposal includes controls on Internet Protocol (IP) surveillance systems
- Such systems act at the carrier level to intercept and analyze messages to produce personal and social information from Internet traffic.
- Can be used for intelligence purposes, or to maintain surveillance on individuals or groups

Licensing Requirements

- With a narrow license exception for shipments or transmissions to agencies of US and allied governments, a validated license will be required for all destinations except Canada.
- Licenses will be reviewed favorably if destined for US companies or subsidiaries outside of restricted/embargoed countries; others reviewed case-by-case.

Industry Impact and Comments

- Most items caught by this proposal are already subject to controls due to encryption functionality; as a result, we already have some impact data from major vendors.
- BIS needs more information on the impact of proposed controls on internal corporate activity, and on the research community.
- We encourage written comments on the technical language, particular fact patterns, and on general impact.
- We are placing interpretation of specific fact patterns on the BIS website (http://www.bis.doc.gov) on a rolling basis.
- Comments due on July 20.