

Encryption Review Decision Flowchart

START → Does the product contain any information-security functionality?

If **NO** →

STOP. No encryption review required.

- (EAR 740.17 & 742.15(b)(3))

If **YES** → Continue ↓

1. Does the product perform encryption, decryption, or key management?

Examples: AES-256, TLS 1.3, RSA/ECC, certificate handling, key exchange.

If **NO** →

- Does it only perform **authentication, DRM, or antivirus**?
 - If **YES** → **STOP.** No review required.
 - If **NO** → Contact Research Compliance.

If **YES** → Continue ↓

2. Identify the cryptography strength

Symmetric

- AES-128 or AES-256
- ChaCha20
- Other modern algorithms

Asymmetric

- RSA-2048 or higher
- ECC (P-256, Curve25519, etc.)
- PQC (Kyber, Dilithium)

If the product uses **any modern strong encryption**, continue ↓

3. Is the product “mass market”?

Criteria include:

- Widely available to the public
- No custom cryptographic interface
- Designed for general consumer use

If **YES** → Continue ↓

If **NO** → Skip to Step 5

4. Mass-Market Encryption Strength

If encryption is **≤64-bit symmetric** →

- **Notification required** (NLR).

If encryption is **>64-bit symmetric** (modern products) →

- **Review required** under License Exception ENC.

Continue ↓

5. Does the product provide an “open cryptographic interface”?

Examples:

- Allows users to insert their own algorithms
- Exposes crypto primitives for general use
- Functions as a crypto library

If **YES** →

- **Review required** (ENC).

If **NO** → Continue ↓

6. Can the encryption component be reused or extracted by end-users?

If **YES** →

- **Review required** (ENC).

If **NO** → Continue ↓

7. Destination & End-User Check

Is the export going to:

- A U.S. company or subsidiary (non-E:1)?
- A private-sector end-user in Canada or Supplement 3 countries?
- Internal development use only?

If **YES** →

- **No review required** (with exceptions).

If **NO** → Continue ↓

8. Final Determination

If any of the following are true:

- Strong encryption (>64-bit symmetric)
- Modern asymmetric algorithms (RSA-2048+, ECC)
- TLS 1.3, SSH, IPsec, VPN
- Cryptographic libraries
- PQC algorithms
- Reusable crypto components
- Non-mass-market product

→ **Export Control Review IS REQUIRED.**

END → Contact Research Compliance

Val Thomas (Export Control Officer) - export@npe.nmt.edu