EAR ‘cyber rule’ FAQs

Contents:

13. Mobile phone jailbreaking tools include platforms for delivering intrusion software to the phone. These generally include fully operational exploits including the delivery code. Are such tools subject to control?

"Vulnerability Disclosure" and "Cyber Incident Response"

14. What are the definitions of "vulnerability disclosure" and "cyber incident response" relevant to 'cybersecurity items' and License Exception ACE, and where do I find them in the EAR?

15. What are some examples of "*individuals or organizations responsible for conducting or coordinating remediation*"?

16. When can I export 'cybersecurity items' pursuant to "vulnerability disclosure" or "cyber incident response" without needing to apply for a license?

17. Are there situations where the processes of "vulnerability disclosure" or "cyber incident response" may involve the "release" (or other "export") of "technology" or "software", including source code, related to "intrusion software"?

18. Do I need a license for training someone if the training involves the release of cybersecurity items?

19. Would prior BIS authorization be required for a researcher to privately disclose an exploit to a vendor outside the U.S. with the understanding that the information would NOT be published?

20. I am a cybersecurity professional chiefly responsible for my organization's "cyber incident response" activities. In that capacity, I have been asked to help train and equip the cyber defenders / cybersecurity incident responders (e.g., "Blue Team" and SOC/CSIRT personnel) of a corporate partner of ours, that is headquartered and located in a Country Group D:1 country.

    In planning for this event, I am informed by my corporate partner that a few Government officials of that D: 1 country have been invited to the event, and it is anticipated that these officials may be accompanied by select technical experts who are known to provide consulting services to that Government.

    Is a license required for me to provide this training, and release information and "software" classified under one or more of the 'cybersecurity items' ECCNs related to "intrusion software" to these various participants?

Penetration testing tools and other 'cybersecurity items' overlap with Category 5 - Part 2 'encryption items'

21. My company produces and exports commercial penetration testing (pen testing) software that commands and controls "intrusion software". We have a CCATS that classifies our product as 5D002 and makes it eligible for License Exception ENC §740.17(b)(2)(i)(F). Does this rule re-classify our encryption product as a 'cybersecurity item' classified under ECCN 4D004?

22. What are some examples of ECCN 5D002 pen testing software encryption capabilities?

23. Does this mean that pen testing "software" and "technology" that include cryptographic or cryptanalytic functionality are always 'encryption items' classified in Category 5 – Part 2, and never 'cybersecurity items' classified in Category 4 for purposes of the EAR?

24. If I have 5D002 pen testing software, would I ever have 4E001 technology?

25. Can 'cybersecurity items' software classified under ECCN 4D004 (whether characterized as a 'pen testing' tool, or not) be "released" or otherwise exported under License Exception ACE to all non-'government end users' of a Country Group D:1 or D:5 country under the "vulnerability disclosure" and "cyber incident response" exclusion Note 2 to paragraph (c)(1)(iii), section 740.22, if the intended end use is to help the customer increase its cybersecurity expertise or otherwise improve its IT security posture?

26. I am a trained commercial cybersecurity professional, skilled in performing penetration tests and leading "Red Team" and "Purple Team" exercises for corporate and government clients. For my overseas clients, I sometimes run 'pen test' software remotely from a server in the U.S., sometimes I run 'pen test' software on the client's IT assets (including such software that I might create 'on the fly' during the exercise), and other times I take such software with me on my laptop when I travel to and from my client locations. Do these scenarios subject me to a license requirement?

27. Assuming at least one of the scenarios in question #26 above does involve an export of a 'cybersecurity item', are those exports released by the carve outs for "vulnerability disclosure' and "cyber incident response"?

28. I am planning to export penetration testing software, with and without encryption, to a Country Group D:1, D:2, D:3, D:4 or D:5 end user who is not eligible to receive that product under License Exceptions ENC or ACE. When I submit my license application, should I list the software under both ECCNs 4D004 and 5D002?

29. There is a lot of discussion of penetration testing products in another FAQ. Is that to say that all penetration testing products would fit the definition of "intrusion software"?

‘Cybersecurity Items’ and the Export Administration Regulations (EAR)

1. **What is a ‘cybersecurity item’ for purposes of this rule and the Export Administration Regulations (EAR), and how does this relate to Wassenaar Arrangement (WA) decisions?**

   Answer: This rule implements multilateral Wassenaar Arrangement (WA) export control decisions regarding certain dual-use items related to “intrusion software” and Internet Protocol (IP) network communications surveillance. The new term ‘cybersecurity item’ refers to these specific items that are now subject to the EAR.

