

CHECKLIST ON ENCRYPTION AND OTHER “INFORMATION SECURITY” FUNCTIONS¹

See [Instruction Sheet](#)

1. Does your product perform "cryptography", or otherwise contain any parts or components that are capable of performing any of the following "information security" functions?
(Mark with an "X" all that apply)
 - a. encryption
 - b. decryption only (no encryption)
 - c. key management / public key infrastructure (PKI)
 - d. authentication (e.g., password protection, digital signatures)
 - e. copy protection
 - f. anti-virus protection
 - g. other (please explain) : _____
 - h. NONE / NOT APPLICABLE
2. For items with encryption, decryption and/or key management functions (1.a,1.b, 1.c above):
 - a. What symmetric algorithms and key lengths (e.g., 56-bit DES, 112 / 168-bit Triple-DES, 128 / 256-bit AES / Rijndael) are implemented or supported?
 - b. What asymmetric algorithms and key lengths (e.g., 512-bit RSA / Diffie-Hellman, 1024 / 2048-bit RSA / Diffie-Hellman) are implemented or supported?
 - c. What encryption protocols (e.g., SSL, SSH, IPSEC or PKCS standards) are implemented or supported?
 - d. What type of data is encrypted?
3. For products that contain an "encryption component", component be easily used by another product, or else accessed by the end-user for cryptographic use?

If you answered “Yes” to any of the questions above,
please contact Deborah Cole at 277-2257 or export@unm.edu
for an Export Control review of the project.

¹ Copied from BIS website with permission, <http://www.bis.doc.gov/encryption/checklistinstr.htm>, where more information on licensing and exemptions can be found.

CHECKLIST ON ENCRYPTION AND OTHER “INFORMATION SECURITY” FUNCTIONS INSTRUCTION SHEET1

1. WHAT IS THE “CHECKLIST”?

Supplement No. 5 to part 742 provides a basic "[checklist](#)"[pdf] on encryption and other "information security" functions. Written in question and answer format, this introductory working aid is designed to help exporters evaluate whether their products are subject to encryption review or notification requirements. If a review or notification is required, then exporters will need to complete [Supplement No. 6](#) [pdf] to part 742 and follow the appropriate instructions for submitting this "Supp. 6" technical information to BIS (and the ENC Encryption Request Coordinator - Ft. Meade, MD).

2. AM I REQUIRED TO COMPLETE THE “CHECKLIST”?

No. Exporters are not required to complete the "checklist". It is simply a working aid that is provided to help exporters more fully consider and identify controlled encryption and "information security" components within their products, when making classification decisions and assessing whether an encryption review by BIS is required.

3. WHO MIGHT WANT TO COMPLETE THE “CHECKLIST”?

Exporters of products with a limited set of encryption functions (as well as exporters who are not sure if their products even contain encryption) may especially wish to consider completing Supplement No. 5 to part 742 before proceeding to Supplement No. 6.

4. HOW MIGHT COMPLETING THE “CHECKLIST” BENEFIT ME OR MY COMPANY?

The "checklist" covers some (but not all) of the topics that are fundamental to most review requests involving encryption, through a much more basic set of questions than are found in Supplement No. 6 to part 742. Should you find that you must submit an encryption review request or notification for your product(s), any insights you gain from having gone through the "checklist" will save you time when you answer the more detailed questions of Supplement No. 6 to part 742. Therefore, depending upon your situation, completing the "checklist" may be a helpful first step towards determining whether you must submit an encryption review request for your item.

5. WHERE DO I GET THE “CHECKLIST”?

[The checklist](#) [pdf] is published in Supplement No. 5 to part 742 of the [Export Administration Regulations \(EAR\)](#). While there is no prescribed form, you may freely copy the checklist from the unabridged Export Administration Regulations or from the Federal Register Rule published June 17, 2003.

