Encryption FAQs

Source: https://www.bis.doc.gov/index.php/policy-guidance/encryption/6-faqs

1. Who is required to submit a classification request or self-classification report?

> Any party who exports certain U.S.-origin encryption products may be required to submit a classification request and/or self-classification report; however, if a manufacturer has self-classified relevant items and/or had items classified by BIS, and has made the classifications available to other parties such as resellers and other exporters/reexporters, such other parties are not required to submit a classification request or to submit an annual self-classification report.

2. What are my responsibilities for exporting or reexporting encryption products where I am not the product manufacturer?

> Exporters or reexporters that are not producers of the encryption items can rely on the self-classification or CCATS that is published by the producer when exporting or reexporting the classified encryption item. Separate commodity classification request or self-classification report to BIS is NOT required.

3. What should I do if I cannot obtain the Export Control Classification Number (ECCN) for the item from the producer or manufacturer?

> If you are not the producer and are unable to obtain the producer's information or if the producer has not submitted a self-classification report or commodity classification for his/her products to BIS, then you are responsible for properly classifying the item and obtaining the proper authorization. This may require you to submit a self-classification report or classification request.

4. I'm a developer of an item that incorporates encryption. If I am incorporating someone else's encryption into my product, does the classification for their encryption item cover the product I am developing?

> No. The classification of your item does not depend on the classification of the encryption you are incorporating. Your product should be classified separately as a standalone item.

5. Once I get a classification from BIS, when is a new classification required?

> Only items listed in 740.17(b)(2) and (b)(3) require a classification. For those items, a new classification is required when the cryptographic functionality changes or other technical characteristics affecting license exception ENC eligibility – e.g., encrypted throughput. New classifications are not required for other changes, including patches, upgrades or releases, name changes. Items described in 740.17(b)(1) do not require a classification to be eligible for ENC.

6. Is Supplement No. 6 to part 742 required for paragraph 740.17(b)(1) authorization?

> If you are requesting a classification of an item described in paragraph 740.(b)(2) or (b)(3), then a classification request is required. If you are requesting a classification of an item described in paragraph 740.17(b)(1) (in other words, the item is not described in either Section 740.17(b)(2)

or (b)(3)), a Supplement No. 6 questionnaire is not required as a supporting document. Provide sufficient information about the item (e.g., technical data sheet and/or other explanation in a separate letter of explanation) for BIS to determine that the item is described in paragraph 740.17(b)(1). If you are not sure that your product is authorized as 740.17(b)(1) and you want BIS to confirm that it is authorized under 740.17(b)(1), providing answers to the questions set forth in Supplement No. 6 to part 742 with your request should provide BIS with sufficient information to make this determination.

7. ECCNs 5A992/5D992.a and b, and 5E992.a have been eliminated from the Commerce Control List. What if I already have a CCATS issued under one of these eliminated ECCNs?

Classifications issued for ECCNs 5A992/5D992.a and b, and 5E002.a prior to the elimination of these ECCNs may now be classified elsewhere (e.g., 5A991) if applicable or designated EAR99. A new CCATS is not required.

8. What happens to Mass Market encryption authorizations filed prior to the updated regulation of Sept. 20, 2016?

Mass market encryption authorizations issued under 742.15(b)(1) or (b)(3) prior to the September 20, 2016 rule change, continue to be authorized under the mass market provisions found in 740.17(b)(1) and (b)(3), respectively. A new classification is NOT required merely because the provision moved from 742.15 to 740.17.

9. Does the EAR definition of "OAM" include using encryption in performing network security monitoring functions?

No. The definition of "OAM" includes "monitoring or managing the operation condition or performance of an item." BIS does not consider network security monitoring or network forensics functions to be part of monitoring or managing operation condition or performance.

The phrase "monitoring or managing the operating condition or performance of an item" is meant to include all the activities associated with keeping a computer or network-capable device in proper operating condition, including: configuring the item; checking or updating its software; monitoring device error or fault indicators; testing, diagnosing or troubleshooting the item; measuring bandwidth, speed, available storage (e.g. free disk space) and processor/memory/power utilization; logging uptime/downtime; and capturing or measuring quality of service (QoS) indicators and Service Level Agreement-related data.