   In adopting these controls to the EAR, a new license exception Authorized Cybersecurity Exports (ACE) has been created to permit a qualified range of license-free exports of ‘cybersecurity items’ while ensuring U.S. Government licensing review in situations as required by the national security and foreign policy interests of the United States.

   This includes that License Exception ACE authorizes exports, reexports and transfers (in-country) to the following ‘favorable treatment cybersecurity end users’ located in any non-embargoed / non-sanctioned destination, except in exceptional circumstances where the exporter knows (or has reason to know) that the ‘cybersecurity items’ may be diverted or otherwise misused:

   - ❖ “U.S. subsidiaries”;
   - ❖ Providers of banking and other financial services;
   - ❖ Insurance companies;
   - ❖ Civil health and medical institutions providing medical treatment or otherwise conducting the practice of medicine, including medical research.

2. **Do the terms “intrusion software” and ‘IP network communications surveillance’ mean the same thing?**

   Answer: No, in this export control context the concepts of “intrusion software” and IP network surveillance have distinct meanings and application. These terms do not describe the same commodities, “software” or “technology”, or the same technical capabilities. The EAR implementation of the WA decisions reflects these technical distinctions and their real-world application.

3. **What are the Export Control Classification Numbers (ECCNs) of these ‘cybersecurity items’, and where do I find them in the EAR?**

   Answer: In implementing the WA decisions, this rule adds ECCNs and updates the control scope of Categories 4 (“Computers”) and 5 – Part 1 (“Telecommunications”) of the Commerce Control List (CCL), Supplement No. 1 to part 774 of the EAR.

   The Category 4 ‘cybersecurity items’ related to “intrusion software” (which is defined in Section 772.1 of the EAR) are identified by the following ECCNs, summarized as follows:

- 4A005 : Systems and equipment specially designed or modified for the generation, command and control, or delivery of “intrusion software”, and components of those systems or equipment that are themselves specially designed or modified to have these capabilities.
- 4D004 : “Software” specially designed or modified for the generation, command and control, or delivery of “intrusion software”.
- 4E001.c : “Technology” for the “development" of “intrusion software”.
  ***Note**: 4E001.c does not apply to “vulnerability disclosure” or to “cyber incident response”*
- 4D001.a (for 4A005 or 4D004) : “Software” specially designed or modified for the “development” or “production” of items controlled by ECCN 4A005 or 4D004.
- 4E001.a : “Technology” (which may include “source code”) for the “development”, “production” or “use” of items controlled by ECCN 4A005, 4D004 or 4D001.a (for 4A005 or 4D004).
  ***Note**: 4E001.a does not apply to “vulnerability disclosure” or to “cyber incident response”*

Meanwhile, the Category 5 – Part 1 ‘cybersecurity items’ related to IP network communications surveillance are identified by the following ECCNs, summarized as follows:

- 5A001.j : Systems and equipment specially designed or modified to have all (not just some) of the functional characteristics and technical capabilities listed in ECCN sub-paragraphs j.1 (5A001.j.1.a., .b, .c) and j.2 (5A001.j.2.a, .b), and components of those systems or equipment that are themselves specially designed or modified to have all these characteristics.
- 5B001.a (for 5A001.j) : Test, inspection and production equipment specially designed for the “development” or “production” of items controlled by ECCN 5A001.j, and components or accessories (of the test, inspection and production equipment) that are themselves specially designed or modified as such.
- 5D001.a (for 5A001.j) : “Software” specially designed or modified for the “development”, “production” or “use” of items controlled by ECCN 5A001.j.
- 5D001.c. (for 5A001.j or 5B001.a (for 5A001.j)) : “Software” specially designed or modified to provide characteristics, functions or features of items controlled by ECCN 5A001.j or 5B001.a (for 5A001.j).
- 5E001.a (for 5A001.j or 5D001.a (for 5A001.j)) : “Technology” (which may include “source code”) for the “development”, “production” or “use” (beyond mere operation) of items controlled by ECCN 5A001.j or 5D001.a (for 5A001.j).

4. **Are ‘publicly available’ software and technology related to “intrusion software”, subject to the EAR?**

   Answer: No. “Software” and “technology” that are ‘publicly available’ are not subject to the EAR. For more information on ‘publicly available’ technology or software, including what it means for “software” or “technology to be considered “published” or the result of “fundamental research”, see sections 734.7 through 734.11 to part 734 of the EAR.

5. **Are non-published, machine-executable exploits (and other forms of proprietary “intrusion software”) ‘cybersecurity items’ for purposes of the EAR?**

Answer: No. The Wassenaar Arrangement (WA) decisions related to "intrusion software" do not place exploits (sometimes referred to as 'payload') within the control scope of ECCN 4D004.

In real-world situations, 'payload' delivered onto a targeted computer or other network-capable device may simultaneously meet the definition of "intrusion software" (classified EAR99) while also having the *command and control* characteristics of "software" classified ECCN 4D004. Such software that both meets the definition of "intrusion software", and is also designed to generate, command and control, or deliver other "intrusion software", is considered "intrusion software" for purposes of the EAR.

If the exploits are designed for military offensive cyberspace operations as defined in the U.S. Munitions List, the U.S. Munitions List takes precedence over dual-use controls.

6. **I have, or have access to, specialized *knowledge* about exploits (and other forms of "intrusion software") that is not "published". Is that "technology" a 'cybersecurity item'?**

   Answer: If that knowledge meets the definition of "technology" for the "development" of "intrusion software" (as those terms are defined in Section 772 of the EAR), it would be a 'cybersecurity item'. However, 4E001.c allows the export of such knowledge for "vulnerability disclosure" and "cyber incident response" activities without control, meaning License Exception ACE would not need to be relied upon. In those qualified circumstances, "technology" that would otherwise be classified ECCN 4E001.c (or 4E001.a) is classified EAR99 for purposes of the EAR.

7. **License Exception ACE has certain restrictions related to 'government end users' of countries listed in Country Group D:1, D:2, D:3, D:4 or D:5. What is this definition of 'government end users' applicable to 'cybersecurity items' and License Exception ACE, and where do I find it in the EAR?**

   Answer: For the purposes of License Exception ACE and the licensing of 'cybersecurity items' subject to the EAR, 'government end- user' means "*a national, regional or local department, agency or entity that provides any governmental function or service, including international governmental organizations, government operated research institutions, and entities and individuals who are acting on behalf of such an entity. This term does not include retail or wholesale firms not engaged in the manufacture, distribution, or provision of items or services, controlled on the Wassenaar Arrangement Munitions List.*"

   This definition is found in License Exception ACE, section 740.22 of the EAR, Technical Note 3 to paragraph (c)(1).

8. **When can I export 'cybersecurity items' without needing to apply for a license?**

   Answer: Unless a license requirement is triggered for some other reason (e.g., "Red Flags", Entity List, embargoes/sanctions, etc.), situations where a license is not required include the following:

   - Items not subject to the EAR, such as "published" technology or software. *(See Answer #4)*
   - "Intrusion software" -- *not a 'cybersecurity item'. (See Answers #3, #5)*
   - "Technology" items excluded from the scope of ECCN 4E001.a and 4E001.c -- *not a 'cybersecurity item'. (See Answers #3, #6)*

- "Encryption items" classified under ECCN 5A002, 5A004, 5D002 or 5E002 -- *these are not 'cybersecurity items'. (See Answers #21, 22, 23)* Note, however, these items may require a license for encryption reasons in Category 5 – Part 2 *(See sections 742.15 and 740.17 of the EAR)*.
- "Tools of Trade". *(See License Exception TMP, section 740.9(a)(1) and License Exception BAG, section 740.14(b)(4) of the EAR)*
- Exports, reexports, and transfers (in-country) made by or consigned to a department or agency of the U.S. Government, or made for or on behalf of a department or agency of the U.S. Government. *(See License Exception GOV, section 740.11(b) of the EAR)*
- Exports, reexports and transfers (in-country) broadly authorized by License Exception ACE as follows, to destinations other than Country Group E:1 or E:2:

    - To 'favorable treatment cybersecurity end users':
        - ❖ "U.S. subsidiaries";
        - ❖ Providers of banking and other financial services;
        - ❖ Insurance companies;
        - ❖ Civil health and medical institutions providing medical treatment or otherwise conducting the practice of medicine, including medical research.
    - To non-'government end users' NOT located in a Country Group D:1 or D:5 country.
    - To qualifying "vulnerability disclosure" or "cyber incident response" non-'government end users', located in a Country Group D:1 or D:5 country. *(See also Answers #15, 16, 17, 25)*
    - To 'government end users' NOT of a Country Group D:1, D:2, D:3, D:4 or D:5 country.

      (See Supplement No. 1 to part 740 of the EAR for the Country Groups, License Exception ACE for the applicable 'government end user' definition)

  Note: License Exception ACE is NOT available whenever "The exporter, reexporter or transferor (in-country) knows or has reason to know at the time of export, reexport or transfer (in-country), including deemed exports and reexports, that the cybersecurity item will be used to affect the confidentiality, integrity or availability of information or information systems, without authorization by the owner, operator or administrator of the information system (including the information and processes within such systems)." *(See section 740.22(c)(2) of the EAR)*

9. What are some situations where License Exception ACE does not authorize the export, reexport or transfer (in-country) of 'cybersecurity items'?

Answer: In addition to when the use of the license exception may be disallowed for some other reason (e.g., "Red Flags", Entity List, embargoes/sanctions, etc.), License Exception ACE is not available in the following circumstances:

- To any Country Group E:1 or E:2 country or end user, including deemed exports and reexports. *(See section 740.22(c)(1)(i) of the EAR)*
- To any 'government end -user' of any country listed in Country Group D:1, D:2, D:3, D:4 or D:5, generally speaking. *(See section 740.22(c)(1)(ii) of the EAR)*

__Note__: See the Notes to section 740.22(c)(1)(ii) for the availability of License Exception ACE regarding exports of certain items to 'government end-users' in Country Group D countries that are also listed in Country Group A:6.

- To non-'government end users' located in a D:1 or D:5 country, that are not authorized for purposes of "vulnerability disclosure" or "cyber incident response". *(See section 740.22(c)(1)(iii) of the EAR, and below FAQ Answers #15, 16, 17)*
- Whenever "The exporter, reexporter or transferor (in-country) knows or has reason to know at the time of export, reexport or transfer (in-country), including deemed exports and reexports, that the cybersecurity item will be used to affect the confidentiality, integrity or availability of information or information systems, without authorization by the owner, operator or administrator of the information system (including the information and processes within such systems)." *(See section 740.22(c)(2) of the EAR and the __Note__ to Answer #8 above)*

10. How would the proposed rule affect software used by multinational companies that monitor their overseas networks?

Answer: Under the proposed rule, only certain exports of specified systems, equipment, components or software that would generate, command and control, or deliver "intrusion software" would require an export license *(See Answers #1, 8)*. For example, License Exception ACE covers intra-company transfers or internal use in any non-embargoed destination by any company headquartered in the United States, or by other non-'government end users' (as that term is defined and applied under the proposed rule) not located in a Country Group D:1 or D:5 country, and for any permitted 'vulnerability disclosure' or 'cyber incident response' use in D:1 or D:5 countries by non-'government end users' – including the prevention and remediation of cybersecurity incidents.

11. Will companies be required to share their zero-day exploits with the government in order to get a license?

Answer: Exploits that meet the definition of "intrusion software" are not controlled, and information pertaining to the discovery of a vulnerability is also not controlled. Therefore, BIS would not request a company to share the technical details of any exploitable vulnerability, zero-day or otherwise.

12. Doesn't the rule potentially criminalize hacking?

Answer: No. The rule would control the export of delivery or command and control tools (hardware and software), as well as the export of technical data for developing exploits ("intrusion software"). The rule as proposed would not control the "release" or other export of exploits to a computer or other information system outside the United States, since "intrusion software" would not be controlled. Also, the Export Administration Regulations (EAR) do not control services, only the export of commodities, software and technology. Thus, "hacking", as that term is generally understood, does not fall under the jurisdiction of the EAR, except to the extent there is an associated export of controlled hardware, software, or technical data.

13. Mobile phone jailbreaking tools include platforms for delivering intrusion software to the phone. These generally include fully operational exploits including the delivery code. Does this rule make it illegal to jailbreak a phone? Are such tools subject to control?

This response divides the question into two parts:

Does this regulation make it illegal to jailbreak a phone?
Answer: No. The Commerce regulation controls exports of certain software, and downloading jailbreaking software to a computer within the United States and using it to jailbreak a phone does not involve an export of software. The proposed rule does not limit the ability of owners to modify their devices.

What if the jailbreak software includes a platform for delivering intrusion software to the phone -- is the jailbreak software subject to control?
Answer: If particular jailbreak software did meet all the requirements for classification under ECCN 4D004 (such as a commercially sold delivery tool "specially designed" to deliver jailbreaking exploits) then it would be subject to control and a license would be required to export it from the United States in situations where License Exception ACE does not apply. Note that if such software were "publicly available," it would not be subject to the Export Administration Regulations.

"Vulnerability Disclosure" and "Cyber Incident Response"

14. What are the definitions of "vulnerability disclosure" and "cyber incident response" relevant to 'cybersecurity items' and License Exception ACE, and where do I find them in the EAR?

Answer: "Vulnerability disclosure" and "cyber incident response" are qualified exclusions, the application of which depends on the end use and the end user. For purposes of the EAR:

- "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.
- "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.

In each definition,

- The eligible end users are "*individuals or organizations responsible for conducting or coordinating remediation…*"
- The eligible end use spans the entire "*process of…*":
  - "*Identifying, reporting, or communicating a vulnerability to, or analyzing a vulnerability*" with the eligible end users. ("vulnerability disclosure")
  - "*Exchanging necessary information on a cybersecurity incident*" with the eligible end users. ("cyber incident response")

These definitions are found in section 772.1 of the EAR.

15. What are some examples of "*individuals or organizations responsible for conducting or coordinating remediation*"?

Answer: For the 'cybersecurity items' purposes of the EAR, the following are a few examples of the many types of "individuals or organizations responsible for…" who, consistent with other provisions of the EAR, may qualify under the definitions of "vulnerability disclosure" and/or "cyber incident response":

- IT network systems administrators and chief information officer (CIO) / chief information security officer (CISO) staff
- 'Bug bounty' organizations and organizers
- Computer Security Incident Response teams (CSIRTs) / Computer Emergency Readiness teams (CERTs), enterprise Security Operations Centers (SOCs)
- Enterprise 'Blue Teams' and 'Purple Teams'
- Commercial Product Development groups, software developers, hardware engineers, etc.
- Information System Security Officers (ISSOs) / Information System Security Managers (ISSMs)
- Cybersecurity standards organizations

16. **When can I export 'cybersecurity items' pursuant to "vulnerability disclosure" or "cyber incident response" without needing to apply for a license?**

    Answer: In addition to <u>all the situations</u> previously addressed where licenses are generally not required *(see Answers #4, 5, 6, 8)*, License Exception ACE authorizes the export of 'cybersecurity items' to all non-'government end users' located in any country not listed in Country Group E:1 or E:2 for "vulnerability disclosure" or "cyber incident response" *(See Answer #15)*, unless the general restrictions of section 740.22(c)(2) apply *("The exporter, reexporter or transferor (in-country) knows or has reason to know …")*. *(See Answers #8, 9)*

    Exports to 'government end-users' in Country Group D:1, D:2, D:3, D:4, and D:5 require a license even if the export is for "vulnerability disclosure" or "cyber incident response".

17. **Are there situations where the processes of "vulnerability disclosure" or "cyber incident response" may involve the "release" (or other "export") of "technology" or "software", including source code, related to "intrusion software"?**

    Answer: Absolutely. It is not uncommon for "individuals and organizations responsible for" remediating cyber vulnerabilities or cyber incidents to exchange "software" and "technology", including technical data and source code, related to malicious network penetrations, system intrusions, and other exploits of software 'bugs' or other system or network vulnerabilities. In fact, the rapid sharing of this information and software by and among responsible persons is a vital aspect of cooperative U.S. and global efforts to secure the Internet and identify, triage, mitigate and otherwise address broad ranges of cybersecurity vulnerabilities and incidents.

    Accordingly, in addition to implementing the Wassenaar Arrangement (WA) exclusions for "vulnerability disclosure" or "cyber incident response" involving "technology" otherwise classified under ECCN 4E001.a or 4E001.c, this rule provides License Exception ACE authorizations for the export of ECCN 4A005 hardware and 4D004 "software" for "vulnerability disclosure" or "cyber incident response", except to Country Group E:1 or E:2 countries or to section 740.22 'government end users' of Country Group D:1, D:2, D:3, D:4 or D:5 countries.

These exclusions and license exceptions, in tandem with EAR licensing requirements where the application of such a license exception runs contrary to U.S. national security and foreign policy interests, reflect the United States' commitment to safeguard the Internet, protect the U.S. Critical Infrastructure, promote cyber hygiene, and defend the interests of the American people at home and abroad.

18. Do I need a license for training someone if the training involves the release of cybersecurity items?

Answer: Information provided as part of a catalogue course open to the general public is not subject to the EAR under Section 734.3. Thus university and other courses that are teaching penetration testing and network security as part of a catalogue course would not need a license for such activity.

Outside of Section 734.3, the exclusion for "vulnerability disclosure" and "cyber incident response" may apply to certain training situations when the training is for purposes of fixing vulnerabilities so they cannot be exploited, or otherwise keeping malicious cyber incidents from happening and remediating them when they do occur. Accordingly, these exclusions do apply to many training (and training-related) activities involving the "release" or other export, reexport or transfer of 'cybersecurity items' subject to the EAR (e.g., when the 'cybersecurity items' information or "software" are not otherwise excluded from the EAR by section 734.3(b)(3)).

For example, exporting or transferring 'cybersecurity items' for purposes of Red/Blue/Purple team instruction and exercises conducted in order to identify and remedy exploitable vulnerabilities, or practice responding to cyber incidents, could fall under these exclusions.

On the other hand, exporting or transferring 'cybersecurity items' subject to the EAR for purposes of training a foreign entity in exploiting a particular vulnerability, or defeating some "cyber incident response", with intent to aid in the conduct of offensive cyber operations would not fall under license exception ACE or the exclusions for "vulnerability disclosure" or "cyber incident response."

Noting, in order to qualify for these particular 'cybersecurity items' exclusions, all of their requirements must be met. Factors that help determine the applicability of the "vulnerability disclosure" or "cyber incident response" exclusion to a particular export situation, include but are not limited to, the following:

- Who is receiving the training?
- Why are they being trained?
- What is being released or conveyed?
- What will the recipients of this training do with the information and software they receive?

19. Would prior BIS authorization be required for a researcher to privately disclose an exploit to a vendor outside the U.S. with the understanding that the information would NOT be published?

Answer: No. As previously explained, the exploit itself is not described in the new control list entries. For this question, a vulnerability is a weakness in a vendor's software or hardware. Exploit code could be written to take advantage of the vulnerability or to prove that the vulnerability can be exploited. The exploit code itself may be considered "intrusion software." Neither the disclosure of the vulnerability nor the disclosure of the exploit code would be controlled under the proposed rule.

Moreover, although information for the development of "intrusion software" that may accompany the disclosure of the exploit may be described in the proposed new ECCN 4E001.c "technology" control, this information about the exploit is also not controlled when shared with the vendor under a "vulnerability disclosure" arrangement for purposes of resolving the vulnerability.

20. **I am a cybersecurity professional chiefly responsible for my organization's "cyber incident response" activities. In that capacity, I have been asked to help train and equip the cyber defenders / cybersecurity incident responders (e.g., "Blue Team" and SOC/CSIRT personnel) of a corporate partner of ours, that is headquartered and located in a Country Group D:1 country.**

    In planning for this event, I am informed by my corporate partner that a few Government officials of that D: 1 country have been invited to the event, and it is anticipated that these officials may be accompanied by select technical experts who are known to provide consulting services to that Government.

    Is a license required for me to provide this training, and release information and "software" classified under one or more of the 'cybersecurity items' ECCNs related to "intrusion software" to these various participants?

    Answer: Yes. The "release" and other "export" of 'cybersecurity items', relevant to "cyber incident response", to the "Blue Team" and other cybersecurity incident response staff of the non-'government end user' corporate partner of the U.S. company would be authorized under License Exception ACE. However, the expected presence of Country Group D:1 Government officials ('government end users') and D:1 foreign nationals performing technical consulting services on behalf of that Government (also 'government end users') indicates that a "release" or other "export" of controlled 'cybersecurity items' may occur that would trigger an EAR license requirement not satisfied by License Exception ACE.

Penetration testing tools and other 'cybersecurity items' overlap with Category 5 - Part 2 'encryption items'

21. **My company produces and exports commercial penetration testing (pen testing) software that commands and controls "intrusion software". We have a CCATS that classifies our product as 5D002 and makes it eligible for License Exception ENC §740.17(b)(2)(i)(F). Does this rule re-classify our encryption product as a 'cybersecurity item' classified under ECCN 4D004?**

    Answer: This rule does not change the classification (ECCN) of any product (hardware or software) classified under ECCN 5A002, 5A004 or 5D002 in CCL Category 5 – Part 2 ("Information Security"), where the cryptographic and/or cryptanalytic capability is present, activated or otherwise usable. These items continue to be controlled in Category 5 – Part 2 for national security (NS) and encryption items (EI) reasons, having licensing policy as set forth in section 742.15 of the EAR and eligible for certain license exceptions including ENC, section 740.17 of the EAR.

22. **What are some examples of ECCN 5D002 pen testing software encryption capabilities?**

Answer: "Red Team exercises" and other uses of penetration testing software seek to emulate, under real-world conditions, an adversarial attack against an enterprise's information systems.

In fact, much pen testing software is specially designed to *deliver* and *command and control* "intrusion software", which are key aspects of the new ECCN 4D004. However, when that 'delivery' or 'command and control' functionality does not implement "cryptography" (i.e., is not encrypted or decrypted), the pen testing software is not controlled under ECCN 5D002.

In terms of encryption capability, commercial penetration testing software designed or modified to perform cryptanalytic functions (e.g., password cracking, security protocol spoofing) is classified ECCN 5D002.c.3.a. Pen testing software that do not have such cryptanalytic capabilities may typically employ a range of cryptographic data confidentiality capabilities (e.g., 128- or 256-bit Advanced Encryption Standard (AES) file and data encryption) that results in these items being classified under ECCN 5D002.c.1. These longstanding encryption controls pre-date the new controls specific to "intrusion software".

23. Does this mean that pen testing "software" and "technology" that include cryptographic or cryptanalytic functionality are always 'encryption items' classified in Category 5 – Part 2, and never 'cybersecurity items' classified in Category 4 for purposes of the EAR?

Answer: No, because of their capabilities related to "intrusion software", there are certainly circumstances where the 'cybersecurity items' ECCNs of Category 4, and the License Exception provisions of EAR § 740.22 Authorized Cybersecurity Exports (ACE), will apply to penetration testing "software" and "technology".

Generally speaking, whenever a product is no longer controlled under ECCN 5A002, 5A004 or 5D002 (e.g., because its controlled "information security" functionality has been removed or securely disabled by the manufacturer), or where a particular transaction subject to the EAR involves source code or other "software" or "technology" for the product's "intrusion software" capability unrelated to its encryption functionality, one or more 'cybersecurity items' ECCNs may then apply.

For example, "software" specially designed for the command and control of "intrusion software" is classified under ECCN 4D004 if it does not implement ECCN 5D002 encryption capability, or if its 5D002 encryption capability can only be made usable by means of secure "cryptographic activation" but has not yet been activated.

24. If I have 5D002 pen testing "software", would I ever have 4E001 "technology"?

Answer: For "technology", ECCN 5E002.a applies to the "development", "production" or "use" of the encryption, decryption or cryptanalytic functionality in the item, while 4E001.a would apply to the item's 4D004 functionality (e.g., its ability to command and control "intrusion software") and 4E001.c would apply to the "development" of "intrusion software" itself.

For source code, those portions of the source code that include the cryptographic or cryptanalytic functions would be classified in Category 5 – Part 2, but other parts of the source code, when exported separately from its cryptographic or cryptanalytic features, could fall under 4D001 or 4E001.

Thus, if I am a developer or producer of 5D002 pen testing "software" my inventory of items subject to the EAR could include source code and "technology" controlled in Category 4.

25. Can 'cybersecurity items' software classified under ECCN 4D004 (whether characterized as a 'pen testing' tool, or not) be "released" or otherwise exported under License Exception ACE to all non-'government end users' of a Country Group D:1 or D:5 country under the "vulnerability disclosure" and "cyber incident response" exclusion Note 2 to paragraph (c)(1)(iii), section 740.22, if the intended end use is to help the customer increase its cybersecurity expertise or otherwise improve its IT security posture?

Answer: No, the ecosystem of non-'government end users' in any country invariably includes a great number of persons, companies, enterprises and other organizations that are not "individuals or organizations responsible for…" "vulnerability disclosure" or "cyber incident response". Furthermore, not every "release" or other "export" of "software" or "technology" is germane to the "process of" those cybersecurity disciplines.

For export situations involving sending (or sharing) 'cybersecurity items' to non-'government end users' of Country Group D:1 or D:5 countries, when one or more of the license exception eligibility requirements of the "vulnerability disclosure" or "cyber incident response" exclusions are not met, a license review by BIS and other relevant departments and agencies of the U.S. Government is needed to ensure such exports are consistent with the national security and foreign policy interests of the United States.

26. I am a trained commercial cybersecurity professional, skilled in performing penetration tests and leading "Red Team" and "Purple Team" exercises for corporate and government clients. For my overseas clients, I sometimes run 'pen test' software remotely from a server in the U.S., sometimes I run 'pen test' software on the client's IT assets (including such software that I might create 'on the fly' during the exercise), and other times I take such software with me on my laptop when I travel to and from my client locations. Do these scenarios subject me to a license requirement?

