Cyber Tools History

• Dec. 2013 – Wassenaar Arrangement agrees to cyber tools controls

• May 2015 – BIS publishes proposed rule with a request for public comments.

• 2016 – 2017 – United States negotiates changes to the Wassenaar Arrangement entries

• October 21, 2021 – BIS publishes interim final rule with delayed effectiveness date of January 19, 2022.

• January 12, 2022 – BIS extends effectiveness date by 45 days to March 7, 2022.

• March 7, 2022 – Rule goes into effect.

• May 26, 2022 – Final rule was published.
Cyber Tools

- **4A005** – Designed or modified for generation, command and control, or delivery of “intrusion software”

- **4D004** – Software specially designed for generation, command and control, or delivery of “intrusion software”
  - Exception: Software update tools

- **4E001.c** – Technology for the “development” of “intrusion software”
  - Exception: “Vulnerability disclosure” and “cyber incident response”

Cyber Tools – Intrusion Software

“Software” specially designed or modified to avoid detection by ‘monitoring tools’, or to defeat ‘protective countermeasures’, of a computer or network-capable device, and performing any of the following:

1. The extraction of data or information, from a computer or network-capable device, or the modification of system or user data; or
2. The modification of the standard execution path of a program or process in order to allow the execution of externally provided instructions
Cyber Tools – What is Not Controlled?

Examples of items not caught by these controls include:

• Port Scanners
• Packet sniffers
• Protocol analyzers
• Vulnerability scanners
• Malware

Cyber Tools – IP Surveillance

• 5A001.j – intended to cover large scale government surveillance systems
  ➢ Must operate on a carrier class IP network and perform ALL of the following:
    ▪ Analyze data at the application layer (OSI Layer 7);
    ▪ Extract selected metadata and application content;
    ▪ Index the data;
    ▪ Execute searches of the indexed data based on “hard selectors”
    ▪ Map the relational network of individuals or groups of people
  ➢ Does not apply to products specially designed for:
    ▪ Marketing
    ▪ QoS, QoE
Other Relevant Provisions

• 740.17(b)(2)(i)(F) – Penetration testing tools

• 5A004.a & 740.17(b)(2)(ii) – Cryptanalytic Items

• 740.17(b)(3)(iii)(A) – Automated network vulnerability & response tools.

• 5A980 - Devices primarily useful for the surreptitious interception of wire, oral, or electronic communications.

• 5A001.f.1 – Mobile telecommunications interception equipment.

Cyber Tools – LE “ACE”

• Catch-all: Licenses required when the exporter “knows or has reason to know” that the item will be used for unauthorized (malicious) cyber activities
  ➢ Also applies to items described in 740.17(b)(2)(i)(F), 740.17(b)(2)(ii), and 740.17(b)(3)(iii)(A)

• E:1/E:2: Licenses required for all E:1/E:2 exports including deemed exports, for any reason. Deemed export licenses not required for other foreign nationals

• “U.S. subsidiaries”, banks/financial, insurance, civil medical entities: No licenses required for any purpose.
Cyber Tools – LE “ACE”

• **Vulnerability Disclosure/Cyber Incident Response:** No licenses required except for government end-users in D:1-D:5.

• **Government End-Users:** Licenses required to government end-users of D:1-D:5 countries.
  - Exception 1: Exports to police and judicial bodies in Cyprus, Israel, and Taiwan of evidence of a cyber security incident for criminal or civil investigations or prosecutions.
  - Exception 2: Exports to national CERTS in Cyprus, Israel, and Taiwan for vulnerability disclosure, cyber incident response, or criminal or civil investigations.
  - Deemed Export licenses required.

Cyber Tools – LE “ACE”

• **Non-government end-users:** Licenses required to non-government end-users in D:1 or D:5 for purposes other than vulnerability disclosure and cyber incident response activities:
  - Exception: U.S. subs, banks/finance, health/insurance, civil medical do not require a license for any reason.
Cyber Tools – LE “ACE”

- **Cyber Incident Response** means the process of exchanging necessary information on a cybersecurity incident with individuals or organizations responsible for conducting or coordinating remediation to address the cybersecurity incident.

- **Vulnerability disclosure** means the process of identifying, reporting, or communicating a vulnerability to, or analyzing a vulnerability with, individuals or organizations responsible for conducting or coordinating remediation for the purpose of resolving the vulnerability.

- **Government end-user**: National, regional or local department, agency or entity that provides any governmental function or service, including entities and individuals who are acting on behalf of such an entity.

  - Does not include ‘favorable treatment cybersecurity end-users’.
Cyber Tools – Government end-user

- A government end-user includes:
  - International governmental orgs
  - Government research institutes
  - “More-sensitive government end-users”
  - “Less-sensitive government end-users”
  - Utilities and transportation orgs
  - Retail or wholesale firms owned by the government that make items on the WA ML.

Cyber Tools – License Review Policy

- Licenses are reviewed for both national security and foreign policy concerns, including human rights.

Cyber Tools – Public Comments

• Some comments raised concerns about the scope of control & possible impacts to legitimate cyber security activity.

• Large number of comments asserted that the rule is complex and asked for additional clarification and guidance.

• Some concerns expressed about industry’s ability to implement compliance programs by the implementation date.

Cyber Tools – Guidance

• Revised FAQs to address some of the comments

• Decision Tree on BIS website

• Additional clarifications
Cyber-Related Defense Articles

Generally includes certain types of software either
- designed for intelligence or cryptography, or
- directly related to other defense articles.

• USML Categories IX(e)(3), XI(b), XIII(b), XVII(a), XXI(a)

• Technical Data entry in each relevant USML category

Cyber-Related Defense Services

Includes activities that:

• furnish technical data as defined in ITAR § 120.10;

• constitute military training of foreign units or forces; or

• are both described in ITAR § 120.9(a)(1) and directly related to a
defense article described on the U.S. Munitions List (USML).
Cyber-Related Defense Services

Includes activities that:

• Furnish assistance in developing or using software described on the USML.

• Directly target or protect defense articles

DDTC Licensing

• Case-by-case review pursuant to Conventional Arms Transfer Policy

• Consistent with U.S. foreign policy and national security interests; includes supporting international human rights law and U.S. values

• Transactions that may present human rights concerns, based on the technology to be exported and the proposed end-user, are subject to increased scrutiny
Cyber Tools
Aaron Amundson, Director, Information Technology Controls Division, BIS
Chris Weil, Division Chief, Technology and Jurisdiction Analysis, DDTC