You may also conveniently access a plain-paper version of the "checklist" here:
DOWNLOAD THE "CHECKLIST" : [[PDF](#) | [Word Perfect](#)]
DOWNLOAD SUPP. 6 TO PART 742 : [[PDF](#) | [Word Perfect](#)]

6. HOW DO I USE THE “CHECKLIST”?

After completing the "checklist" questionnaire, follow the guidance below to decide whether further encryption review or notification (through BIS and the ENC Encryption Request

Coordinator) is required. This list provides general scenarios of common situations involving the sale or transfer of encryption commodities and software (special provisions apply to exports and transfers of technology) outside the United States and Canada (except to sanctioned or embargoed destinations and end-users). It is not a comprehensive list and is offered as a working aid to exporters.

Notes: Rules governing exports and reexports of encryption are found in the Export Administration Regulations (EAR), 15 C.F.R. Parts 730-774. Sections 740.13, 740.17 and 742.15 of the EAR are the principal references for the export and reexport of encryption items. In addition, Section 748.3 provides an introduction (§748.3(a)) and basic sets of instructions regarding commodity classifications (§748.3(b)) and encryption review requests (§748.3(d)). For specific regulatory provisions for ["publicly available" source code](#) (and corresponding object code), see §740.13(e).

1. Encryption review or notification is NOT required (per §740.17 and §742.15(b)(3) of the EAR) for commodities and software that:
 - a. Do not provide, and have not been designed for (or in connection with) the production, development or use of any encryption, decryption and/or key management functionality ("checklist" question 1.h).
 - b. Are exported or reexported to U.S. companies and their subsidiaries in any country not listed in Country Group E:1, for internal company use (except source code to nationals of countries listed in Country Group E:1), including for the development of new products. See §740.17(b)(1) and §742.15(b)(3)(i).
 - c. Are exported or reexported to private sector end-users headquartered in Canada or in countries listed in Supplement No. 3 to part 740, only for internal use for the development of new products. See §740.17(a)(1).
 - d. Would not otherwise be controlled under Category 5 (telecommunications and "information security") of the Commerce Control List (CCL), but which are so controlled only because they incorporate components or software ("checklist" question 3) that provide short-range wireless encryption functions (e.g., with an operating range typically not exceeding 100 meters). See §740.17(b)(3)(iii)(H) and §742.15(b)(3)(ii).
 - e. Employ limited forms of cryptography, such as authentication, copy protection, and anti-virus protection ("checklist" questions 1.d-f). For additional such items that do not require review or notification, see the Related Controls and Technical Notes under ECCN 5A002 in Category 5, part 2 of the CCL (Supplement 1 to part 774). See §742.15(b)(3)(iii).
2. Notification by the time of export IS required for encryption commodities and software that:
 - a. Are "mass market" products with symmetric key length not exceeding 64-bit algorithms ("checklist" question 2.a). See §742.15(b)(1)(i) and the Cryptography Note (Note 3) of Category 5, part 2 of the CCL. [Notification for NLR](#) is required.
 - b. Do not qualify as "mass market" and employ key lengths less than or equal to 56-bits for symmetric algorithms, 512-bits for asymmetric algorithms and 112-bits for elliptic

curve algorithms ("checklist" questions 2.a and 2.b). See §742.15(b)(1)(ii). [Notification for NLR](#) is required.

3. Review IS required for encryption commodities and software that:
 - a. Are "mass market" products with symmetric key length exceeding 64-bit algorithms ("checklist" question 2.a). See §742.15(b)(2) of the EAR and the Cryptography Note (Note 3) of Category 5, part 2 of the CCL for [>64-bit mass-market encryption](#).
 - b. Do not qualify as "mass market" and employ key lengths greater than 56-bits for symmetric algorithms, 512-bits for asymmetric algorithms and 112-bits for elliptic curve algorithms ("checklist" questions 2.a and 2.b), or which provide an open cryptographic interface as defined in §772.1. See §740.17 of the EAR for [License Exception ENC](#).

NOTE : For transactions for which a [license](#) is required (e.g., the provisions of License Exception ENC or "mass market" do not apply), see §742.15(a) for information regarding encryption licensing requirements and policy.