Answer: Not necessarily. In the first scenario, in order to be subject to a potential licensing requirement, the transaction must be an "export" as defined in Section 734 of the EAR. Running pen testing software from a server in the U.S. is not an "export" subject to the EAR. Thus running software remotely from a server in the U.S. would not trigger any licensing requirements.

For the second scenario, merely running software programs or executing scripts on a machine located overseas (whether remotely or when physically on-premises) does not necessarily constitute the "release" or "export" of that software subject to the EAR, and merely operating software tools related to "intrusion software" for legitimate cybersecurity purposes does not necessarily suggest or infer that any "export" of 'cybersecurity items' subject to the EAR has, or will, occur. However, if such items were exported and downloaded on the client's network prior to being used, that export could be subject to a license requirement.

For the third scenario, taking pen testing software on a laptop while temporarily overseas at a client location would be eligible for License Exception TMP Tools of Trade (section 740.9(a)(1) of the EAR) to all countries not located in Country Group E:1, assuming the exporter can meet the other provisions of that license exception. If the exporter can meet all the provisions of 740.9(a)(1), a license would not be required.

27. **Assuming at least one of the scenarios in question #26 above does involve an export of a 'cybersecurity item', are those exports released by the carve outs for "vulnerability disclosure' and "cyber incident response"?**

    Answer: In some cases, penetration testing activities and "Red Team" and "Purple Team" exercises could involve exports for "vulnerability disclosure" and "cyber incident response". For example, suppose if, as a result of pen testing or other technical activities undertaken in response to a cybersecurity incident, you discover digital artifacts or other information revealing 4E001.c "development" "technology" pertaining to "intrusion software". Releasing that information to the client so they can take steps to remediate that vulnerability could meet the definition of "vulnerability disclosure" and not require a license. Whether a particular export involving penetration testing or "Red Team" and "Purple Team" exercises meets those definitions depends on the particular facts of the scenario.

28. **I am planning to export penetration testing software, with and without encryption, to a Country Group D:1, D:2, D:3, D:4 or D:5 end user who is not eligible to receive that product under License Exceptions ENC or ACE. When I submit my license application, should I list the software under both ECCNs 4D004 and 5D002?**

    Answer: Yes, BIS anticipates that certain penetration testing situations (e.g., "Red Team" exercises) may involve some "software" classified under ECCN 4D004 (without encryption) and some "software" classified under ECCN 5D002 (with encryption).

    For example, when the end user meets the definition of "more sensitive government end users (as applied to encryption items)" and 'government end users' (as applied to 'cybersecurity items'), such as a Country Group D:1, D:2, D:3, D:4 or D:5 defense, intelligence or state security end user, the export of either type of "software" (with or without encryption) would not be authorized under License Exception ENC (for the 5D002 encryption software) or License Exception ACE (for the 4D004 cybersecurity software).

    Hence, a license is required to send the ECCN 4D004 'cybersecurity items' and the ECCN 5D002 'encryption items' to this customer abroad.

    As with any license application, the applicant should separately list and detail all items for which the license authorization is sought, and include the information required by Supplement No. 1 to part 748 of the EAR to describe each item (to include ECCN, Model Number, CCATS Number (as applicable), Quantity, Units, Unit Price, Total Price, Manufacturer (if different from the applicant), Technical Description).

    Failure to include all relevant information may cause your license application to be held without action or returned without action, including (for encryption items) if the encryption CCATS-related information on file with BIS and the ENC Encryption Request Coordinator is not current or has otherwise changed since the item was last reviewed for reasons of its encryption items (EI) control.

29. **There is a lot of discussion of penetration testing products in another FAQ. Is that to say that all penetration testing products would fit the definition of "intrusion software"?**

Answer: Some penetration testing products meet the description of systems, equipment or software "specially designed" or modified for the generation, operation or delivery of, or communication with, "intrusion software" set forth in proposed ECCNs 4A005 and 4D004. The tools that meet the entry are ones that are "specially designed" or modified to launch exploits or other malware that meet the definition of "intrusion software" – including extracting or modifying data on the system.

However, there are some tools that are used in penetration testing that are not caught by the entries because they do not do the things described in the definition. For example, tools such as port scanners, packet sniffers and protocol analyzers would not be controlled. A penetration testing tool not designed to avoid detection by 'monitoring tools' would not be controlled. Also, a vulnerability scanner, which just finds vulnerabilities in a system without actually exploiting them and extracting data, would not be captured by the proposed rule.