However, the "OAM" definition does not apply to cryptographic functions performed on the forwarding or data plane, such as: decrypting network traffic to reveal or analyze content (e.g., activity signatures, indicators or event data extracted from monitored network traffic) over the forwarding plane; or securing the re-transmission of captured network activity.

Thus, products that use encryption for such network security monitoring or forensics operations, or to provision these cryptographic services, would not be released by the OAM decontrol notes (l) or (m), or the Note to 5D002.c.

Created by: EA/NSTTC/ITCD
Published Date: March 2017
Last Updated:

Similarly, the "OAM" decontrol does not apply to security operations directed against data traversing the network, such as capturing, profiling, tracking or mapping potentially malicious network activity, or "hacking back" against such activity.

10. What happens to old ELAs where the end user is now eligible for ENC?

Prior to the September 20, 2016 updates, licenses were required to "government end users" outside the countries listed in Supplement No. 3 to part 740. Now, "less sensitive government end users" worldwide (except to AT-controlled countries) are eligible for ENC. Licenses previously submitted for these end users who are now eligible for ENC may use ENC without any further submissions to BIS. These exports were subject to a semi-annual sales reporting license condition. The semi-annual sales report still remains for these exports per 740.17(e) of ENC.

11. Why was the grandfathering provisions removed?

The grandfathering provision is no longer required. The September 20, 2016 rule eliminated requirements for the encryption registration and self-classification report when the exporter has obtained a CCATS from BIS for the item. As a result, CCATS issued prior to June 25, 2010 are still valid without submission of an encryption registration or self-classification report unless the encryption functionality of the item changes.

12. Are universities with research institutes on the less- or more sensitive government end user list?

Universities are "less-sensitive government end users" while government research institutes are "more sensitive government end users." If a university has a government research institute, BIS considers exports to the university itself to be an export to a "less-sensitive government end user." Exports directly to a government research institute within the university, for use by a government research institute within the university, would be considered an export to a "more sensitive government end user." If you are unsure about how a particular transaction should be treated, please seek guidance from BIS.

13. Does Decontrol Note (j) cover Single Board Computers (SBC)?

Yes, Note (j) part 2.a and b can apply to single board computers (SBC) where the cryptography is integral to (within) a mass market (Note 3 to Category 5 Part 2) processor on the SBC (e.g., processor with hardware accelerated encryption primitives); or integral to (within) an operating system that is not in 5D002 (e.g., mass market OS).

Part 2.c of the Decontrol note (j) makes reference to OAM. See #8 above for OAM.

14. What happened to old Note (g) for dormant encryption?

Before the Wassenaar 2016 rule, Note (g) to 5A002.a released products where the encryption functionality could not be used or could only be made useable by "cryptographic activation." This decontrol note has been moved to 5A002.a and stated in a more positive manner. It now says that 5A002.a controls products "where that cryptographic capability is usable without "cryptographic activation" or has been activated." This change does not impact the scope of what was released under Note (g).

Created by: EA/NSTTC/ITCD
Published Date: March 2017
Last Updated:

15. What happened to Note 4 to Category 5 Part 2?

Similar to the dormant encryption decontrol note, Note 4 was moved to 5A002.a and stated in a positive manner. Instead of saying what is not controlled in Category 5 Part 2, 5A002.a now specifies that, to be controlled, the item must have "information security" as a primary function, it must be a digital communications or networking system, or it must be a computer or have information storage or processing as a primary function. This change does not impact the scope of Note 4.

16. I have a previous classification under 5A002.a.1, but now, 5A002.a.1 applies to items that have "information security" as a primary function. Do I need to get a new classification?

No. ECCN 5A002 was restructured in 2017 for readability. Because of the change in structure to 5A002.a, BIS is now issuing classifications under 5A002.a instead of 5A002.a.1. Previous classifications issued under 5A002.a.1 remain valid under the new structure. Those classifications can be understood to be under 5A002.a now.

Created by: EA/NSTTC/ITCD
Published Date: March 2017
Last Updated: