

CHART 1A

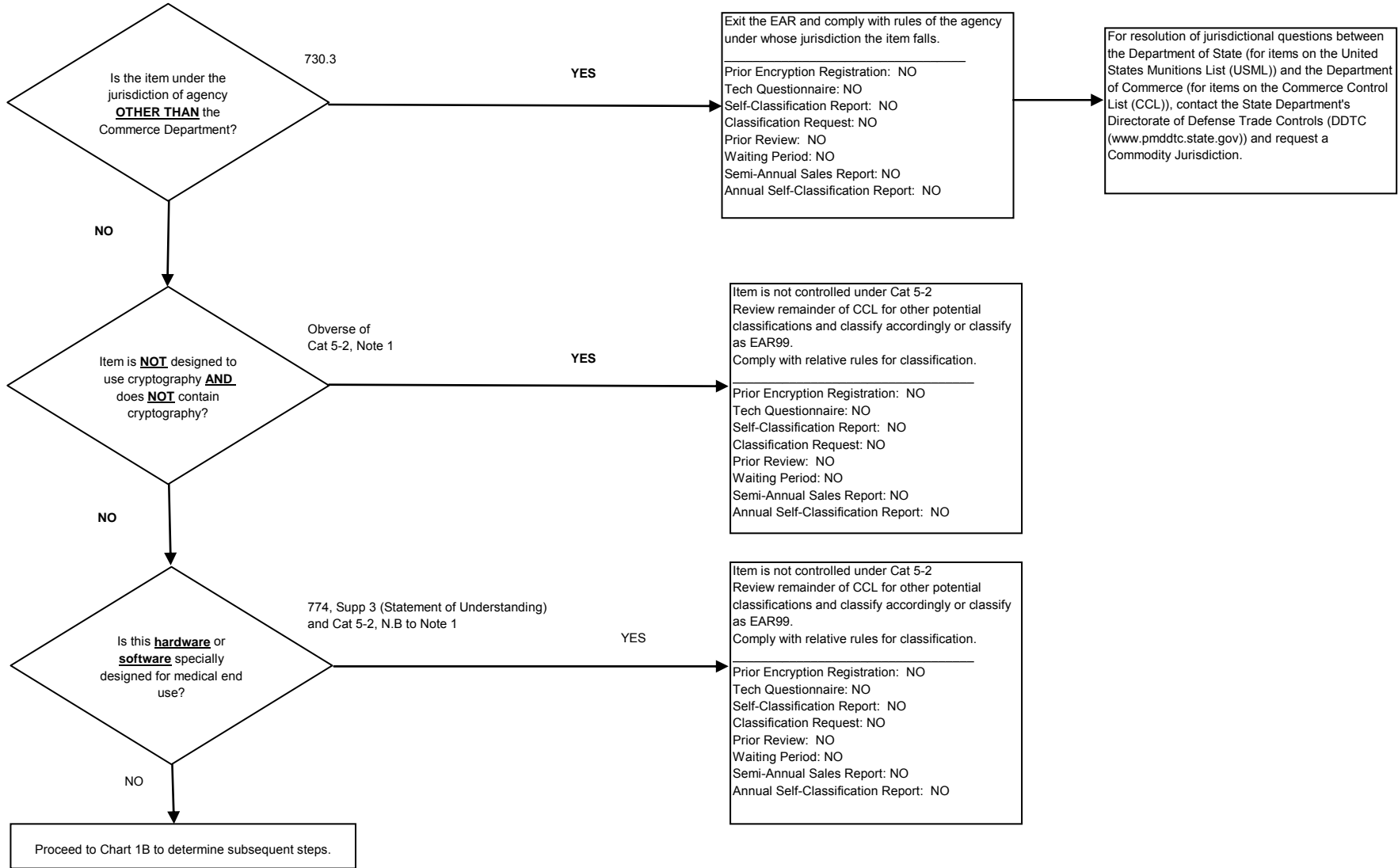


CHART 1B

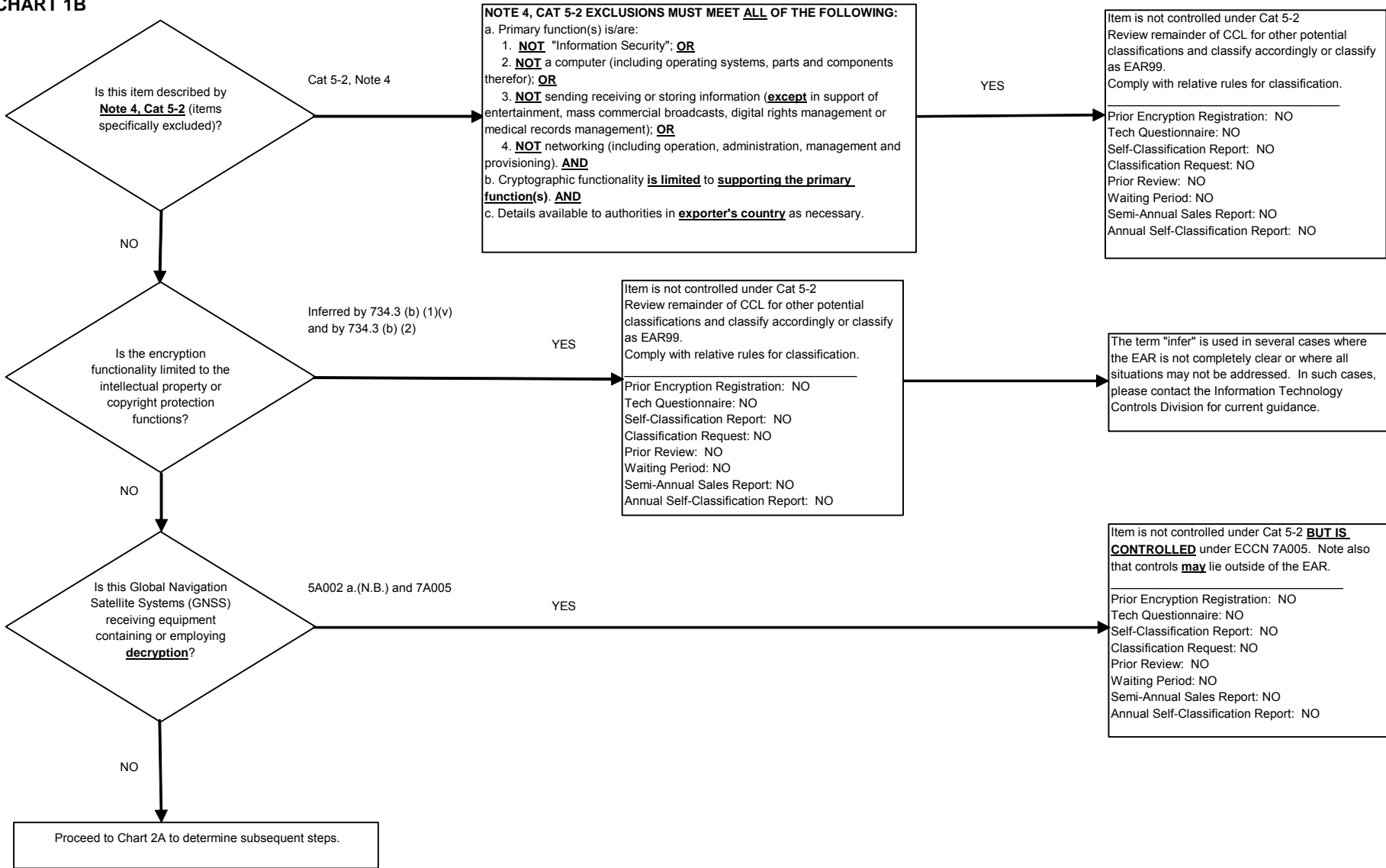


CHART 2A

PARTIAL LIST OF ITEMS CONTROLLED UNDER 5A002

This is **ONLY** a partial listing provided for immediate reference in training. Do **NOT** take export action based upon this information. Refer instead to the current version of Category 5, Part 2 of the EAR.

- a. Systems, equipment, application specific "electronic assemblies," modules and integrated circuits for "information security," as follows, and components therefor specially designed for "information security":
- a.1. **(E/NS/AT)** Designed or modified to use "cryptography" employing digital techniques performing any **cryptographic function other than authentication or digital signature and** having any of the following:
- a.1.a. A "**symmetric** algorithm" employing a key length in **excess of 56-bits**; or
- a.1.b. An "**asymmetric** algorithm" where the security of the algorithm is based on any of the following:
- a.1.b.1. Factorization of integers in **excess of 512 bits** (e.g., RSA);
- a.1.b.2. Computation of discrete logarithms in a multiplicative group of a finite field of size **greater than 512 bits** (e.g., Diffie-Hellman over Z/pZ); or
- a.1.b.3. Discrete logarithms in a group other than mentioned in 5A002.a.1.b.2 in **excess of 112 bits** (e.g., Diffie-Hellman over an **elliptic curve**);
- a.2. **(E/NS/AT)** Designed or modified to perform **cryptanalytic functions**;
- a.4. **(NS/AT)** Specially designed or modified to reduce the compromising emanations of information bearing signals beyond what is necessary for health, safety or electromagnetic interference standards;
- a.5. **(E/NS/AT)** Designed or modified to use cryptographic techniques to **generate the spreading code for "spread spectrum" systems**, not controlled in 5A002.a.6., including the **hopping code** for "frequency hopping" systems;
- a.6. **(E/NS/AT)** Designed or modified to use cryptographic techniques to **generate channelizing codes, scrambling codes or network identification codes**, for systems using **ultra-wideband modulation** techniques **and** having any of the following:
- a.6.a. A **bandwidth** exceeding **500 MHz**; or
- a.6.b. A "**fractional bandwidth**" of **20%** or more;
- a.7. **(NS/AT)** Non-cryptographic information and communications technology (ICT) security systems and devices evaluated to an assurance level exceeding class EAL-6;
- a.8. **(NS/AT)** Communications cable systems designed or modified using mechanical, electrical or electronic means to detect surreptitious intrusion;
- a.9. **(E/NS/AT)** Designed or modified to use '**quantum cryptography**.'

PARTIAL LIST OF ITEMS CONTROLLED UNDER 5B002

- a. **(NS/AT)** Equipment specially designed for the "development" or "production" of equipment controlled by 5A002 or 5B002.b;
- b. **(NS/AT)** Measuring equipment specially designed to evaluate and validate the "information security" functions of equipment controlled by 5A002 or "software" controlled by 5D002.a or 5D002.c.

PARTIAL LIST OF ITEMS CONTROLLED UNDER 5D002

- a. **(EI CONTROLS APPLY TO THIS ITEM IF FOR EQUIPMENT CONTROLLED FOR EI)** "Software" specially designed or modified for the "development", "production" or "use" of equipment controlled by 5A002 or "software" controlled by 5D002.c;
- b. **(NS/AT)** "Software" specially designed or modified to support "technology" controlled by 5E002;
- c. Specific "software" as follows:
- c.1. **(EI CONTROLS APPLY TO THIS ITEM IF FOR EQUIPMENT CONTROLLED FOR EI)** "Software" having the characteristics, or performing or simulating the functions of the equipment, controlled by 5A002;
- c.2. **(NS/AT)** "Software" to certify "software" controlled by 5D002.c.1.

PARTIAL LIST OF ITEMS CONTROLLED UNDER 5E002

(EI CONTROLS APPLY TO THIS ITEM IF FOR COMMODITIES/SOFTWARE CONTROLLED FOR EI) "Technology" according to the General Technology Note for the "development," "production" or "use" of equipment controlled by 5A002 or 5B002 or "software" controlled by 5D002.a or 5D002.c.

Proceed to Chart 2B to determine subsequent steps.

CHART 2B

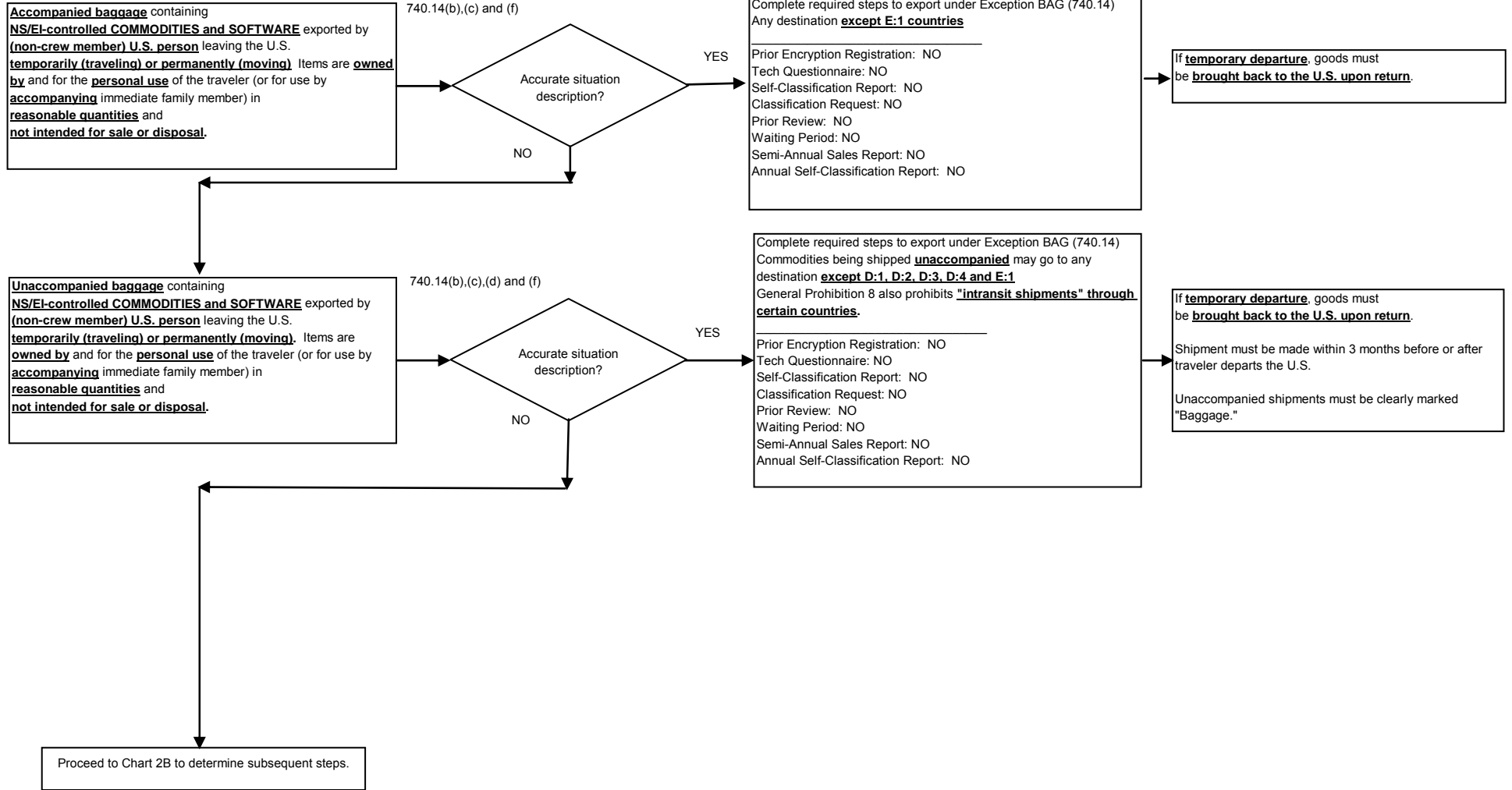


CHART 2C

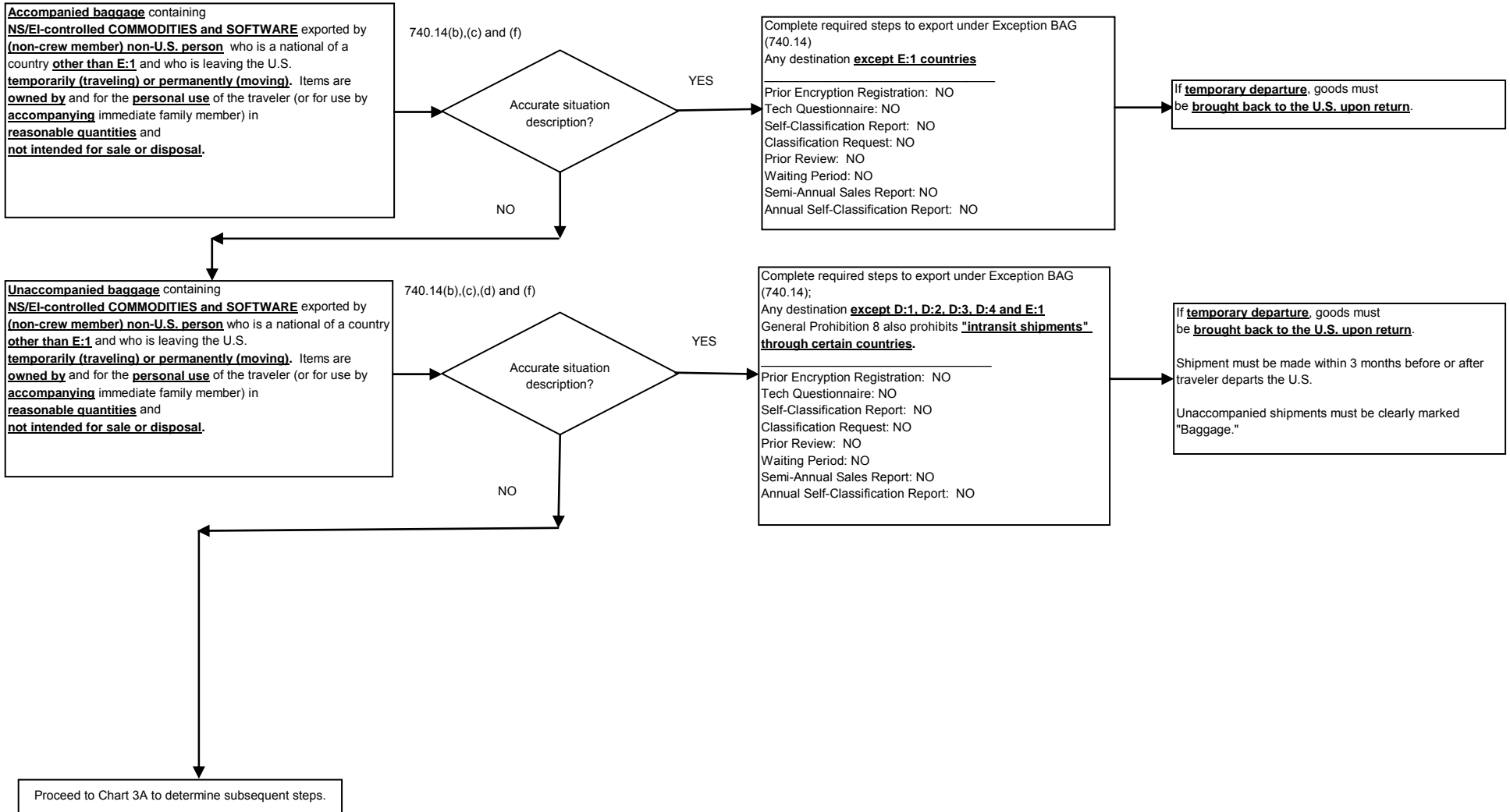


CHART 3A

PARTIAL LIST OF ITEMS CONTROLLED UNDER 5A002

This is **ONLY** a partial listing provided for immediate reference in training. Do **NOT** take export action based upon this information. Refer instead to the current version of Category 5, Part 2 of the EAR.

- a. Systems, equipment, application specific "electronic assemblies," modules and integrated circuits for "information security," as follows, and components therefor specially designed for "information security":
- a.1. **(E/NS/AT)** Designed or modified to use "cryptography" employing digital techniques performing any **cryptographic function other than authentication or digital signature and** having any of the following:
- a.1.a. A **"symmetric algorithm"** employing a key length in **excess of 56-bits**; or
- a.1.b. An **"asymmetric algorithm"** where the security of the algorithm is based on any of the following:
- a.1.b.1. Factorization of integers in **excess of 512 bits** (e.g., RSA);
- a.1.b.2. Computation of discrete logarithms in a multiplicative group of a finite field of size **greater than 512 bits** (e.g., Diffie-Hellman over Z/pZ); or
- a.1.b.3. Discrete logarithms in a group other than mentioned in 5A002.a.1.b.2 in **excess of 112 bits** (e.g., Diffie-Hellman over an **elliptic curve**);
- a.2. **(E/NS/AT)** Designed or modified to perform **cryptanalytic functions**;
- a.4. **(NS/AT)** Specially designed or modified to reduce the compromising emanations of information bearing signals beyond what is necessary for health, safety or electromagnetic interference standards;
- a.5. **(E/NS/AT)** Designed or modified to use cryptographic techniques to **generate the spreading code for "spread spectrum" systems**, not controlled in 5A002.a.6., including the **hopping code** for "frequency hopping" systems;
- a.6. **(E/NS/AT)** Designed or modified to use cryptographic techniques to **generate channelizing codes, scrambling codes or network identification codes**, for systems using **ultra-wideband modulation techniques and** having any of the following:
- a.6.a. A **bandwidth exceeding 500 MHz**; or
- a.6.b. A **"fractional bandwidth" of 20% or more**;
- a.7. **(NS/AT)** Non-cryptographic information and communications technology (ICT) security systems and devices evaluated to an assurance level exceeding class EAL-6;
- a.8. **(NS/AT)** Communications cable systems designed or modified using mechanical, electrical or electronic means to detect surreptitious intrusion;
- a.9. **(E/NS/AT)** Designed or modified to use **'quantum cryptography.'**

PARTIAL LIST OF ITEMS CONTROLLED UNDER 5B002

- a. **(NS/AT)** Equipment specially designed for the "development" or "production" of equipment controlled by 5A002 or 5B002.b;
- b. **(NS/AT)** Measuring equipment specially designed to evaluate and validate the "information security" functions of equipment controlled by 5A002 or "software" controlled by 5D002.a or 5D002.c.

PARTIAL LIST OF ITEMS CONTROLLED UNDER 5D002

- a. **(EI CONTROLS APPLY TO THIS ITEM IF FOR EQUIPMENT CONTROLLED FOR EI)** "Software" specially designed or modified for the "development", "production" or "use" of equipment controlled by 5A002 or "software" controlled by 5D002.c;
- b. **(NS/AT)** "Software" specially designed or modified to support "technology" controlled by 5E002;
- c. Specific "software" as follows:
- c.1. **(EI CONTROLS APPLY TO THIS ITEM IF FOR EQUIPMENT CONTROLLED FOR EI)** "Software" having the characteristics, or performing or simulating the functions of the equipment, controlled by 5A002;
- c.2. **(NS/AT)** "Software" to certify "software" controlled by 5D002.c.1.

PARTIAL LIST OF ITEMS CONTROLLED UNDER 5E002

(EI CONTROLS APPLY TO THIS ITEM IF FOR COMMODITIES/SOFTWARE CONTROLLED FOR EI) "Technology" according to the General Technology Note for the "development," "production" or "use" of equipment controlled by 5A002 or 5B002 or "software" controlled by 5D002.a or 5D002.c.

Proceed to Chart 3B to determine subsequent steps.

CHART 3B

NS/EI-controlled Commodities and Software as well as 5E992 Technology (but specifically excluding 5E002) exported and reexported for **temporary use** in **usual and reasonable** kinds and quantities.

No **new** technology may be released and persons receiving the technology must already be authorized to receive it through license, exception or NLR authorization.

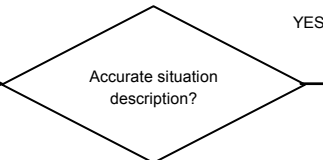
Items remain under the **effective control** of the exporter or employee with authorized access.

Usual and reasonable kinds and quantities for use in lawful enterprise.

Can include (but is not limited to) equipment, software and technology to commission or service items of foreign origin not subject to the EAR or items of U.S. origin provided they were exported/reexported lawfully.

Technology may not be used for foreign production or technical assistance unless so authorized.

740.9(a)(1) and (2)(i)(A)



Complete required steps to export under Exception TMP (Tools of Trade) (740.9(a)(2)(i)(A))

Any destination **except E:2 (Cuba) (including to ENTITIES controlled by a NATIONAL OF THAT COUNTRY and except to Sudan)** (740.9(a)(2)(i)(A)). In addition, 740.2(a)(6) prohibits use of this exception to comprehensively embargoed destinations of **Cuba, Iran and North Korea**. If unaccompanied shipment, General Prohibition 8 which prohibits **"intransit shipments" through certain countries** may apply.

See SPECIAL REPORTING REQUIREMENT

Prior Encryption Registration: NO
 Tech Questionnaire: NO
 Self-Classification Report: NO
 Classification Request: NO
 Prior Review: NO
 Waiting Period: NO
 Semi-Annual Sales Report: NO
 Annual Self-Classification Report: NO

Special Reporting Requirement: For the export/reexport of **Technology UNDER TMP to employees who are not U.S. persons**. Part 740.9(a)(3)(iv) requires that those persons must already be eligible for access to the technology; AND the U.S. employer must demonstrate and **document** the need of that employee to have the technology aboard with documentation maintained according to Part 762

Unless consumed, items must be returned to country from which exported or reexported as soon as practicable but no later than one year (unless otherwise authorized).

Shipment can accompany traveler, be shipped unaccompanied within one month before traveler's departure or at any time after that departure.

Technology exports and reexports may be made as shipments, transmissions or releases.

Cannot be used in support of any sensitive nuclear activity except in A:1, Iceland and New Zealand.

Sudan-specific Situation

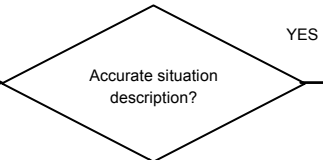
5D992 software loaded on specified and authorized commodities (4A994.b, .d, .e, .g and .h and on 5A991) before arrival in Sudan and 5A992 parts and components installed with and to remain so loaded while in Sudan.

Under sponsorship of a **specified and authorized** non-governmental organization.

In support of **Darfur Peace Agreement, Comprehensive Peace Agreement** or other **development and relief activities** by an **OFAC-Registered organization**.

Items remain under the **effective control** of the permissible user.

740.9(a)(1) and (2)(i)(B)



Complete required steps to export under Exception TMP (Tools of Trade) (740.9(a)(2)(i)(B))

Sudan-specific requirements.

Must accompany traveler or be shipped/transmitted in manner reasonably calculated to reach the intended user.

If unaccompanied shipment, General Prohibition 8 which prohibits **"intransit shipments" through certain countries** may apply.

Prior Encryption Registration: NO
 Tech Questionnaire: NO
 Self-Classification Report: NO
 Classification Request: NO
 Prior Review: NO
 Waiting Period: NO
 Semi-Annual Sales Report: NO
 Annual Self-Classification Report: NO

Goods must remain with the permissible user while in Sudan.

Unless consumed, items must be returned to country from which exported as soon as practicable but no later than one year.

Proceed to Chart 3C to determine subsequent steps.

CHART 3C

Kits of Replacement Parts for NS/EI-controlled Commodities and Software which would otherwise qualify for shipment as individual parts under License Exception RPL.

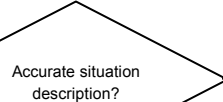
Items remain under the **effective control** of the exporter or employee with authorized access.

Can include subassemblies but does not include major subsystems, test instruments or operating supplies.

No changes or improvements to the basic design.

Only on lawfully exported items or items manufactured in a foreign country and not under the EAR.

740.9(a)(1) and (2)(ii) and 740.10 (a) (RPL-Parts)



YES

Complete required steps to export under Exception TMP (Kits of Replacement Parts) (740.9(a)(2)(ii))
 Any destination **except E:2 (Cuba) including to ENTITIES controlled by a NATIONAL OF THAT COUNTRY.** In addition, 740.2(a)(6) prohibits use of this exception to comprehensively embargoed destinations of **Cuba, Iran and North Korea.**
 If unaccompanied shipment, General Prohibition 8 which prohibits **"intransit shipments" through certain countries** may apply.

Prior Encryption Registration: NO
 Tech Questionnaire: NO
 Self-Classification Report: NO
 Classification Request: NO
 Prior Review: NO
 Waiting Period: NO
 Semi-Annual Sales Report: NO
 Annual Self-Classification Report: NO

All parts in the kit must be returned except one-for-one replacements may be made with defective parts returned.

Cannot be used to overcome license requirement for parts if original license conditions require separate parts licenses.

Return to country from which exported as soon as practicable but no later than one year.

For Replacement Parts (as opposed to Kits) refer to License Exception (RPL (Parts))

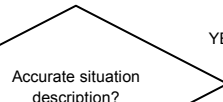
NO

NS/EI-controlled Commodities and Software exported and reexported for **temporary use in exhibition or demonstration in usual and reasonable** kinds and quantities.

Items remain under the **effective control** of the exporter or under the **effective control** of an employee or sales representative with authorized access.

Except as necessary for effective demonstration, goods are not used for their intended purpose while abroad and are not exhibited for more than 120 days at one site.

740.9(a)(1) and (2)(iii)



YES

Complete required steps to export under Exception TMP (Exhibition and Demonstration) (740.9(a)(2)(iii))
 Any destination **except E:1 (Cuba (including ENTITIES controlled by a NATIONAL OF THAT COUNTRY), Iran, North Korea, Sudan and Syria).**
 If unaccompanied shipment, General Prohibition 8 which prohibits **"intransit shipments" through certain countries** may apply.

Prior Encryption Registration: NO
 Tech Questionnaire: NO
 Self-Classification Report: NO
 Classification Request: NO
 Prior Review: NO
 Waiting Period: NO
 Semi-Annual Sales Report: NO
 Annual Self-Classification Report: NO

Unless consumed, items must be returned to country from which exported as soon as practicable but no later than one year.

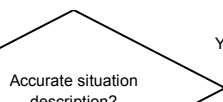
Exporter must be shown as the **ultimate consignee** in care of the person who will have control over the items abroad.

NO

NS/EI-controlled Commodities temporarily exported and reexported to be **inspected, tested, calibrated or repaired abroad.**

Items remain under the **effective control** of the exporter or under the **effective control** of an employee with authorized access.

740.9(a)(1) and (2)(iv)



YES

Complete required steps to export under Exception TMP (Inspection and Calibration) (740.9(a)(2)(iv))
 Note that 740.9(a)(2)(iv) authorizes any destination **to except E:2 (Cuba) or to Sudan and Syria.** However, 740.9(a)(3)(i)(B) conflicts by **DISALLOWING E:2 (Cuba) AND THE D:1 countries (currently numbered at 22 countries) as well as ENTITIES controlled by a NATIONAL OF ANY OF THOSE COUNTRIES.**
 If unaccompanied shipment, General Prohibition 8 which prohibits **"intransit shipments" through certain countries** may apply.

Prior Encryption Registration: NO
 Tech Questionnaire: NO
 Self-Classification Report: NO
 Classification Request: NO
 Prior Review: NO
 Waiting Period: NO
 Semi-Annual Sales Report: NO
 Annual Self-Classification Report: NO

Unless consumed, items must be returned to country from which exported as soon as practicable but no later than one year.

NO

Proceed to Chart 3D to determine subsequent steps.

CHART 3D

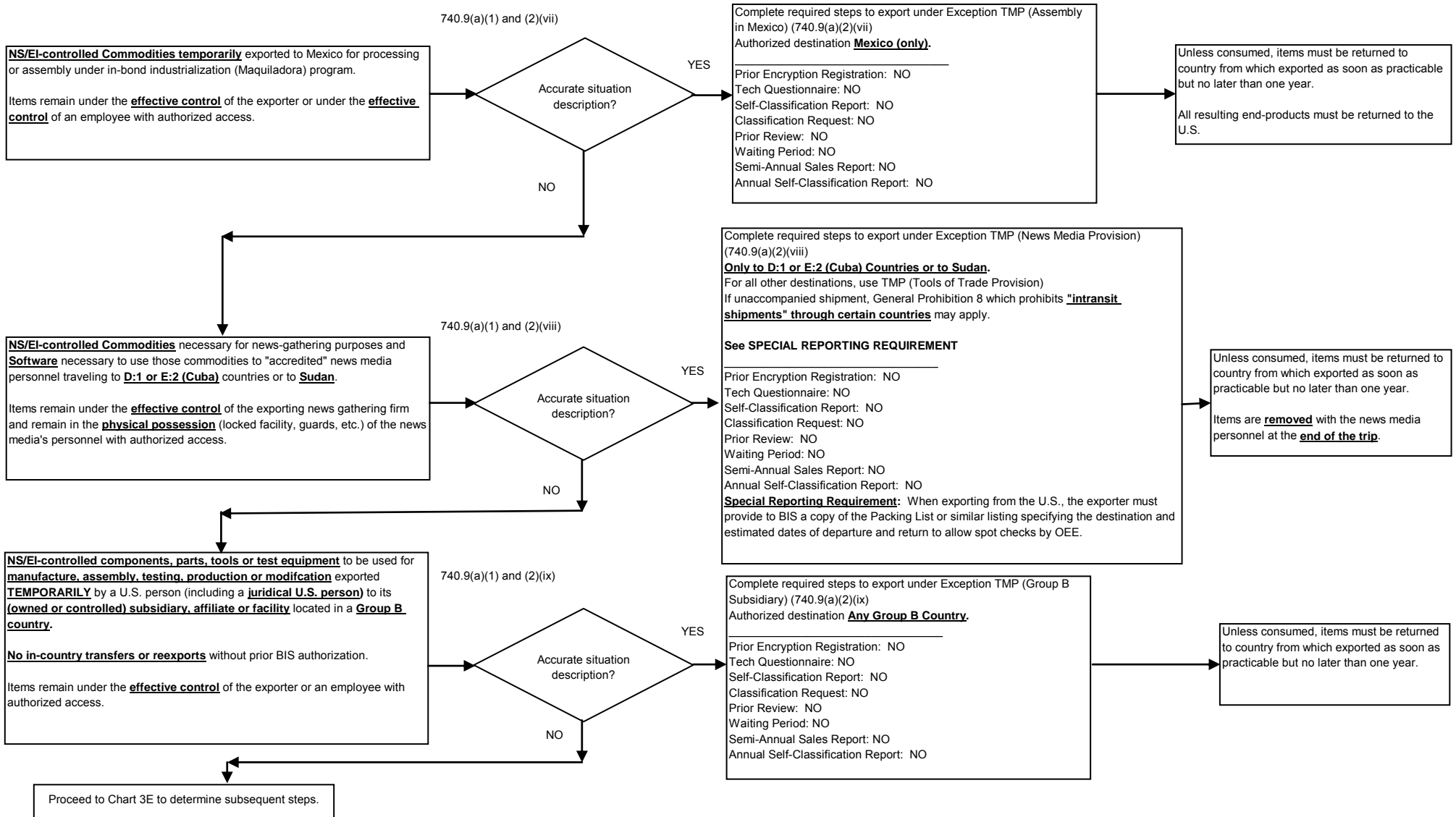
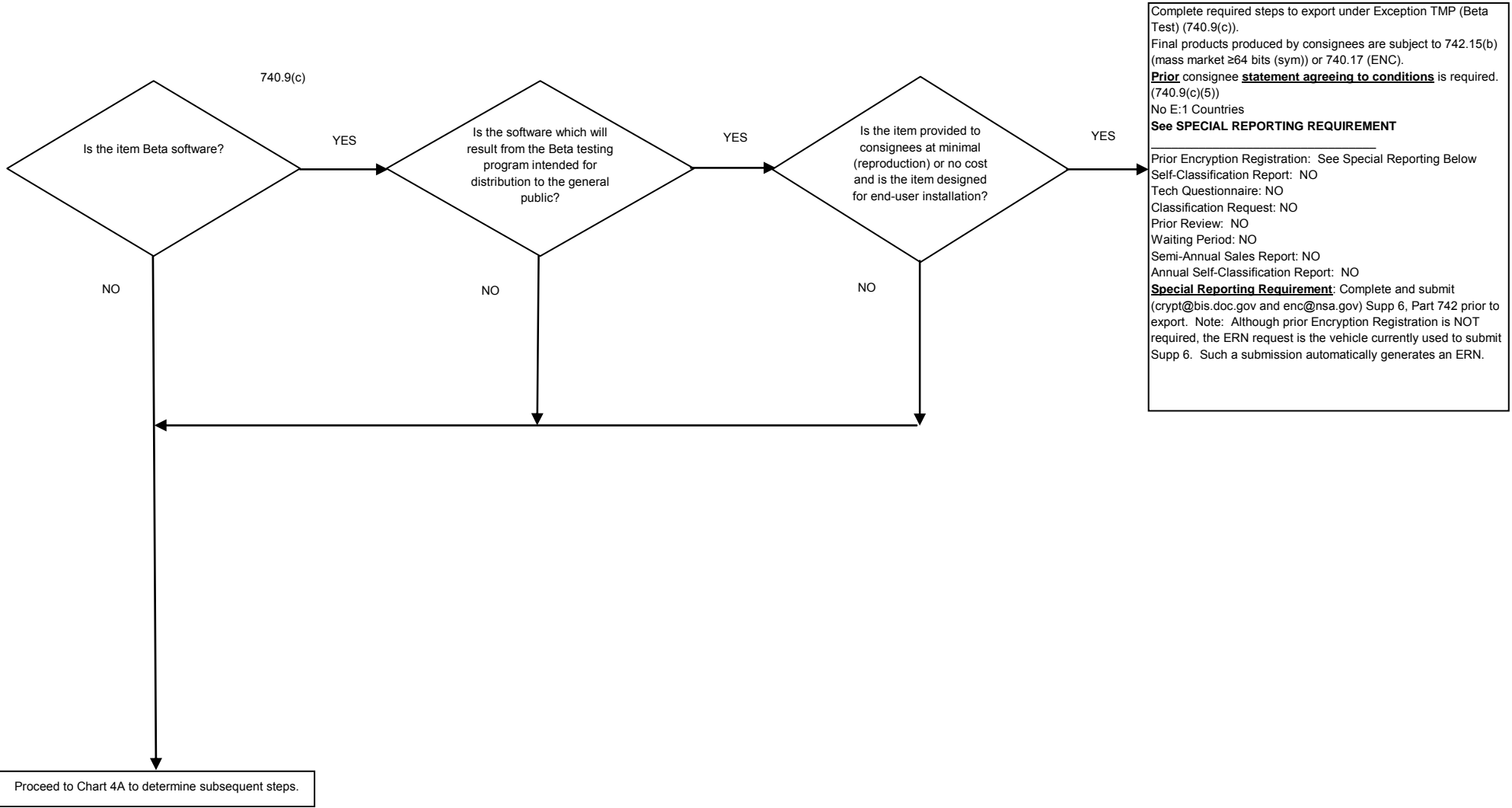


CHART 3E



Complete required steps to export under Exception TMP (Beta Test) (740.9(c)).
Final products produced by consignees are subject to 742.15(b) (mass market ≥64 bits (sym)) or 740.17 (ENC).
Prior consignee **statement agreeing to conditions** is required. (740.9(c)(5))
No E:1 Countries
See SPECIAL REPORTING REQUIREMENT

Prior Encryption Registration: See Special Reporting Below
Self-Classification Report: NO
Tech Questionnaire: NO
Classification Request: NO
Prior Review: NO
Waiting Period: NO
Semi-Annual Sales Report: NO
Annual Self-Classification Report: NO
Special Reporting Requirement: Complete and submit (crypt@bis.doc.gov and enc@nsa.gov) Supp 6, Part 742 prior to export. Note: Although prior Encryption Registration is NOT required, the ERN request is the vehicle currently used to submit Supp 6. Such a submission automatically generates an ERN.

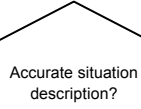
CHART 4A

Replacement Parts needed for immediate repair including defective or worn parts for previously exported equipment.

Can include subassemblies but does not include major subsystems, test instruments or operating supplies. No changes or improvements to the basic design.

Only available for use on lawfully exported end items where the terms of the original authorization have not been violated. This means that this exception can only be used by the party who originally exported the end item or by a party who has confirmed that the end item is lawfully at the current location.

740.10(a)



YES

Complete required steps to export under Exception RPL (Parts) (740.10(a))
Any destination **except to comprehensively embargoed countries (Cuba, Iran, North Korea), (740.2(a)(6) and to AT controlled countries 742.8 (Iran), 742.9 (Syria) and 742.10 (Sudan).**
If unaccompanied shipment, General Prohibition 8 which prohibits "**intransit shipments**" through certain countries may apply.

Prior Encryption Registration: NO
Tech Questionnaire: NO
Self-Classification Report: NO
Classification Request: NO
Prior Review: NO
Waiting Period: NO
Semi-Annual Sales Report: NO
Annual Self-Classification Report: NO

Parts are exported only to replace defective parts on a **one-for-one replacement** basis with defective parts promptly returned or destroyed abroad.

Cannot be used to overcome license requirement for parts if original license conditions require separate parts licenses.

Cannot be used to **build** a stock of spares but **CAN** be used to **maintain** a stock of spares that have been lawfully exported.

For kits consisting of replacement parts refer to TMP (Kits of Replacement Parts).

Commodities and Software sent to U.S. or authorized foreign party for **servicing** (including inspection, testing, calibration, repair, overhaul or reconditioning).

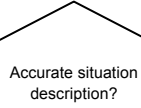
May include replacement or rebuilt parts but the **basic characteristics** as originally authorized for export or reexport **cannot be improved or changed.**

Only available for use on lawfully exported end items where the terms of the original authorization have not been violated.

Export MUST be to the person/firm to whom original license was issued.

End use and end user must remain unchanged from original license.

740.10(b)(2)



YES

Complete required steps to export under Exception RPL (Servicing) (740.10(b)(2))
Export to any **D:1 country EXCEPT People's Republic of China (PRC) and EXCEPT E:1 countries (Cuba, Iran, North Korea, Syria and Sudan).**
If unaccompanied shipment, General Prohibition 8 which prohibits "**intransit shipments**" through certain countries may apply.

Prior Encryption Registration: NO
Tech Questionnaire: NO
Self-Classification Report: NO
Classification Request: NO
Prior Review: NO
Waiting Period: NO
Semi-Annual Sales Report: NO
Annual Self-Classification Report: NO

Upon completion of servicing returning goods may be accompanied by any necessary spare part, tool, accessory or other item that was **sent with it for servicing.**

Commodities and Software exported or reexported to **replace defective or otherwise unusable (e.g., erroneously supplied)** items.

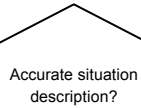
Not to replace **worn out equipment** or to **build a stock** abroad.

Basic characteristics as originally authorized for export or reexport **not improved or changed.**

Item being replaced previously exported or reexported to current location under BIS license or authorization.

If a reexport, the reexporting party has ensured the items being replaced were lawfully shipped to the current destination and continue to be used in accordance with U.S. law.

740.10(b)(3)



YES

Complete required steps to export under Exception RPL (Replacement) (740.10(b)(3))
Export to any destination **EXCEPT E:1 countries (Cuba, Iran, North Korea, Syria and Sudan) and EXCEPT to ENTITY controlled by a NATIONAL OF THOSE COUNTRIES.**
If unaccompanied shipment, General Prohibition 8 which prohibits "**intransit shipments**" through certain countries may apply.

Prior Encryption Registration: NO
Tech Questionnaire: NO
Self-Classification Report: NO
Classification Request: NO
Prior Review: NO
Waiting Period: NO
Semi-Annual Sales Report: NO
Annual Self-Classification Report: NO

If replacement item is being shipped to a **Group B or Group D:1** country, the following conditions apply:

(A) The **exporter** represents that all conditions have been met and that items being replaced will be returned or destroyed; AND

(B) The replacement is made **free of charge** (except transportation and labor) and (**if to D:1 (less PRC)**) within the **warranty period or 12-months (as shorter)**; AND

(C) The replaced item must be destroyed abroad or returned to the U.S. or to a foreign firm in **Group B** under the effective control of the exporter.

Return or destruction must be **before or promptly after** the replacement item is exported **from the U.S.**

Proceed to Chart 5A to determine subsequent steps.

CHART 5A

Cuba-specific Situation
Export or Reexport to and for use by **non-government** organizations and individuals as specified (receipt by certain government and party officials is prohibited);

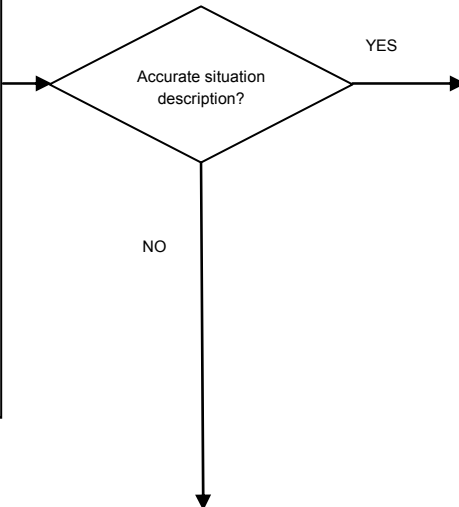
Donated or given **free of charge** (excluding shipping costs and charges levied by government of importing country);

Includes following commodities and software:
EAR99 and **4A994.b** Computers ≤0.02 Weighted TeraFlops (WT)

and the following commodities and software that has been classified **ONLY** as indicated:

- Disk drives/solid state storage equipment (5A992 or EAR99)
- Input/output control units (other than industrial controllers for chem (EAR99)
- Graphics accerators and coprocessors (EAR99)
- Monitors (5A992 or EAR99)
- Printers (5A992 or EAR99)
- Modems (5A992.b.2, 5A992 or EAR99)
- Network access controllers (5A991.b.4 or EAR99)
- Communications channel controllers (5A991.b.4 or EAR99)
- Keyboards, mice and similar devices (EAR99)
- Mobile phones (including cellular and satellite) (5A992 or 5A991 or EAR99)
- PDA & SIM Cards and similar devices (5A992 or 5A991 or EAR99)
- Memory Devices (5A992 or EAR99)
- "Information Security" equipment, software (except encryption source code) and peripherals (5A992 or 5D992 or EAR99)
- Digital cameras and memory cards (5A992 or EAR99)
- Television and Radio Receivers (5A992 or EAR99)
- Recording Devices (5A992 or EAR99)
- Batteries, chargers, carrying cases adn accessories for above (EAR99)
- Software (except encryption source code) for above ((4D994 or 5D991 or 5D992 or EAR99)

740.19



Complete required steps to export under Exception CCD (740.19)
Export to Cuba **Only**

Prior Encryption Registration: NO
Tech Questionnaire: NO
Self-Classification Report: NO
Classification Request: NO
Prior Review: NO
Waiting Period: NO
Semi-Annual Sales Report: NO
Annual Self-Classification Report: NO

Proceed to Chart 6A to determine subsequent steps.

CHART 6A

PARTIAL LIST OF ITEMS CONTROLLED UNDER 5A002

This is **ONLY** a partial listing provided for immediate reference in training. Do **NOT** take export action based upon this information. Refer instead to the current version of Category 5, Part 2 of the EAR.

- a. Systems, equipment, application specific "electronic assemblies," modules and integrated circuits for "information security," as follows, and components therefor specially designed for "information security":
- a.1. **(E/NS/AT)** Designed or modified to use "cryptography" employing digital techniques performing any **cryptographic function other than authentication or digital signature and** having any of the following:
 - a.1.a. A "**symmetric** algorithm" employing a key length in **excess of 56-bits**; or
 - a.1.b. An "**asymmetric** algorithm" where the security of the algorithm is based on any of the following:
 - a.1.b.1. Factorization of integers in **excess of 512 bits** (e.g., RSA);
 - a.1.b.2. Computation of discrete logarithms in a multiplicative group of a finite field of size **greater than 512 bits** (e.g., Diffie-Hellman over Z/pZ); or
 - a.1.b.3. Discrete logarithms in a group other than mentioned in 5A002.a.1.b.2 in **excess of 112 bits** (e.g., Diffie-Hellman over an **elliptic curve**);
 - a.2. **(E/NS/AT)** Designed or modified to perform **cryptanalytic functions**;
 - a.4. **(NS/AT)** Specially designed or modified to reduce the compromising emanations of information bearing signals beyond what is necessary for health, safety or electromagnetic interference standards;
 - a.5. **(E/NS/AT)** Designed or modified to use cryptographic techniques to **generate the spreading code for "spread spectrum" systems**, not controlled in 5A002.a.6., including the **hopping code** for "frequency hopping" systems;
 - a.6. **(E/NS/AT)** Designed or modified to use cryptographic techniques to **generate channelizing codes, scrambling codes or network identification codes**, for systems using **ultra-wideband modulation** techniques **and** having any of the following:
 - a.6.a. A **bandwidth** exceeding **500 MHz**; or
 - a.6.b. A "**fractional bandwidth**" of **20%** or more;
 - a.7. **(NS/AT)** Non-cryptographic information and communications technology (ICT) security systems and devices evaluated to an assurance level exceeding class EAL-6;
 - a.8. **(NS/AT)** Communications cable systems designed or modified using mechanical, electrical or electronic means to detect surreptitious intrusion;
 - a.9. **(E/NS/AT)** Designed or modified to use '**quantum cryptography**.'

PARTIAL LIST OF ITEMS CONTROLLED UNDER 5B002

- a. **(NS/AT)** Equipment specially designed for the "development" or "production" of equipment controlled by 5A002 or 5B002.b;
- b. **(NS/AT)** Measuring equipment specially designed to evaluate and validate the "information security" functions of equipment controlled by 5A002 or "software" controlled by 5D002.a or 5D002.c.

PARTIAL LIST OF ITEMS CONTROLLED UNDER 5D002

- a. **(EI CONTROLS APPLY TO THIS ITEM IF FOR EQUIPMENT CONTROLLED FOR EI)** "Software" specially designed or modified for the "development", "production" or "use" of equipment controlled by 5A002 or "software" controlled by 5D002.c;
- b. **(NS/AT)** "Software" specially designed or modified to support "technology" controlled by 5E002;
- c. Specific "software" as follows:
 - c.1. **(EI CONTROLS APPLY TO THIS ITEM IF FOR EQUIPMENT CONTROLLED FOR EI)** "Software" having the characteristics, or performing or simulating the functions of the equipment, controlled by 5A002;
 - c.2. **(NS/AT)** "Software" to certify "software" controlled by 5D002.c.1.

PARTIAL LIST OF ITEMS CONTROLLED UNDER 5E002

(EI CONTROLS APPLY TO THIS ITEM IF FOR COMMODITIES/SOFTWARE CONTROLLED FOR EI) "Technology" according to the General Technology Note for the "development," "production" or "use" of equipment controlled by 5A002 or 5B002 or "software" controlled by 5D002.a or 5D002.c.

Proceed to Chart 6B to determine subsequent steps.

CHART 6B

MASS MARKET CRITERIA

Cat 5-2, Note 3: Cryptography Note:

ECCN's 5A002 and 5D002 do **NOT** control items that meet all of the following:

- a. Generally **available to the public** by being **sold without restriction** from stock at **retail selling points** (over-the-counter, mail order, electronic transactions, telephone transactions); AND
- b. **Cryptographic functionality** is **NOT** easily be **changed** by the user; AND
- c. Designed for **installation by the user** without further substantial support by the supplier; AND
- d. When necessary, **details are available** and will be provided upon request to the appropriate authority in the exporter's country to confirm compliance with the above.

742.15(b)(6)

EXAMPLES OF ITEMS WHICH **MAY BE ELIGIBLE** FOR MASS MARKET TREATMENT

Examples of Mass Market encryption items include **but are not limited to**:

General purpose operating systems;

Desktop applications designed for use with computers which are classified under ECCN 4A994 or designated EAR99 (such as e-mail, browsers, games, word processing, database, financial applications or utilities);

Laptops, hand-held devices;

Commodities and software for client internet appliances

Client wireless LAN devices;

Home use networking commodities and software (such as personal firewalls, cable modems for personal computers and consumer set top boxes);

Portable or mobile civil telecommunications commodities and software (such as Personal Data Assistants (PDA's), radios or cellular products);

```
graph TD; A["MASS MARKET CRITERIA..."] --> B["Proceed to Chart 6C to determine subsequent steps."];
```

Proceed to Chart 6C to determine subsequent steps.

CHART 6C

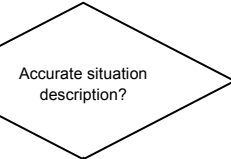
Minimum technology necessary for the **installation, operation, maintenance (checking) and repair** of commodities and software that have been **lawfully exported**.

Does **not** include technology for **development or production**.

Includes **only** technology to extent required to ensure **safe and efficient use** of the commodities or software.

Operation **software** exported/reexported **only** if it is the **minimum necessary to operate** equipment authorized for export and **only** if in **object code (not source code)**.

740.13(a)



YES

Complete required steps to export under Exception TSU (Operation Technology and Software).
Export to any country to which the equipment for which it is required is/was legally exported
No E:1 Countries

Prior Encryption Registration: NO
Tech Questionnaire: NO
Self-Classification Report: NO
Classification Request: NO
Prior Review: NO
Waiting Period: NO
Semi-Annual Sales Report: NO
Annual Self-Classification Report: NO

Note that individual entries in the software and technology subcategories **may further restrict** the export/reexport of operation technology.

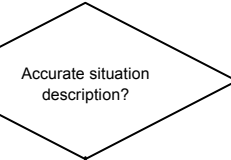
NO

Data supporting prospective or actual quotation, bid, offer to sell, lease or supply any item (known as **Sales Technology**).

Type customarily transmitted with a bid in established business practice.

Does **not** disclose detailed design, production or manufacture technology or means of reconstruction of the quoted item or its product (**prevents disclosure of technology**).

740.13(b)



YES

Complete required steps to export under Exception TSU (Sales Technology).
Export to any destination (see Note)

Prior Encryption Registration: NO
Tech Questionnaire: NO
Self-Classification Report: NO
Classification Request: NO
Prior Review: NO
Waiting Period: NO
Semi-Annual Sales Report: NO
Annual Self-Classification Report: NO

Note that the use of this provision does not insure that a license will be issued. It is therefore **recommended** that quotes and related correspondence **include a disclaimer** to protect the quoting company in the event a license is denied.

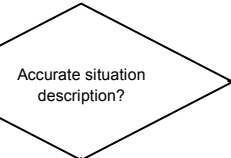
NO

Software update limited to correction of errors (**bug fixes**) for **lawfully exported original software**.

Does **not** enhance the functional capacities of the original software.

Shipping **only** to the **original consignee**.

740.13(c)



YES

Complete required steps to export under Exception TSU (Software Updates).
Export **only** to the **consignee** to whom the **original software** was **lawfully shipped**.
No E:1 Countries

Prior Encryption Registration: NO
Tech Questionnaire: NO
Self-Classification Report: NO
Classification Request: NO
Prior Review: NO
Waiting Period: NO
Semi-Annual Sales Report: NO
Annual Self-Classification Report: NO

NO

Proceed to Chart 6D to determine subsequent steps.

CHART 6D

Software but **specifically excluding** encryption software controlled for **EI (5D002)**.

Software meets criteria for mass market software ((1) Sold from stock at retail selling points without restriction (over-the-counter, mail order, electronic or telephone transactions); and (2) Designed for user-installation without further substantial supplier support).

Software is **not encryption** software controlled for EI (5D002) nor is it encryption software with a symmetric key length **>64-bits sym** (asym & ellip not addressed) that qualifies as mass market encryption.

740.13(d) and Gen. Software Note, Supp 2, Part 774 and Cat 5-2 Note 3: (Cryptography Note)

Accurate situation description?

YES

NO

Complete required steps to export under Exception TSU (Mass Market).
No E:1 Countries

Prior Encryption Registration: NO
Tech Questionnaire: NO
Self-Classification Report: NO
Classification Request: NO
Prior Review: NO
Waiting Period: NO
Semi-Annual Sales Report: NO
Annual Self-Classification Report: NO

Note that License Exception TSU does **not** apply to **software** controlled for EI reasons under ECCN 5D002. In addition and once such software has been reviewed by BIS and **released from EI controls** as mass market encryption software, it is then controlled under 5D992.c and is then outside the scope of TSU.

Encryption Source Code that although controlled by **5D002** would be considered **publicly available** if it were not controlled by **5D002**.

Corresponding Object Code (that is, code that is compiled from this same authorized source code).

The item is Source and (authorized and corresponding) Object Code.

The item is not encryption software, other than as described above even if it incorporates or is specially designed to use other encryption software that meets this requirement.

Note that 734.3 defines "Publicly Available" as:

1. Already published or will be published (generally accessible to the interested public in any form) (734.7); or
2. Arise during or result from fundamental research (734.8); or
3. Educational information (734.9); or
4. Included in patent applications (734.10).

740.13(e)

Accurate situation description?

YES

NO

Complete required steps to export under Exception TSU (Encryption Source Code).
No E:1 Countries

See SPECIAL REPORTING REQUIREMENT

Prior Encryption Registration: NO
Tech Questionnaire: NO
Self-Classification Report: NO
Classification Request: NO
Prior Review: NO
Waiting Period: NO
Semi-Annual Sales Report: NO
Annual Self-Classification Report: NO

Special Reporting Requirement: BIS & ENC Coord must both be notified **by e-mail** of the URL/Internet Address or provided a copy of the source code before posting or making publicly available. Both must also be kept advised of updates of the cryptographic functionality and/or change of URL.

Note 1: An agreement for payment of royalties, licensing, etc., is not relevant to nor does it disqualify use of this exception.

Note 2: Posting encryption source code and corresponding object code on the internet where it can be downloaded by anyone does not establish "knowledge" of a prohibited export nor is it a "red flag" as described by 732, Supp 3.

Proceed to Chart 7A to determine subsequent steps.

CHART 7A

PARTIAL LIST OF ITEMS CONTROLLED UNDER 5A002

This is **ONLY** a partial listing provided for immediate reference in training. Do **NOT** take export action based upon this information. Refer instead to the current version of Category 5, Part 2 of the EAR.

- a. Systems, equipment, application specific "electronic assemblies," modules and integrated circuits for "information security," as follows, and components therefor specially designed for "information security":
- a.1. **(E/NS/AT)** Designed or modified to use "cryptography" employing digital techniques performing any **cryptographic function other than authentication or digital signature and** having any of the following:
- a.1.a. A "**symmetric** algorithm" employing a key length in **excess of 56-bits**; or
- a.1.b. An "**asymmetric** algorithm" where the security of the algorithm is based on any of the following:
- a.1.b.1. Factorization of integers in **excess of 512 bits** (e.g., RSA);
- a.1.b.2. Computation of discrete logarithms in a multiplicative group of a finite field of size **greater than 512 bits** (e.g., Diffie-Hellman over Z/pZ); or
- a.1.b.3. Discrete logarithms in a group other than mentioned in 5A002.a.1.b.2 in **excess of 112 bits** (e.g., Diffie-Hellman over an **elliptic curve**);
- a.2. **(E/NS/AT)** Designed or modified to perform **cryptanalytic functions**;
- a.4. **(NS/AT)** Specially designed or modified to reduce the compromising emanations of information bearing signals beyond what is necessary for health, safety or electromagnetic interference standards;
- a.5. **(E/NS/AT)** Designed or modified to use cryptographic techniques to **generate the spreading code for "spread spectrum" systems**, not controlled in 5A002.a.6., including the **hopping code** for "frequency hopping" systems;
- a.6. **(E/NS/AT)** Designed or modified to use cryptographic techniques to **generate channelizing codes, scrambling codes or network identification codes**, for systems using **ultra-wideband modulation** techniques **and** having any of the following:
- a.6.a. A **bandwidth** exceeding **500 MHz**; or
- a.6.b. A "**fractional bandwidth**" of **20%** or more;
- a.7. **(NS/AT)** Non-cryptographic information and communications technology (ICT) security systems and devices evaluated to an assurance level exceeding class EAL-6;
- a.8. **(NS/AT)** Communications cable systems designed or modified using mechanical, electrical or electronic means to detect surreptitious intrusion;
- a.9. **(E/NS/AT)** Designed or modified to use '**quantum cryptography**.'

PARTIAL LIST OF ITEMS CONTROLLED UNDER 5B002

- a. **(NS/AT)** Equipment specially designed for the "development" or "production" of equipment controlled by 5A002 or 5B002.b;
- b. **(NS/AT)** Measuring equipment specially designed to evaluate and validate the "information security" functions of equipment controlled by 5A002 or "software" controlled by 5D002.a or 5D002.c.

PARTIAL LIST OF ITEMS CONTROLLED UNDER 5D002

- a. **(EI CONTROLS APPLY TO THIS ITEM IF FOR EQUIPMENT CONTROLLED FOR EI)** "Software" specially designed or modified for the "development", "production" or "use" of equipment controlled by 5A002 or "software" controlled by 5D002.c;
- b. **(NS/AT)** "Software" specially designed or modified to support "technology" controlled by 5E002;
- c. Specific "software" as follows:
- c.1. **(EI CONTROLS APPLY TO THIS ITEM IF FOR EQUIPMENT CONTROLLED FOR EI)** "Software" having the characteristics, or performing or simulating the functions of the equipment, controlled by 5A002;
- c.2. **(NS/AT)** "Software" to certify "software" controlled by 5D002.c.1.

PARTIAL LIST OF ITEMS CONTROLLED UNDER 5E002

(EI CONTROLS APPLY TO THIS ITEM IF FOR COMMODITIES/SOFTWARE CONTROLLED FOR EI) "Technology" according to the General Technology Note for the "development," "production" or "use" of equipment controlled by 5A002 or 5B002 or "software" controlled by 5D002.a or 5D002.c.

Proceed to Chart 7B to determine subsequent steps.

CHART 7B

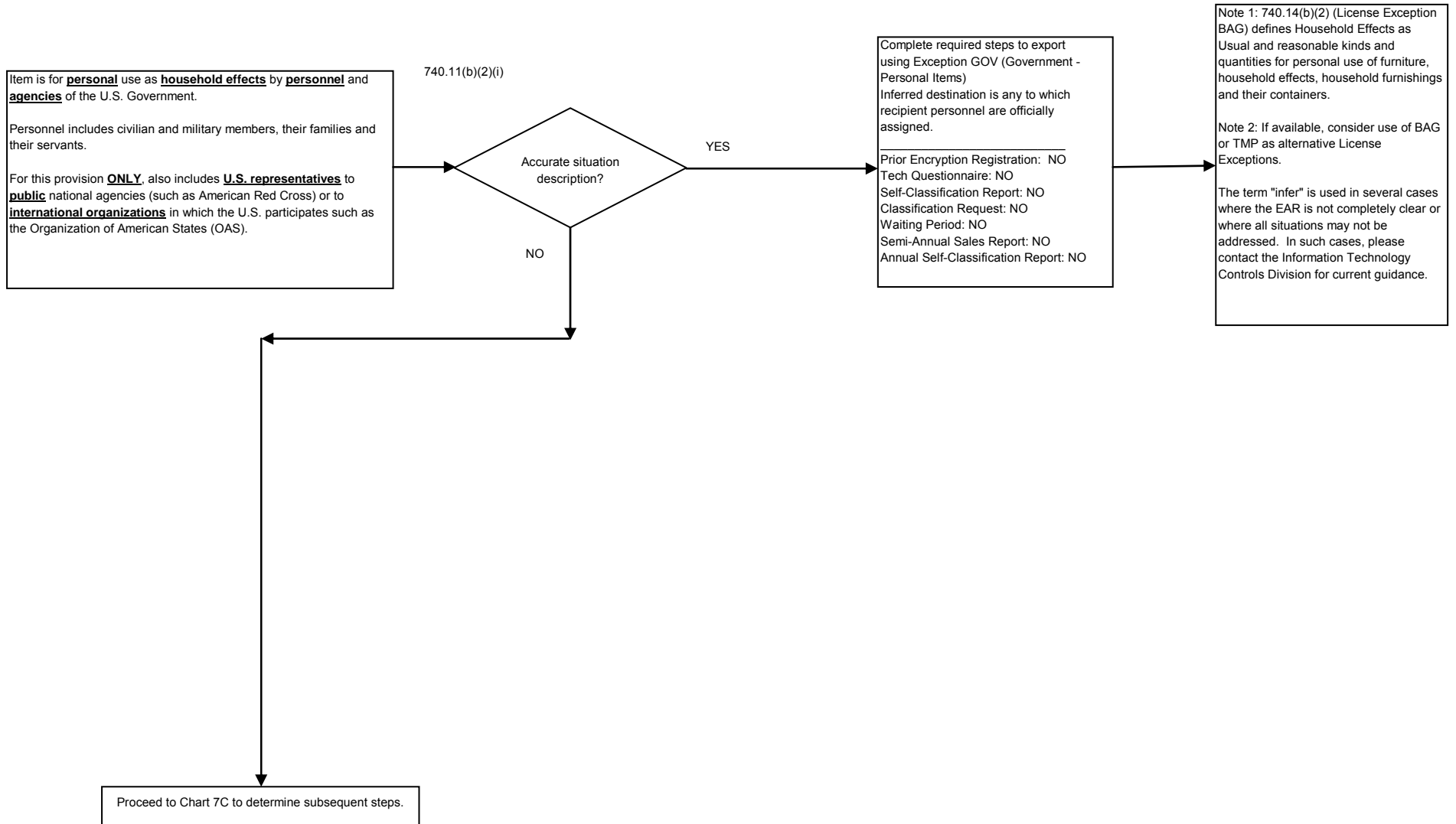


CHART 7C

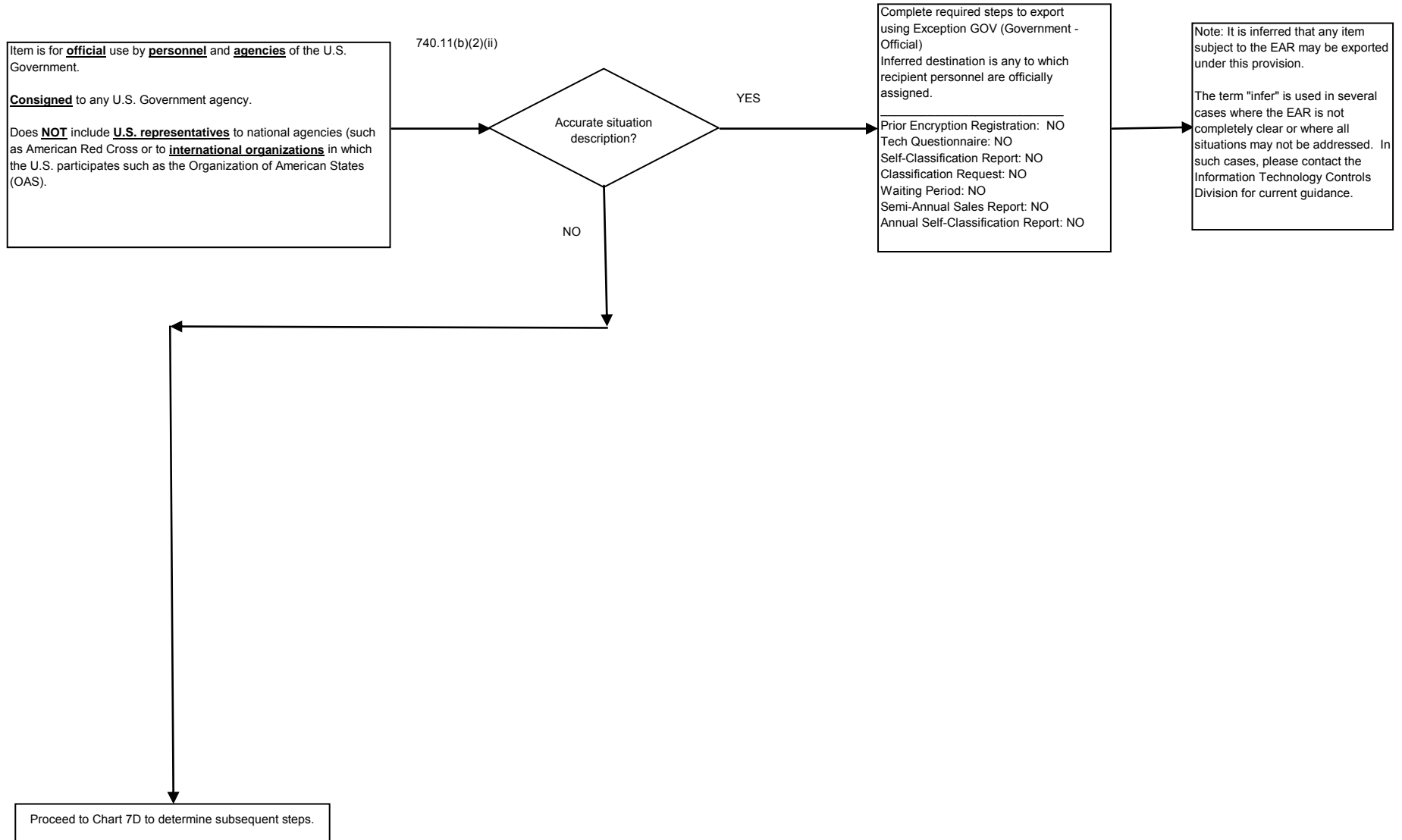


CHART 7D

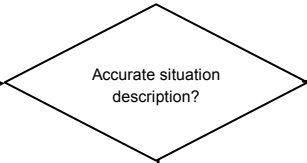
Items **consigned** to and for the **official use** within **national territory** by agencies (all civilian and military departments) of **cooperating national governments**.

Authorized destination is **only** Country Group A:1 **and** Argentina, Austria, Finland, Hong Kong, Ireland, (Republic of) Korea, New Zealand, Singapore, Sweden, Switzerland and Taiwan.

Only includes 5A002.a4, a.7, a.8 **or** 5B002 **or** 5D002.a, b, c, (for equipment **NOT** controlled for EI) **or** 5E002 (for technology **NOT** controlled for EI).

Does **NOT** include encryption items **controlled for EI** (5A002.a.1, a.2, a.5, a.6 and a.9 **or** 5D002.a, c.1 (for software to be used on equipment controlled for EI) **or** 5E002 (for technology controlled for EI)).

740.11(b)(2)(iii)



YES

Complete required steps to export using Exception GOV (Cooperating Governments)
Note Destination Requirements

Prior Encryption Registration: NO
Tech Questionnaire: NO
Self-Classification Report: NO
Classification Request: NO
Waiting Period: NO
Semi-Annual Sales Report: NO
Annual Self-Classification Report: NO

NO

Proceed to Chart 7E to determine subsequent steps.

CHART 7E

Items **consigned** to and for the **official use** of a **diplomatic or consular mission** of a **cooperating governments**.

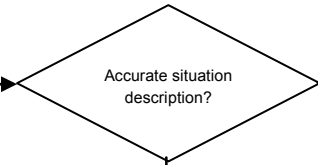
Mission is located **only** in a Group B country.

Cooperating governments include **only** Country Group A:1 **and** Argentina, Austria, Finland, Hong Kong, Ireland, (Republic of) Korea, New Zealand, Singapore, Sweden, Switzerland and Taiwan.

Only includes 5A002.4, a.7, a.8 **or** 5B002 **or** 5D002.a, b, c, (for equipment **NOT** controlled for EI) **or** 5E002 (for technology **NOT** controlled for EI).

Does **NOT** include encryption items **controlled for EI** (5A002.a.1, a.2, a.5, a.6 and a.9 **or** 5D002.a, c.1 (for software to be used on equipment controlled for EI) **or** 5E002 (for technology controlled for EI)).

740.11(b)(2)(iv)



YES

Complete required steps to export using Exception GOV (Diplomatic / Consular)
Note Destination Requirements

Prior Encryption Registration: NO
Tech Questionnaire: NO
Self-Classification Report: NO
Classification Request: NO
Waiting Period: NO
Semi-Annual Sales Report: NO
Annual Self-Classification Report: NO

NO

Proceed to Chart 8A to determine subsequent steps.

CHART 8A

MASS MARKET CRITERIA

Cat 5-2, Note 3: Cryptography Note:

ECCN's 5A002 and 5D002 do **NOT** control items that meet all of the following:

- a. Generally **available to the public** by being **sold without restriction** from stock at **retail selling points** (over-the-counter, mail order, electronic transactions, telephone transactions); AND
- b. **Cryptographic functionality** is **NOT** easily be **changed** by the user; AND
- c. Designed for **installation by the user** without further substantial support by the supplier; AND
- d. When necessary, **details are available** and will be provided upon request to the appropriate authority in the exporter's country to confirm compliance with the above.

742.15(b)(6)

EXAMPLES OF ITEMS WHICH **MAY BE ELIGIBLE** FOR MASS MARKET TREATMENT

Examples of Mass Market encryption items include **but are not limited to**:

General purpose operating systems;

Desktop applications designed for use with computers which are classified under ECCN 4A994 or designated EAR99 (such as e-mail, browsers, games, word processing, database, financial applications or utilities);

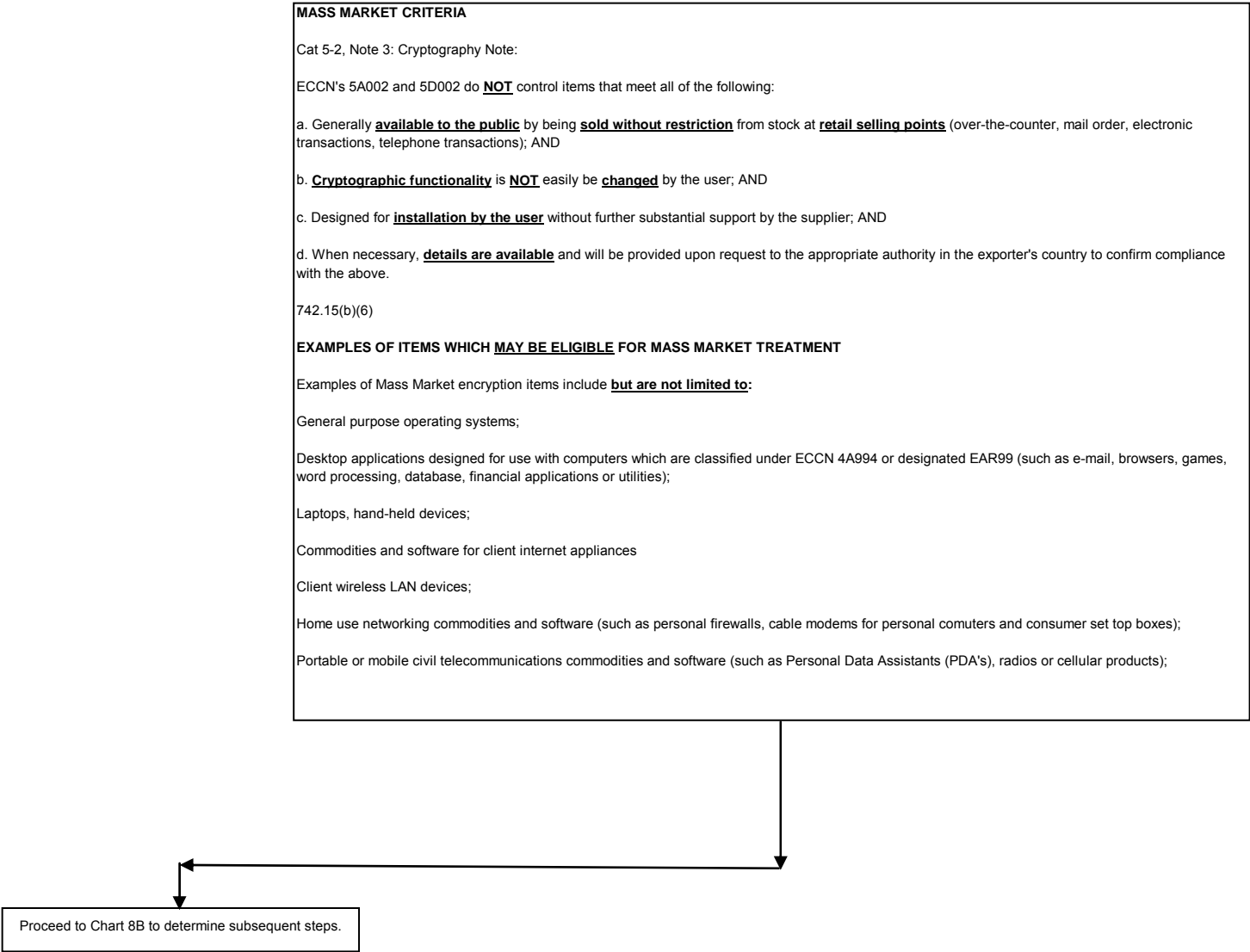
Laptops, hand-held devices;

Commodities and software for client internet appliances

Client wireless LAN devices;

Home use networking commodities and software (such as personal firewalls, cable modems for personal computers and consumer set top boxes);

Portable or mobile civil telecommunications commodities and software (such as Personal Data Assistants (PDA's), radios or cellular products);

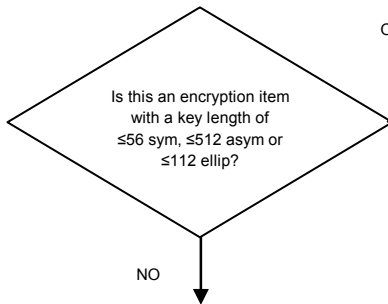


```
graph TD; A["MASS MARKET CRITERIA..."] --> B["Proceed to Chart 8B to determine subsequent steps."];
```

Proceed to Chart 8B to determine subsequent steps.

CHART 8B

Obverse of Details of Cat 5-2, 5A002 a.1.a.



YES

NO

Self-Classify as 5A992 or 5D992
 Complete required steps to export using authorization NLR.
 No E:1 Countries

Prior Encryption Registration: NO
 Tech Questionnaire: NO
 Self-Classification Report: NO
 Classification Request: NO
 Prior Review: NO
 Waiting Period: NO
 Semi-Annual Sales Report: NO
 Annual Self-Classification Report: NO

NOTE 4, CAT 5-2 EXCLUSIONS MUST MEET ALL OF THE FOLLOWING:

a. Primary function(s) is/are:

- NOT** "Information Security"; **OR**
- NOT** a computer (including operating systems, parts and components therefor); **OR**
- NOT** sending receiving or storing information (**except** in support of entertainment, mass commercial broadcasts, digital rights management or medical records management); **OR**
- NOT** networking (including operation, administration, management and provisioning). **AND**

b. Cryptographic functionality **is limited to supporting the primary function(s)**. **AND**

c. Details available to local authorities as necessary.

Item is a Smart Card or an electronically readable personal document (e.g., token coin, e-passport) for use **limited to equipment excluded from 5A002 by Note 4, Cat 5-2 above**.

Readers/writers specially designed or modified and **limited for use with these devices**.

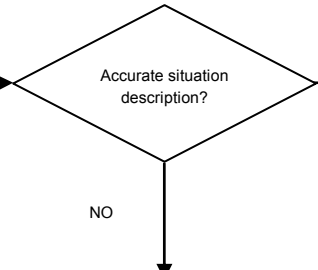
Designed for and **limited to protection of personal data within**.

Can **only** be personalized for public or commercial transactions or individual identification.

Cannot be reprogrammed for any other use.

Cryptographic functionality not user-accessible.

Cat 5-2, 5A002 Note (a)



YES

NO

Self-Classify as 5A992 or 5D992
 Complete required steps to export using authorization NLR.
 No E:1 Countries

Prior Encryption Registration: NO
 Tech Questionnaire: NO
 Self-Classification Report: NO
 Classification Request: NO
 Prior Review: NO
 Waiting Period: NO
 Semi-Annual Sales Report: NO
 Annual Self-Classification Report: NO

Technical Note 1: "Personal Data" includes any data specific to a particular person or **entity**, such as the amount of money stored and **data necessary for authentication**.

Technical Note 2: Readers/writers include equipment that **communicates with smart cards or electronically readable documents** through a network.

Proceed to Chart 8C to determine subsequent steps.

CHART 8C

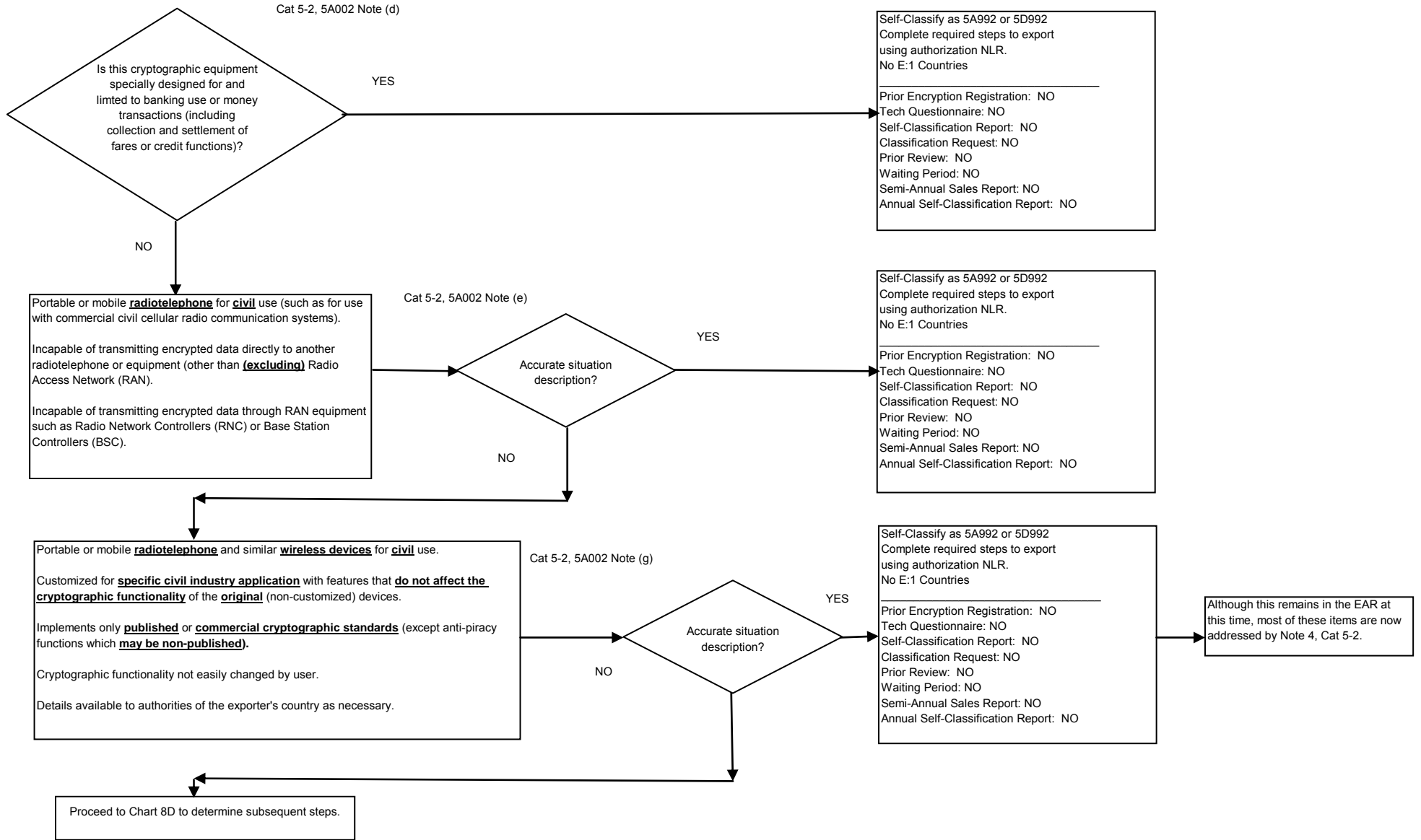
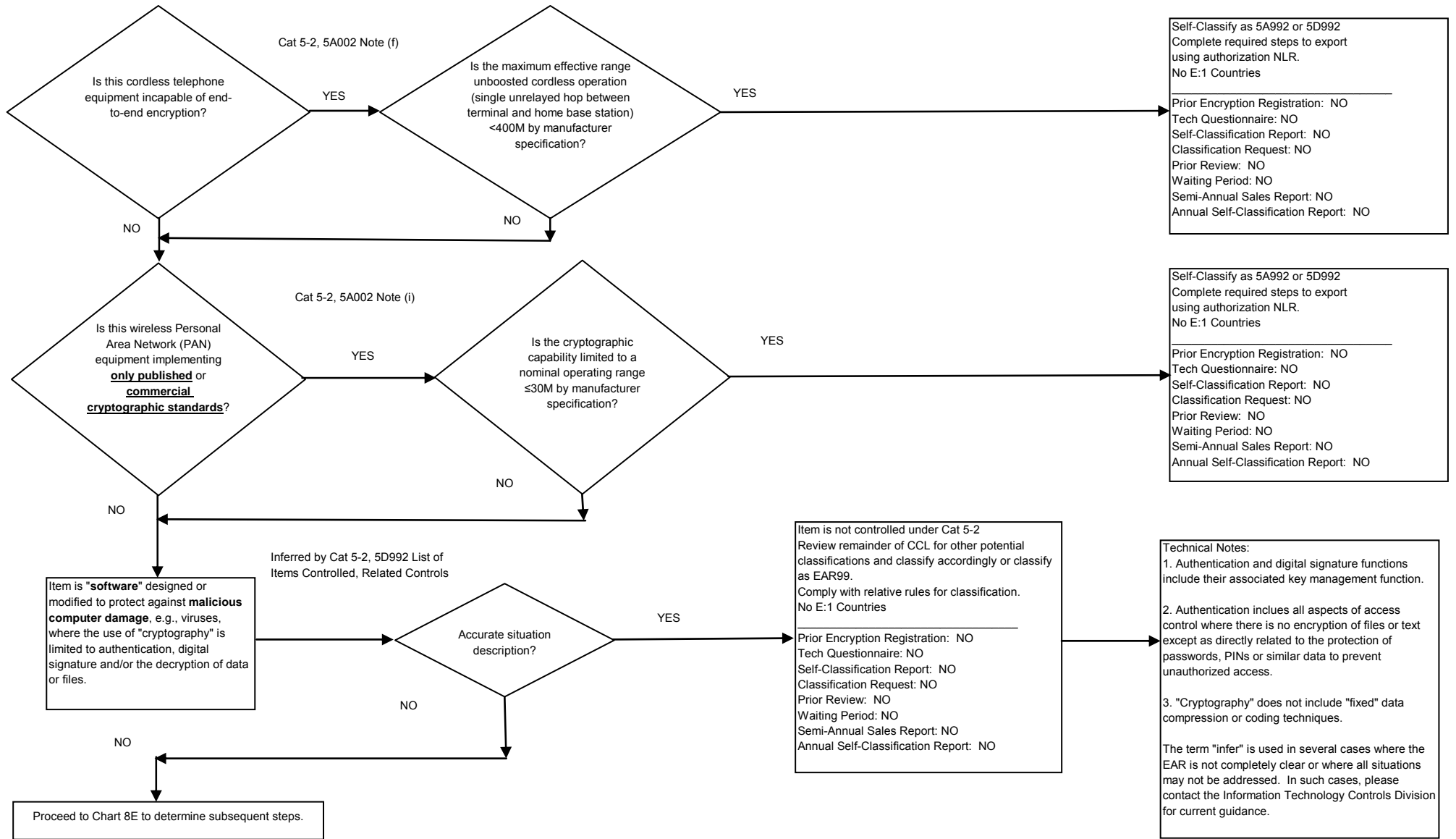


CHART 8D



Self-Classify as 5A992 or 5D992
 Complete required steps to export using authorization NLR.
 No E:1 Countries

Prior Encryption Registration: NO
 Tech Questionnaire: NO
 Self-Classification Report: NO
 Classification Request: NO
 Prior Review: NO
 Waiting Period: NO
 Semi-Annual Sales Report: NO
 Annual Self-Classification Report: NO

Self-Classify as 5A992 or 5D992
 Complete required steps to export using authorization NLR.
 No E:1 Countries

Prior Encryption Registration: NO
 Tech Questionnaire: NO
 Self-Classification Report: NO
 Classification Request: NO
 Prior Review: NO
 Waiting Period: NO
 Semi-Annual Sales Report: NO
 Annual Self-Classification Report: NO

Item is not controlled under Cat 5-2
 Review remainder of CCL for other potential classifications and classify accordingly or classify as EAR99.
 Comply with relative rules for classification.
 No E:1 Countries

Prior Encryption Registration: NO
 Tech Questionnaire: NO
 Self-Classification Report: NO
 Classification Request: NO
 Prior Review: NO
 Waiting Period: NO
 Semi-Annual Sales Report: NO
 Annual Self-Classification Report: NO

Technical Notes:

1. Authentication and digital signature functions include their associated key management function.
2. Authentication includes all aspects of access control where there is no encryption of files or text except as directly related to the protection of passwords, PINs or similar data to prevent unauthorized access.
3. "Cryptography" does not include "fixed" data compression or coding techniques.

The term "infer" is used in several cases where the EAR is not completely clear or where all situations may not be addressed. In such cases, please contact the Information Technology Controls Division for current guidance.

Item is "software" designed or modified to protect against malicious computer damage, e.g., viruses, where the use of "cryptography" is limited to authentication, digital signature and/or the decryption of data or files.

Proceed to Chart 8E to determine subsequent steps.

CHART 8E

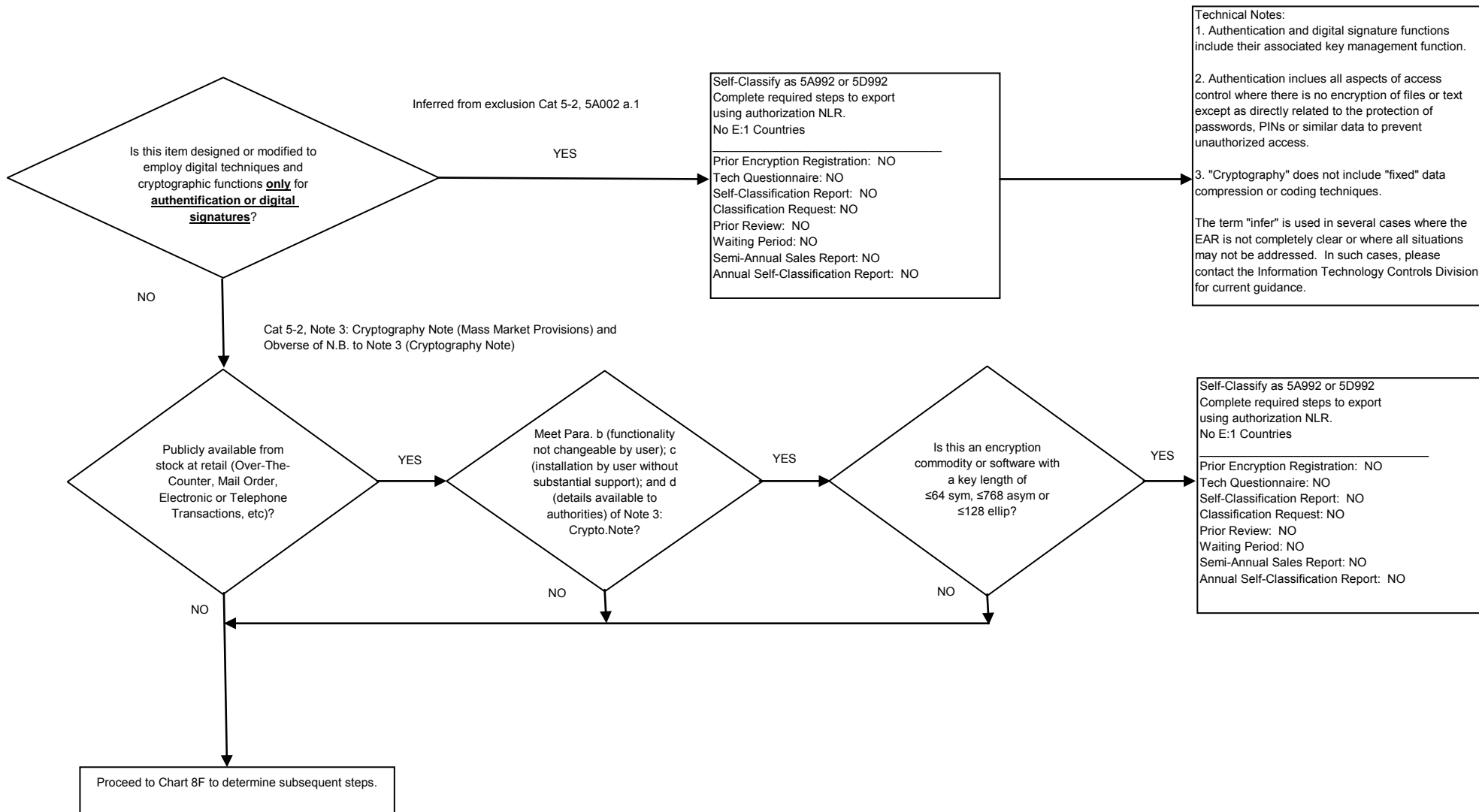


CHART 8F

Commodity or software controlled under Cat 5-2 only because it incorporates a **short-range wireless** encryption function (≤100M by manufacturer specification or IEEE 802.11 (wireless LAN standard) or 802.15.1 standard).

Item would be controlled under **another ECCN if it were not for this short-range encryption** function (e.g. a laptop controlled under 5A992 without the Short-Range Wireless might otherwise be controlled under 4A994).

May be a commodity or software with an encryption key length >64 sym, >768 asym or >128 ellip.

742.15(b)(4)(i)

Accurate situation description?

YES

NO

Self-Classify as 5A992, 5D992 or other ECCN if more stringently controlled.
 Complete required steps to export using authorization NLR if 5A/D992 (**MASS MARKET**). If under other ECCN, follow appropriate rules for that ECCN.
 No E:1 Countries

Prior Encryption Registration: NO
 Tech Questionnaire: NO
 Self-Classification Report: NO
 Classification Request: NO
 Prior Review: NO
 Waiting Period: NO
 Semi-Annual Sales Report: NO
 Annual Self-Classification Report: NO

Foreign product.

Developed with or incorporating **U.S. origin encryption** source code, components or toolkits that are subject to EAR.

U.S. origin encryption items **previously classified** or registered and authorized by BIS.

Employed cryptographic **functionality** remains **unchanged**.

Can include foreign developed products designed to operate with U.S. products through a **cryptographic interface**.

U.S. origin encryption functionality may employ a key length of >64 sym, >768 asym or >128 ellip.

742.15(b)(4)(ii) and 734.4(a) and (b)

Accurate situation description?

YES

NO

Exported from a country **other than the U.S.**?

YES

NO

Self-Classify as 5A992, 5D992 or other ECCN if more stringently controlled.
 Complete required steps to export using authorization NLR if 5A/D992 (**MASS MARKET**). If under other ECCN, follow appropriate rules for that ECCN.
 No E:1 Countries

Prior Encryption Registration: NO
 Tech Questionnaire: NO
 Self-Classification Report: NO
 Classification Request: NO
 Prior Review: NO
 Waiting Period: NO
 Semi-Annual Sales Report: NO
 Annual Self-Classification Report: NO

Export of these items **from the United States** is not permitted under this provision.

Proceed to Chart 9A to determine subsequent steps.



List Based License Exceptions

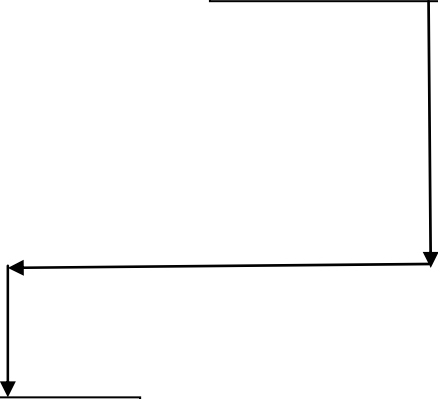
These are license exceptions which **might** be available in a particular situation to overcome a requirement for a license but **only** under the conditions **specifically stated** at the particular Commerce Control List (CCL) entry.

List based License Exceptions which **might sometimes** be available are:

- Shipments of Limited Value (LVS)
- Shipments to Country Group B (GBS)
- Civil End-Users (CIV)
- Technology and Software under Restriction (TSR)
- Computers of a specified Adjusted Peak Performance (APP)
- Encryption Commodities, Software and Tecnology (ENC)

For products controlled under Cat 5-2, **only two** of these list based exceptions **might** be available.

These are **LVS** and **ENC**.



Proceed to Chart 9B to determine subsequent steps.

CHART 9B

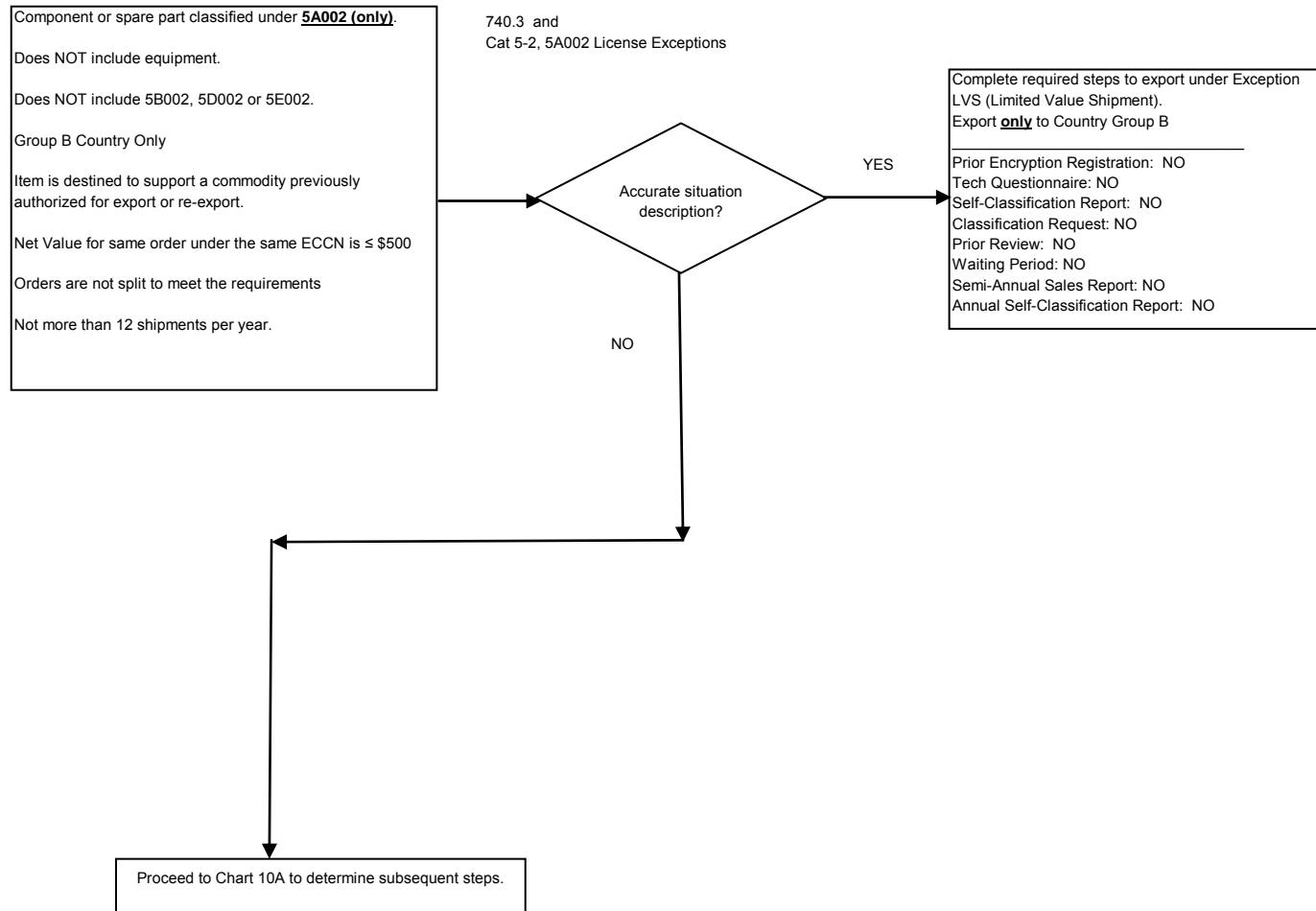


CHART 10A

PARTIAL LIST OF ITEMS CONTROLLED UNDER 5A002

This is **ONLY** a partial listing provided for immediate reference in training. Do **NOT** take export action based upon this information. Refer instead to the current version of Category 5, Part 2 of the EAR.

- a. Systems, equipment, application specific "electronic assemblies," modules and integrated circuits for "information security," as follows, and components therefor specially designed for "information security":
- a.1. **(E/NS/AT)** Designed or modified to use "cryptography" employing digital techniques performing any **cryptographic function other than authentication or digital signature and** having any of the following:
- a.1.a. A "**symmetric** algorithm" employing a key length in **excess of 56-bits**; or
- a.1.b. An "**asymmetric** algorithm" where the security of the algorithm is based on any of the following:
- a.1.b.1. Factorization of integers in **excess of 512 bits** (e.g., RSA);
- a.1.b.2. Computation of discrete logarithms in a multiplicative group of a finite field of size **greater than 512 bits** (e.g., Diffie-Hellman over Z/pZ); or
- a.1.b.3. Discrete logarithms in a group other than mentioned in 5A002.a.1.b.2 in **excess of 112 bits** (e.g., Diffie-Hellman over an **elliptic curve**);
- a.2. **(E/NS/AT)** Designed or modified to perform **cryptanalytic functions**;
- a.4. **(NS/AT)** Specially designed or modified to reduce the compromising emanations of information bearing signals beyond what is necessary for health, safety or electromagnetic interference standards;
- a.5. **(E/NS/AT)** Designed or modified to use cryptographic techniques to **generate the spreading code for "spread spectrum" systems**, not controlled in 5A002.a.6., including the **hopping code** for "frequency hopping" systems;
- a.6. **(E/NS/AT)** Designed or modified to use cryptographic techniques to **generate channelizing codes, scrambling codes or network identification codes**, for systems using **ultra-wideband modulation** techniques **and** having any of the following:
- a.6.a. A **bandwidth** exceeding **500 MHz**; or
- a.6.b. A "**fractional bandwidth**" of **20%** or more;
- a.7. **(NS/AT)** Non-cryptographic information and communications technology (ICT) security systems and devices evaluated to an assurance level exceeding class EAL-6;
- a.8. **(NS/AT)** Communications cable systems designed or modified using mechanical, electrical or electronic means to detect surreptitious intrusion;
- a.9. **(E/NS/AT)** Designed or modified to use '**quantum cryptography**.'

PARTIAL LIST OF ITEMS CONTROLLED UNDER 5B002

- a. **(NS/AT)** Equipment specially designed for the "development" or "production" of equipment controlled by 5A002 or 5B002.b;
- b. **(NS/AT)** Measuring equipment specially designed to evaluate and validate the "information security" functions of equipment controlled by 5A002 or "software" controlled by 5D002.a or 5D002.c.

PARTIAL LIST OF ITEMS CONTROLLED UNDER 5D002

- a. **(EI CONTROLS APPLY TO THIS ITEM IF FOR EQUIPMENT CONTROLLED FOR EI)** "Software" specially designed or modified for the "development", "production" or "use" of equipment controlled by 5A002 or "software" controlled by 5D002.c;
- b. **(NS/AT)** "Software" specially designed or modified to support "technology" controlled by 5E002;
- c. Specific "software" as follows:
- c.1. **(EI CONTROLS APPLY TO THIS ITEM IF FOR EQUIPMENT CONTROLLED FOR EI)** "Software" having the characteristics, or performing or simulating the functions of the equipment, controlled by 5A002;
- c.2. **(NS/AT)** "Software" to certify "software" controlled by 5D002.c.1.

PARTIAL LIST OF ITEMS CONTROLLED UNDER 5E002

(EI CONTROLS APPLY TO THIS ITEM IF FOR COMMODITIES/SOFTWARE CONTROLLED FOR EI) "Technology" according to the General Technology Note for the "development," "production" or "use" of equipment controlled by 5A002 or 5B002 or "software" controlled by 5D002.a or 5D002.c.

Proceed to Chart 10B to determine subsequent steps.

CHART 10B

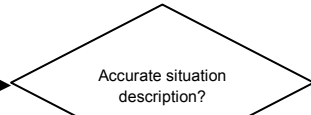
5A002.a.1, a.2, a.5, a.6, a.9 and 5B002 and equivalent or related software and technology under 5D002 or 5E002.

Export/Reexport to "**private sector**" end-users **wherever located** provided they are **headquartered in a Supp 3 country**.

End-use is **internal development or production of new products** by those end-users.

Not acting for, controlled by or wholly owned by a **foreign government**.

740.17 (a)(1)



YES

Complete required steps to export under Exception ENC (Internal Development)
No E:1 Countries

Prior Encryption Registration: NO
Tech Questionnaire: NO
Self-Classification Report: NO
Classification Request: NO
Waiting Period: NO
Semi-Annual Sales Report: NO
Annual Self-Classification Report: NO

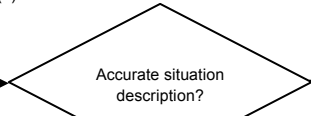
Resulting products ARE **SUBJECT TO EAR**.
Encryption Registration and Classification Request **MAY BE** required prior to sale, reexport or transfer of resulting products.

5A002.a.1, a.2, a.5, a.6, a.9 and systems and components therefor under 5B002 and equivalent or related software and technology under 5D002 or 5E002.

Export/Reexport to any **U.S. subsidiary** wherever located.

Export/Reexport by U.S. company and its subsidiaries to **foreign nationals who are employees, contractors or interns** of the U.S. company/subsidiary provided items are used for internal company use including (but not limited to) development/production of new products.

740.17 (a)(2)



YES

Complete required steps to export under ENC (U.S. Subsidiaries)
No E:1 Countries

Prior Encryption Registration: NO
Tech Questionnaire: NO
Self-Classification Report: NO
Classification Request: NO
Waiting Period: NO
Semi-Annual Sales Report: NO
Annual Self-Classification Report: NO

Resulting products ARE **SUBJECT TO EAR**.
Encryption Registration and Classification Request **MAY BE** required prior to sale, reexport or transfer of resulting products to **non-U.S. subsidiaries**.

Proceed to Chart 10C to determine subsequent steps.

CHART 10C

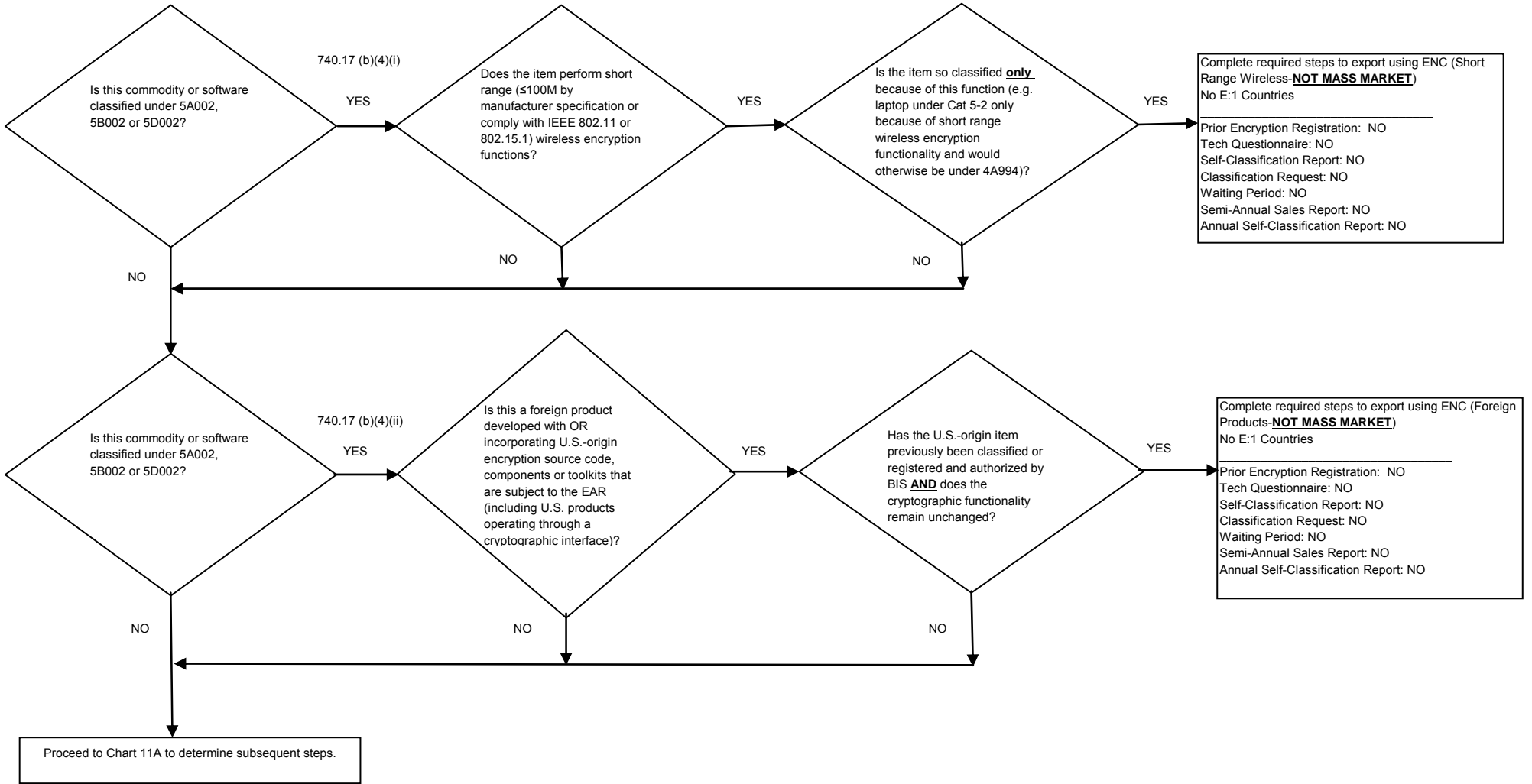
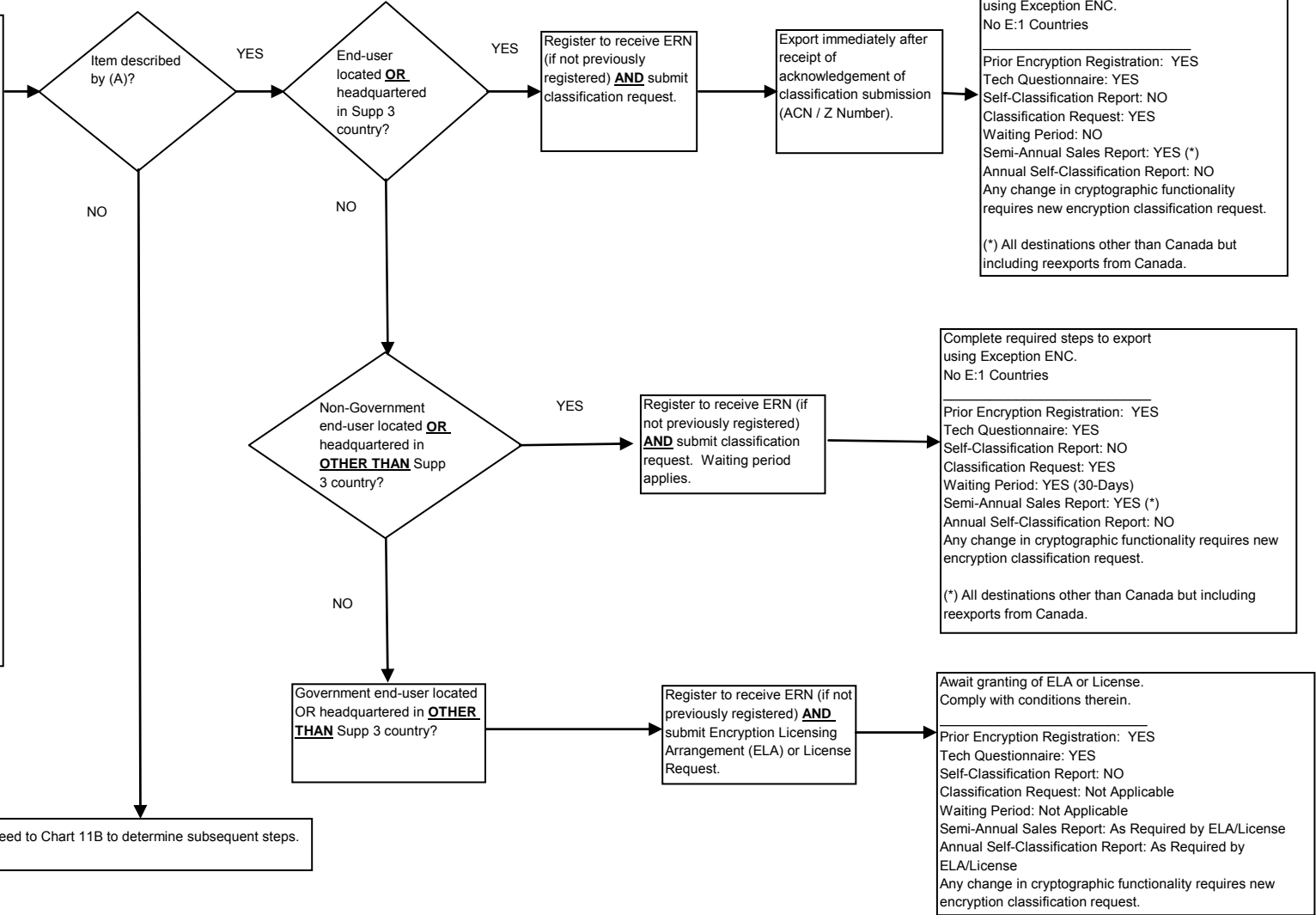


CHART 11A

740.17 (b) (2)(i)(A)

Cryptographic commodities, software and components.
 (A) Network infrastructure software and commodities and components thereof (including those necessary to activate or enable cryptographic functionality in network infrastructure products) providing WAN, MAN, VPN, satellite, digital packet telephony/media (voice, video, data) over internet protocol, cellular or trunked communications meeting **ANY** of the following **AND** with key lengths >80 bits sym (asym & ellip not addressed):
 (1) Aggregate encrypted WAN, MAN, VPN or backhaul throughput >90 Mbps (including communications through wireless network elements (gateways, mobile switches, controllers, etc.)); **OR**
 (2) Wire (line), cable or fiber optic WAN, MAN or VPN single channel input data rate >154 Mbps; **OR**
 (3) Transmission over satellite at data rates exceeding 10 Mbps; **OR**
 (4) Media (voice/video/data) encryption or centralized key management supporting >250 concurrent encrypted data channels, **OR** encrypted signalling to >1,000 endpoints for digital packet telephony/media (voice/video/data) over internet protocol communications; **OR**
 (5) Air interface coverage (e.g. through base stations, access points to mesh networks, bridges, etc.) >1,000M **AND** where **ANY** of the following apply:
 (i) Maximum transmission data rates >10 Mbps at operating ranges >1,000M; **OR**
 (ii) Maximum number of concurrent full-duplex voice channels >30; **OR**
 (iii) Substantial support is required for installation or use.

Proceed to Chart 11B to determine subsequent steps.



Complete required steps to export using Exception ENC.
 No E:1 Countries
 Prior Encryption Registration: YES
 Tech Questionnaire: YES
 Self-Classification Report: NO
 Classification Request: YES
 Waiting Period: NO
 Semi-Annual Sales Report: YES (*)
 Annual Self-Classification Report: NO
 Any change in cryptographic functionality requires new encryption classification request.
 (*) All destinations other than Canada but including reexports from Canada.

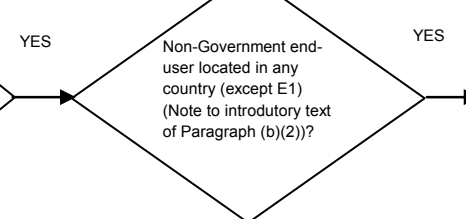
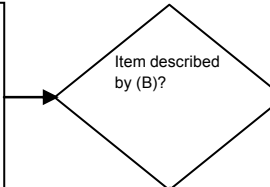
Complete required steps to export using Exception ENC.
 No E:1 Countries
 Prior Encryption Registration: YES
 Tech Questionnaire: YES
 Self-Classification Report: NO
 Classification Request: YES
 Waiting Period: YES (30-Days)
 Semi-Annual Sales Report: YES (*)
 Annual Self-Classification Report: NO
 Any change in cryptographic functionality requires new encryption classification request.
 (*) All destinations other than Canada but including reexports from Canada.

Await granting of ELA or License. Comply with conditions therein.
 Prior Encryption Registration: YES
 Tech Questionnaire: YES
 Self-Classification Report: NO
 Classification Request: Not Applicable
 Waiting Period: Not Applicable
 Semi-Annual Sales Report: As Required by ELA/License
 Annual Self-Classification Report: As Required by ELA/License
 Any change in cryptographic functionality requires new encryption classification request.

CHART 11B

740.17 (b) (2)(i)(B)

Cryptographic commodities, software and components.
 (B) Encryption source code that would not be eligible for export or reexport under License Exception TSU because it is **NOT PUBLICLY AVAILABLE** as that term is used in 740.13(e)(1).
 740.13(e)(1) further refers to 734.3(b)(3).
 734.3(b)(3) states that the following items are **NOT** subject to the EAR:
 Publicly available **technology and software** excludes software controlled for EI reasons under 5D002 **AND** mass market encryption software >64-bits sym (asym & ellip not addressed) and controlled under 5D992. However, it does include software and technology that:
 (i) Are already published or will be published (734.7); **OR**
 (ii) Arise or result from fundamental research (734.8); **OR**
 (iii) Are educational (734.9); **OR**
 (iv) Are included in certain patent applications (734.10).
 Note to 734.3(b)(2) and (b)(3) states that encryption source code in a printed book or other printed material is **NOT** itself subject to the EAR. However, such code in an electronic form or media remains subject to the EAR.



Register to receive ERN (if not previously registered) **AND** submit classification request.

Export immediately after receipt of acknowledgement of classification submission (ACN / Z Number).

Complete required steps to export using Exception ENC.
 No E:1 Countries

Prior Encryption Registration: YES
 Tech Questionnaire: YES
 Self-Classification Report: NO
 Classification Request: YES
 Waiting Period: NO
 Semi-Annual Sales Report: YES (*)
 Annual Self-Classification Report: NO
 Any change in cryptographic functionality requires new encryption classification request.

(*) All destinations other than Canada but including reexports from Canada.

Government end-user located in any country.

Register to receive ERN (if not previously registered) **AND** submit Encryption Licensing Arrangement (ELA) or License Request.

Await granting of ELA or License. Comply with conditions therein.

Prior Encryption Registration: YES
 Tech Questionnaire: YES
 Self-Classification Report: NO
 Classification Request: Not Applicable
 Waiting Period: Not Applicable
 Semi-Annual Sales Report: As Required by ELA/License
 Annual Self-Classification Report: As Required by ELA/License
 Any change in cryptographic functionality requires new encryption classification request.

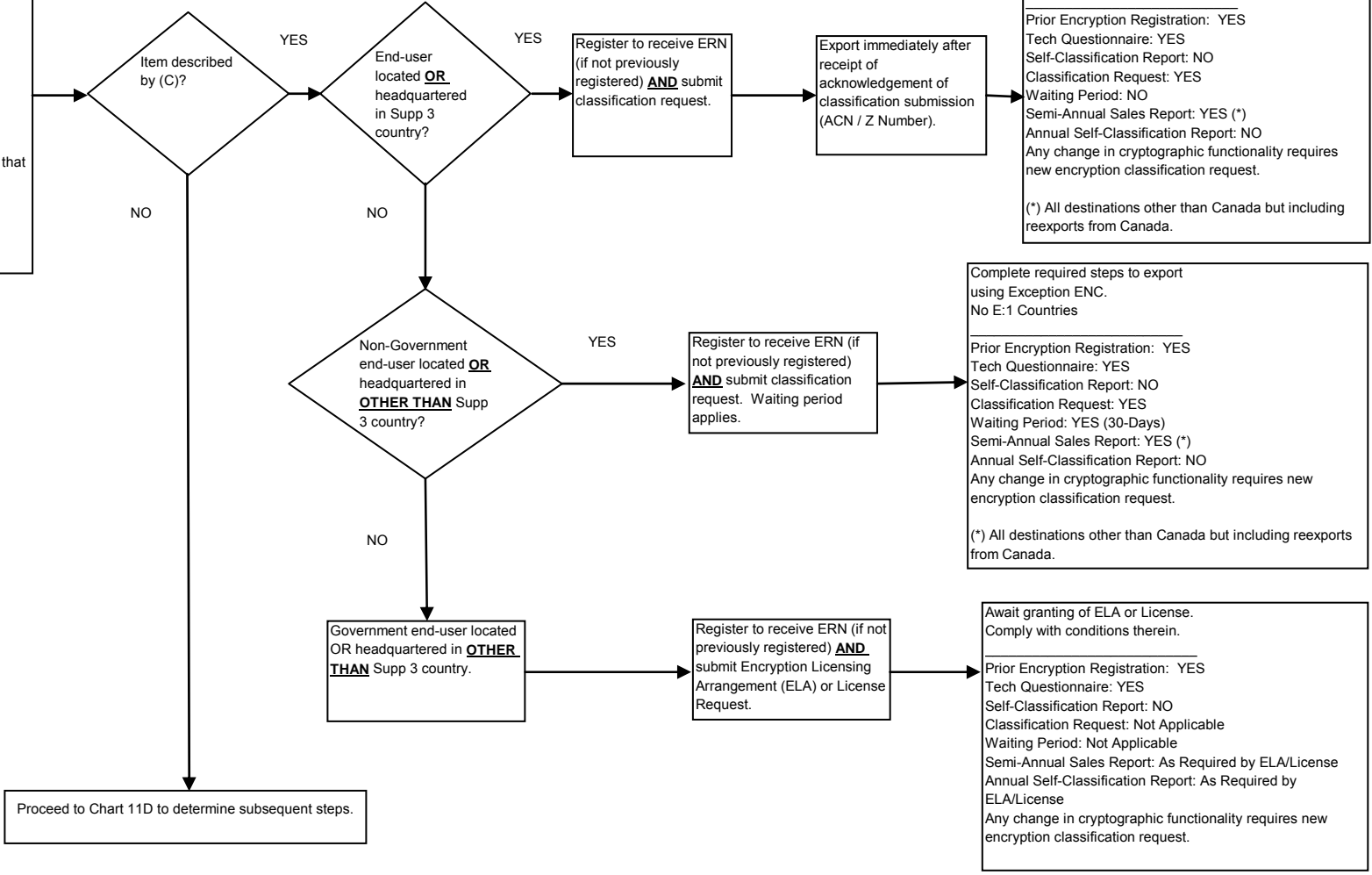
Proceed to Chart 11C to determine subsequent steps.

CHART 11C

Cryptographic commodities, software and components.
 (C) Encryption software, commodities and components therefor that have **ANY** of the following characteristics:

- (1) Designed, modified, adapted or customized for government end-users; **OR**
- (2) Cryptographic functionality has been modified or customized to customer specification; **OR**
- (3) Cryptographic functionality or encryption component that is user-accessible and can be easily changed by user (excluding publicly available encryption software (740.13(e)(1)).

740.17 (b) (2)(i)(C)



Complete required steps to export using Exception ENC.
 No E:1 Countries

Prior Encryption Registration: YES
 Tech Questionnaire: YES
 Self-Classification Report: NO
 Classification Request: YES
 Waiting Period: NO
 Semi-Annual Sales Report: YES (*)
 Annual Self-Classification Report: NO
 Any change in cryptographic functionality requires new encryption classification request.
 (*) All destinations other than Canada but including reexports from Canada.

Complete required steps to export using Exception ENC.
 No E:1 Countries

Prior Encryption Registration: YES
 Tech Questionnaire: YES
 Self-Classification Report: NO
 Classification Request: YES
 Waiting Period: YES (30-Days)
 Semi-Annual Sales Report: YES (*)
 Annual Self-Classification Report: NO
 Any change in cryptographic functionality requires new encryption classification request.
 (*) All destinations other than Canada but including reexports from Canada.

Await granting of ELA or License.
 Comply with conditions therein.

Prior Encryption Registration: YES
 Tech Questionnaire: YES
 Self-Classification Report: NO
 Classification Request: Not Applicable
 Waiting Period: Not Applicable
 Semi-Annual Sales Report: As Required by ELA/License
 Annual Self-Classification Report: As Required by ELA/License
 Any change in cryptographic functionality requires new encryption classification request.

Proceed to Chart 11D to determine subsequent steps.

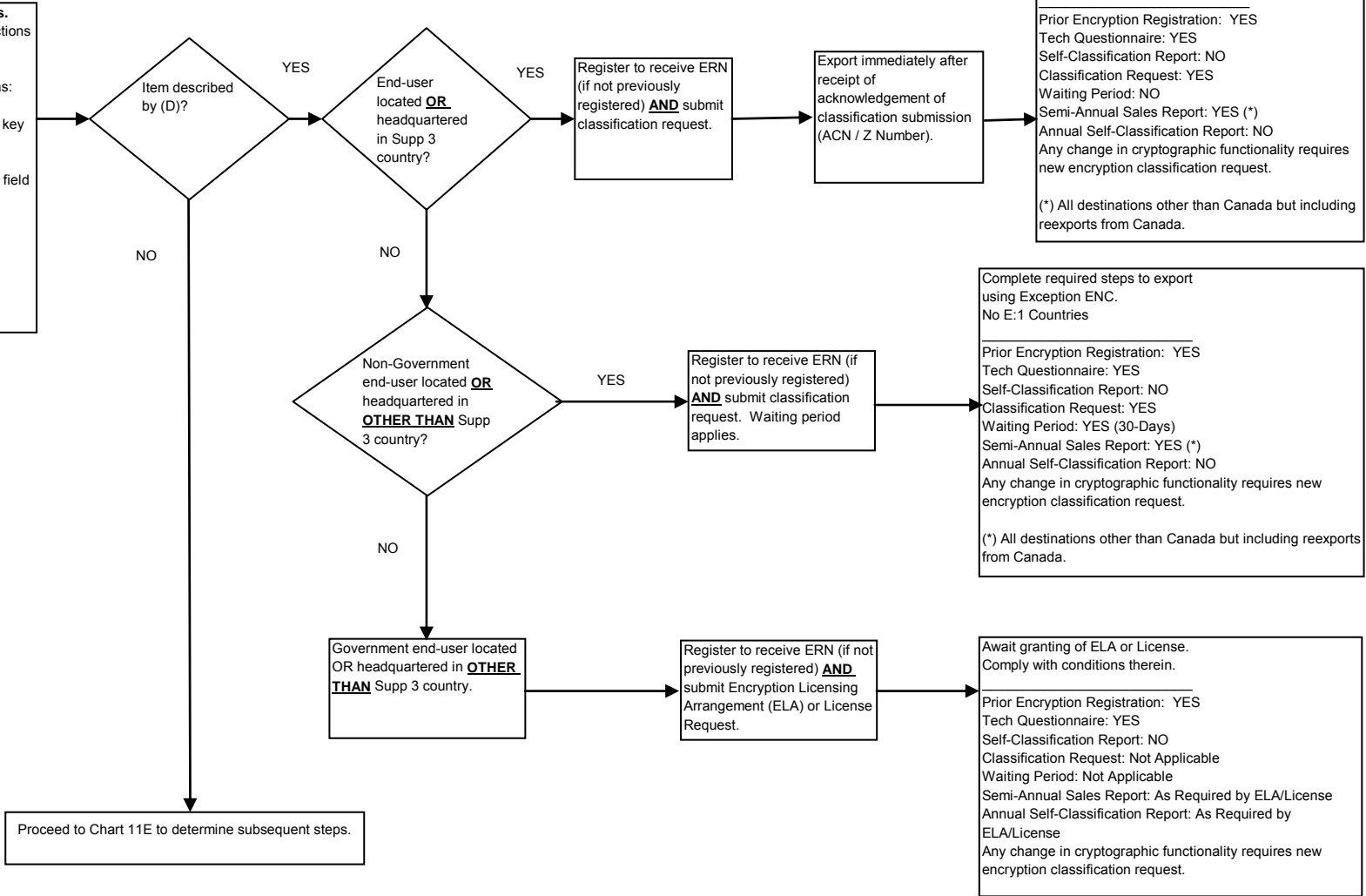
CHART 11D

740.17 (b) (2)(i)(D)

Cryptographic commodities, software and components.
 (D) Encryption commodities and software that provide functions necessary for Quantum Cryptography.

Technical Notes to 5A002 define Quantum Cryptography as:

1. A family of techniques for the establishment of a shared key for "cryptography" by measuring the quantum-mechanical properties of a physical system including those physical properties explicitly governed by quantum optics, quantum field theory or quantum electrodynamics.
2. Quantum cryptography is also known as Quantum Key Distribution (QKD).



Complete required steps to export using Exception ENC.
 No E:1 Countries

Prior Encryption Registration: YES
 Tech Questionnaire: YES
 Self-Classification Report: NO
 Classification Request: YES
 Waiting Period: NO
 Semi-Annual Sales Report: YES (*)
 Annual Self-Classification Report: NO
 Any change in cryptographic functionality requires new encryption classification request.

(*) All destinations other than Canada but including reexports from Canada.

Complete required steps to export using Exception ENC.
 No E:1 Countries

Prior Encryption Registration: YES
 Tech Questionnaire: YES
 Self-Classification Report: NO
 Classification Request: YES
 Waiting Period: YES (30-Days)
 Semi-Annual Sales Report: YES (*)
 Annual Self-Classification Report: NO
 Any change in cryptographic functionality requires new encryption classification request.

(*) All destinations other than Canada but including reexports from Canada.

Await granting of ELA or License. Comply with conditions therein.

Prior Encryption Registration: YES
 Tech Questionnaire: YES
 Self-Classification Report: NO
 Classification Request: Not Applicable
 Waiting Period: Not Applicable
 Semi-Annual Sales Report: As Required by ELA/License
 Annual Self-Classification Report: As Required by ELA/License
 Any change in cryptographic functionality requires new encryption classification request.

Proceed to Chart 11E to determine subsequent steps.

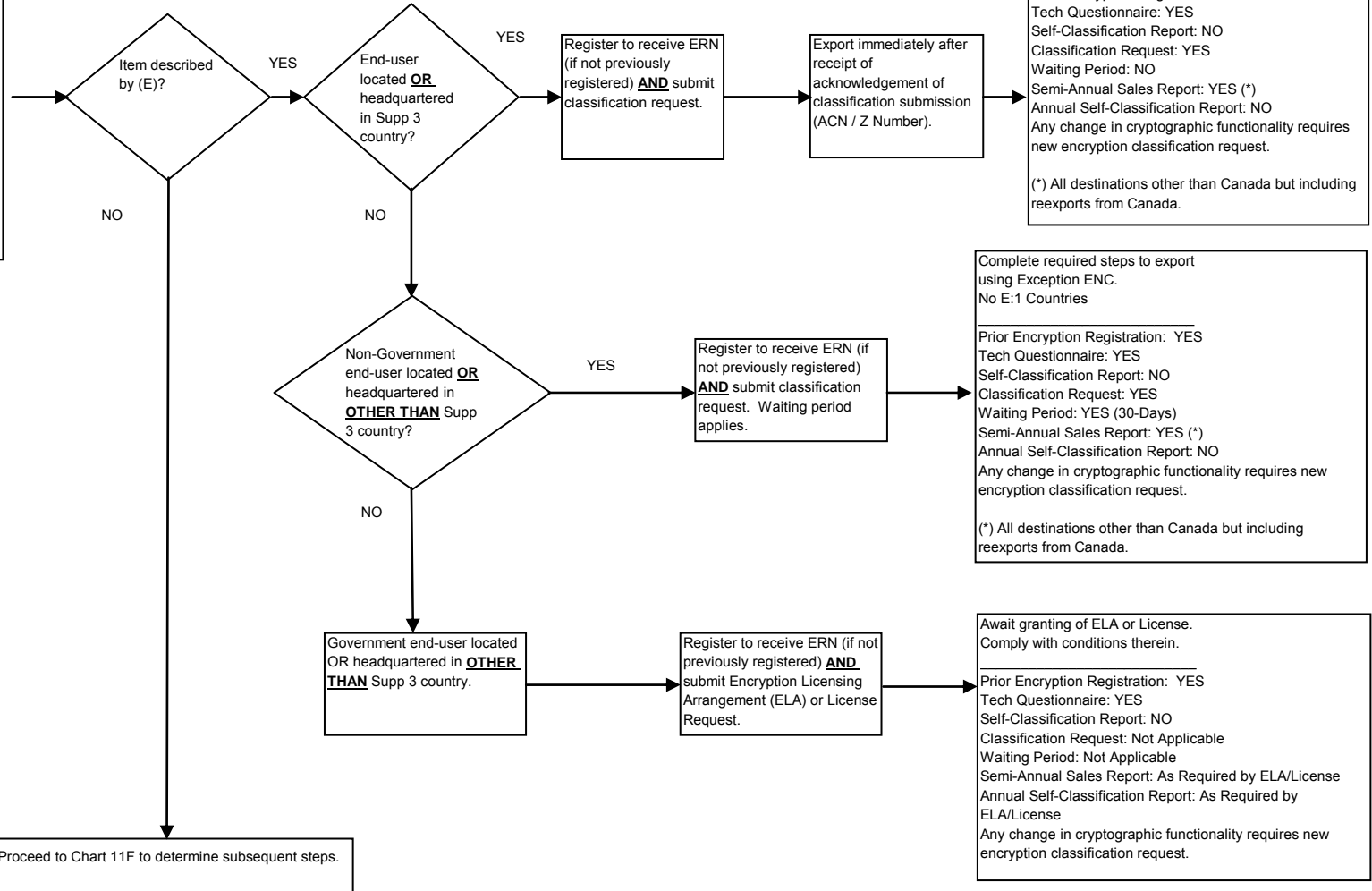
CHART 11E

Cryptographic commodities, software and components.
 (E) Encryption commodities and software that have been modified or customized for use with computers classified under 4A003

The CCL defines 4A003 as "Digital computers," "electronic assemblies" and related equipment therefor and specially designed components therefor.

It includes Vector processors, Digital Signal processors, Logic processors, Equipment designed for "image enhancement," and Equipment designed for "signal processing."

740.17 (b) (2)(i)(E)



Complete required steps to export using Exception ENC.
 No E:1 Countries

Prior Encryption Registration: YES
 Tech Questionnaire: YES
 Self-Classification Report: NO
 Classification Request: YES
 Waiting Period: NO
 Semi-Annual Sales Report: YES (*)
 Annual Self-Classification Report: NO
 Any change in cryptographic functionality requires new encryption classification request.

(*) All destinations other than Canada but including reexports from Canada.

Complete required steps to export using Exception ENC.
 No E:1 Countries

Prior Encryption Registration: YES
 Tech Questionnaire: YES
 Self-Classification Report: NO
 Classification Request: YES
 Waiting Period: YES (30-Days)
 Semi-Annual Sales Report: YES (*)
 Annual Self-Classification Report: NO
 Any change in cryptographic functionality requires new encryption classification request.

(*) All destinations other than Canada but including reexports from Canada.

Await granting of ELA or License. Comply with conditions therein.

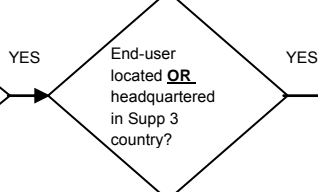
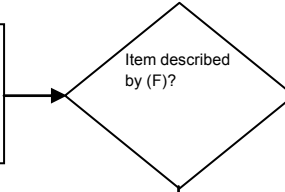
Prior Encryption Registration: YES
 Tech Questionnaire: YES
 Self-Classification Report: NO
 Classification Request: Not Applicable
 Waiting Period: Not Applicable
 Semi-Annual Sales Report: As Required by ELA/License
 Annual Self-Classification Report: As Required by ELA/License
 Any change in cryptographic functionality requires new encryption classification request.

Proceed to Chart 11F to determine subsequent steps.

CHART 11F

740.17 (b) (2)(i)(F)

Cryptographic commodities, software and components.
 (F) Encryption commodities and software that provide penetration capabilities that are capable of attacking, denying, disrupting or otherwise impairing the use of cyber infrastructure or networks.



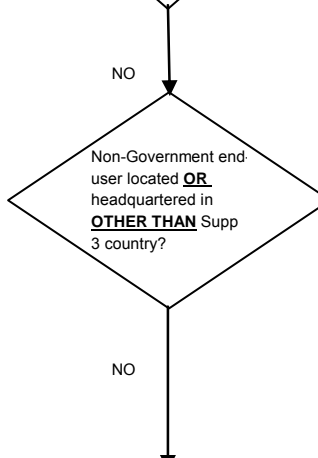
Register to receive ERN (if not previously registered) **AND** submit classification request.

Export immediately after receipt of acknowledgement of classification submission (ACN / Z Number).

Complete required steps to export using Exception ENC.
 No E:1 Countries

Prior Encryption Registration: YES
 Tech Questionnaire: YES
 Self-Classification Report: NO
 Classification Request: YES
 Waiting Period: NO
 Semi-Annual Sales Report: YES (*)
 Annual Self-Classification Report: NO
 Any change in cryptographic functionality requires new encryption classification request.

(*) All destinations other than Canada but including reexports from Canada.



Register to receive ERN (if not previously registered) **AND** submit classification request. Waiting period applies.

Complete required steps to export using Exception ENC.
 No E:1 Countries

Prior Encryption Registration: YES
 Tech Questionnaire: YES
 Self-Classification Report: NO
 Classification Request: YES
 Waiting Period: YES (30-Days)
 Semi-Annual Sales Report: YES (*)
 Annual Self-Classification Report: NO
 Any change in cryptographic functionality requires new encryption classification request.

(*) All destinations other than Canada but including reexports from Canada.

Government end-user located **OR** headquartered in **OTHER THAN** Supp 3 country.

Register to receive ERN (if not previously registered) **AND** submit Encryption Licensing Arrangement (ELA) or License Request.

Await granting of ELA or License. Comply with conditions therein.

Prior Encryption Registration: YES
 Tech Questionnaire: YES
 Self-Classification Report: NO
 Classification Request: Not Applicable
 Waiting Period: Not Applicable
 Semi-Annual Sales Report: As Required by ELA/License
 Annual Self-Classification Report: As Required by ELA/License
 Any change in cryptographic functionality requires new encryption classification request.

Proceed to Chart 11G to determine subsequent steps.

CHART 11G

740.17 (b) (2)(i)(G)

Cryptographic commodities, software and components.
 (G) Public safety / first responder radio (e.g., implementing Terrestrial Trunked Radio (TETRA) and/or Association of Public-Safety Communications Officials International (APCO) Project 25 (P25) standards).

Item described by (G)?

NO

Proceed to Chart 12A to determine subsequent steps.

End-user located OR headquartered in Supp 3 country?

YES

YES

Register to receive ERN (if not previously registered) **AND** submit classification request.

Export immediately after receipt of acknowledgement of classification submission (ACN / Z Number).

Complete required steps to export using Exception ENC.
 No E:1 Countries

Prior Encryption Registration: YES
 Tech Questionnaire: YES
 Self-Classification Report: NO
 Classification Request: YES
 Waiting Period: NO
 Semi-Annual Sales Report: YES (*)
 Annual Self-Classification Report: NO
 Any change in cryptographic functionality requires new encryption classification request.

(*) All destinations other than Canada but including reexports from Canada.

NO

Non-Government end-user located OR headquartered in **OTHER THAN** Supp 3 country?

YES

Register to receive ERN (if not previously registered) **AND** submit classification request. Waiting period applies.

Complete required steps to export using Exception ENC.
 No E:1 Countries

Prior Encryption Registration: YES
 Tech Questionnaire: YES
 Self-Classification Report: NO
 Classification Request: YES
 Waiting Period: YES (30-Days)
 Semi-Annual Sales Report: YES (*)
 Annual Self-Classification Report: NO
 Any change in cryptographic functionality requires new encryption classification request.

(*) All destinations other than Canada but including reexports from Canada.

NO

Government end-user located OR headquartered in **OTHER THAN** Supp 3 country.

Register to receive ERN (if not previously registered) **AND** submit Encryption Licensing Arrangement (ELA) or License Request.

Await granting of ELA or License. Comply with conditions therein.

Prior Encryption Registration: YES
 Tech Questionnaire: YES
 Self-Classification Report: NO
 Classification Request: Not Applicable
 Waiting Period: Not Applicable
 Semi-Annual Sales Report: As Required by ELA/License
 Annual Self-Classification Report: As Required by ELA/License
 Any change in cryptographic functionality requires new encryption classification request.

CHART 12A

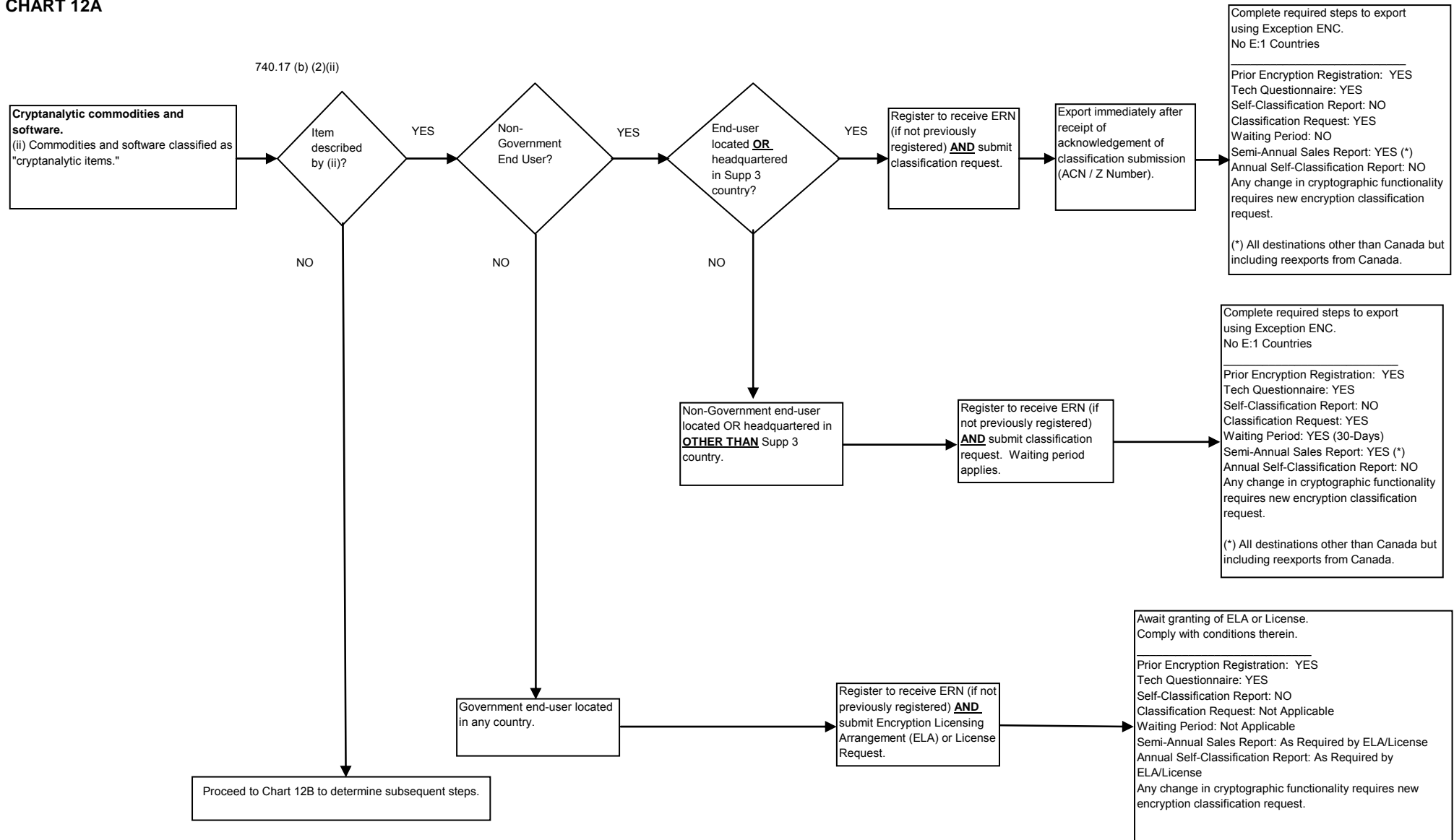


CHART 12B

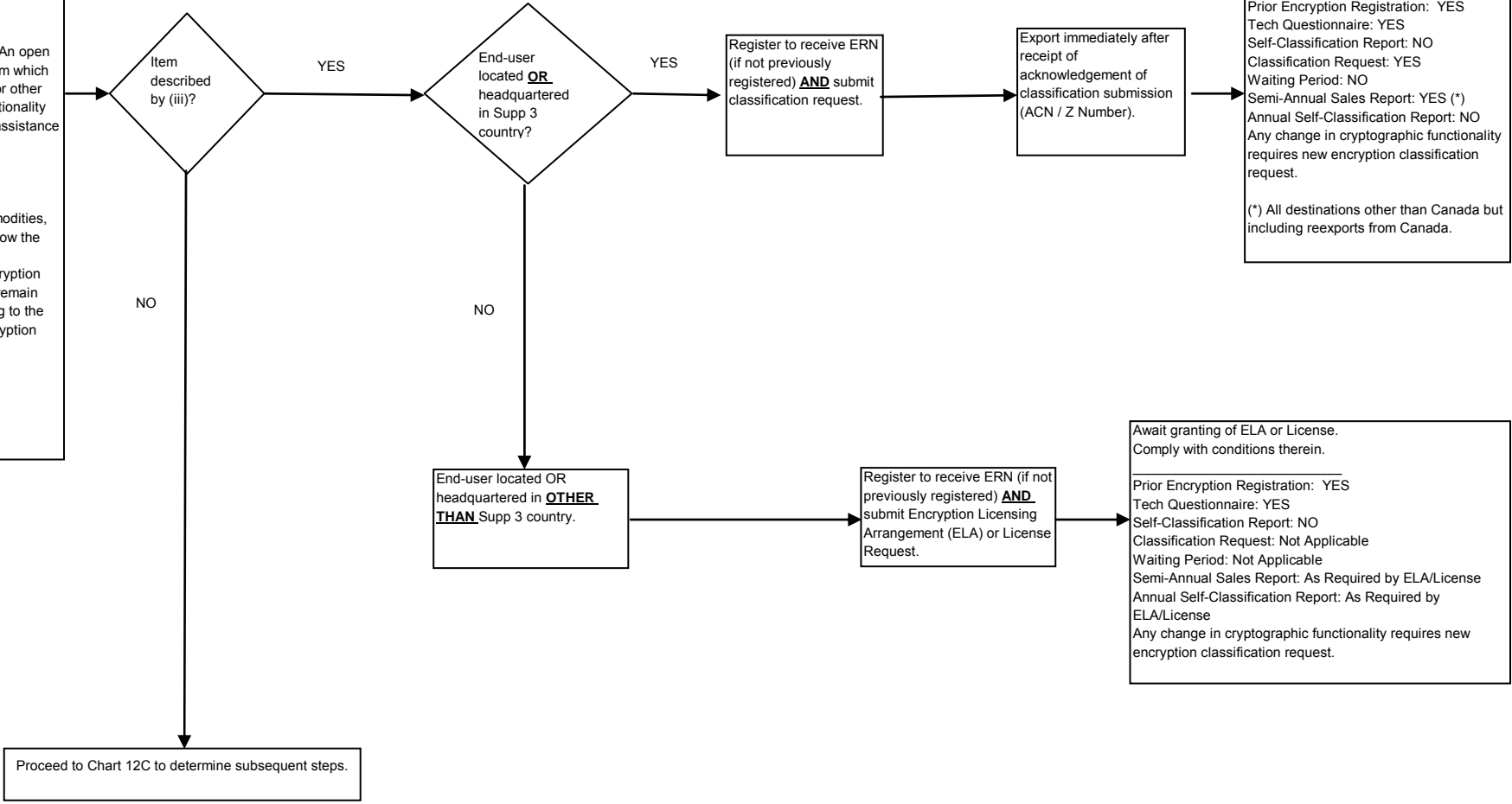
Open cryptographic interface items.

(iii) Items that provide an open cryptographic interface, to any end user located or headquartered in countries listed in Supplement 3.

Note partial definition of term: An open cryptographic face is a mechanism which is designed to allow a customer or other party to insert cryptographic functionality without the intervention, help or assistance of the manufacturer or its agents.

Note of Paragraph (b)(2): Commodities, software and components that allow the end-user to activate or enable cryptographic functionality in encryption products which would otherwise remain disabled, are controlled according to the functionality of the activated encryption product.

740.17 (b) (2)(iii)



Complete required steps to export using Exception ENC.
No E:1 Countries

Prior Encryption Registration: YES
Tech Questionnaire: YES
Self-Classification Report: NO
Classification Request: YES
Waiting Period: NO
Semi-Annual Sales Report: YES (*)
Annual Self-Classification Report: NO
Any change in cryptographic functionality requires new encryption classification request.

(*) All destinations other than Canada but including reexports from Canada.

Await granting of ELA or License.
Comply with conditions therein.

Prior Encryption Registration: YES
Tech Questionnaire: YES
Self-Classification Report: NO
Classification Request: Not Applicable
Waiting Period: Not Applicable
Semi-Annual Sales Report: As Required by ELA/License
Annual Self-Classification Report: As Required by ELA/License
Any change in cryptographic functionality requires new encryption classification request.

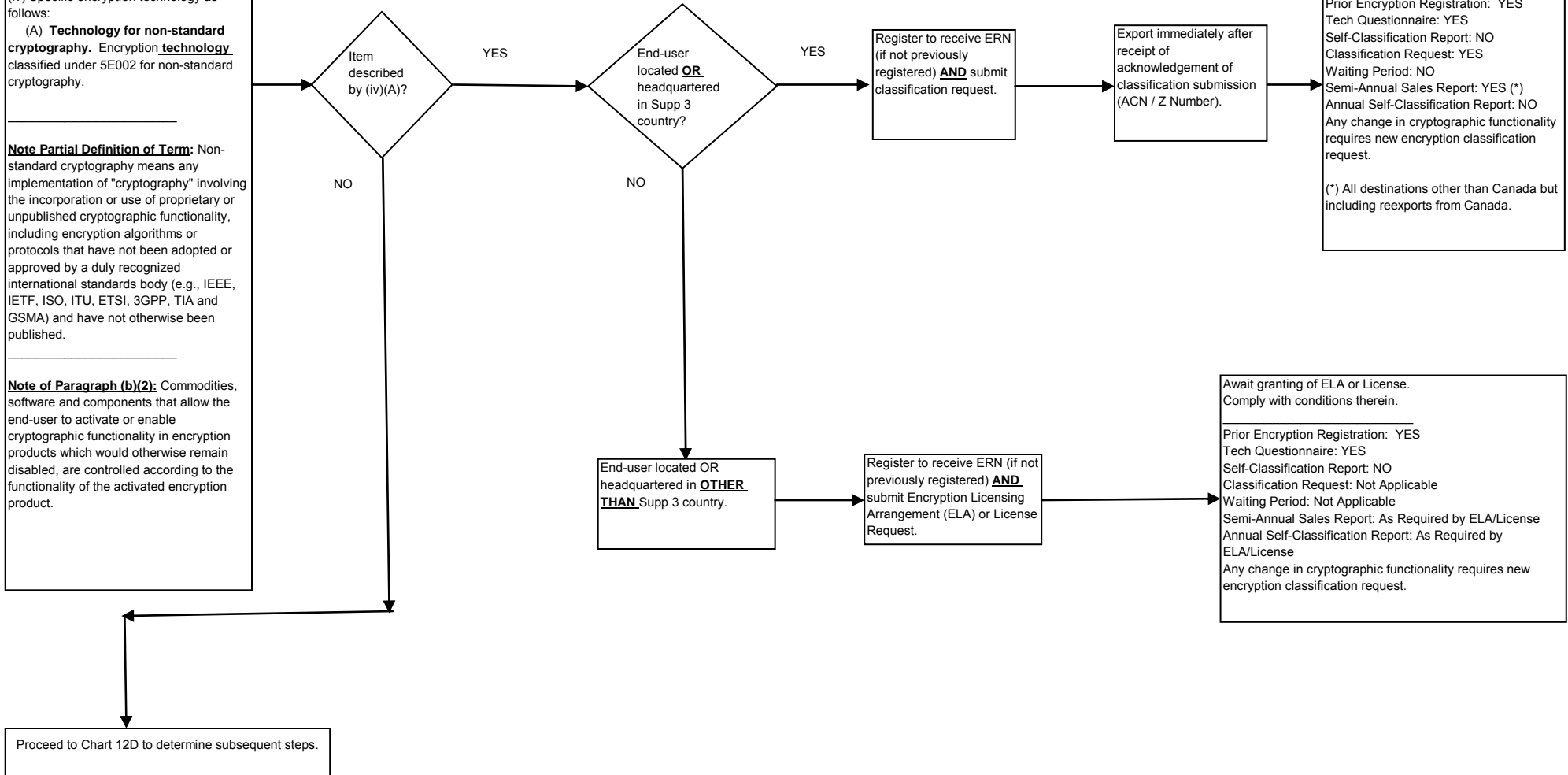
CHART 12C

Specific encryption technology.
 (iv) Specific encryption technology as follows:
 (A) **Technology for non-standard cryptography.** Encryption technology classified under 5E002 for non-standard cryptography.

Note Partial Definition of Term: Non-standard cryptography means any implementation of "cryptography" involving the incorporation or use of proprietary or unpublished cryptographic functionality, including encryption algorithms or protocols that have not been adopted or approved by a duly recognized international standards body (e.g., IEEE, IETF, ISO, ITU, ETSI, 3GPP, TIA and GSMA) and have not otherwise been published.

Note of Paragraph (b)(2): Commodities, software and components that allow the end-user to activate or enable cryptographic functionality in encryption products which would otherwise remain disabled, are controlled according to the functionality of the activated encryption product.

740.17 (b) (2)(iv)(A)



Complete required steps to export using Exception ENC.
 No E:1 Countries

Prior Encryption Registration: YES
 Tech Questionnaire: YES
 Self-Classification Report: NO
 Classification Request: YES
 Waiting Period: NO
 Semi-Annual Sales Report: YES (*)
 Annual Self-Classification Report: NO
 Any change in cryptographic functionality requires new encryption classification request.

(*) All destinations other than Canada but including reexports from Canada.

Await granting of ELA or License.
 Comply with conditions therein.

Prior Encryption Registration: YES
 Tech Questionnaire: YES
 Self-Classification Report: NO
 Classification Request: Not Applicable
 Waiting Period: Not Applicable
 Semi-Annual Sales Report: As Required by ELA/License
 Annual Self-Classification Report: As Required by ELA/License
 Any change in cryptographic functionality requires new encryption classification request.

Proceed to Chart 12D to determine subsequent steps.

CHART 12D

Specific encryption technology.
 (iv) Specific encryption technology as follows:
 (B) **Other technology.** Encryption technology classified under 5E002 **except (excluding) technology for cryptanalytic items and except (excluding) any "open cryptographic interface.**

Note Partial Definition of Term: Non-standard cryptography means any implementation of "cryptography" involving the incorporation or use of proprietary or unpublished cryptographic functionality, including encryption algorithms or protocols that have not been adopted or approved by a duly recognized international standards body (e.g., IEEE, IETF, ISO, ITU, ETSI, 3GPP, TIA and GSMA) and have not otherwise been published.

Note of Paragraph (b)(2): Commodities, software and components that allow the end-user to activate or enable cryptographic functionality in encryption products which would otherwise remain disabled, are controlled according to the functionality of the activated encryption product.

740.17 (b) (2)(iv)(B)

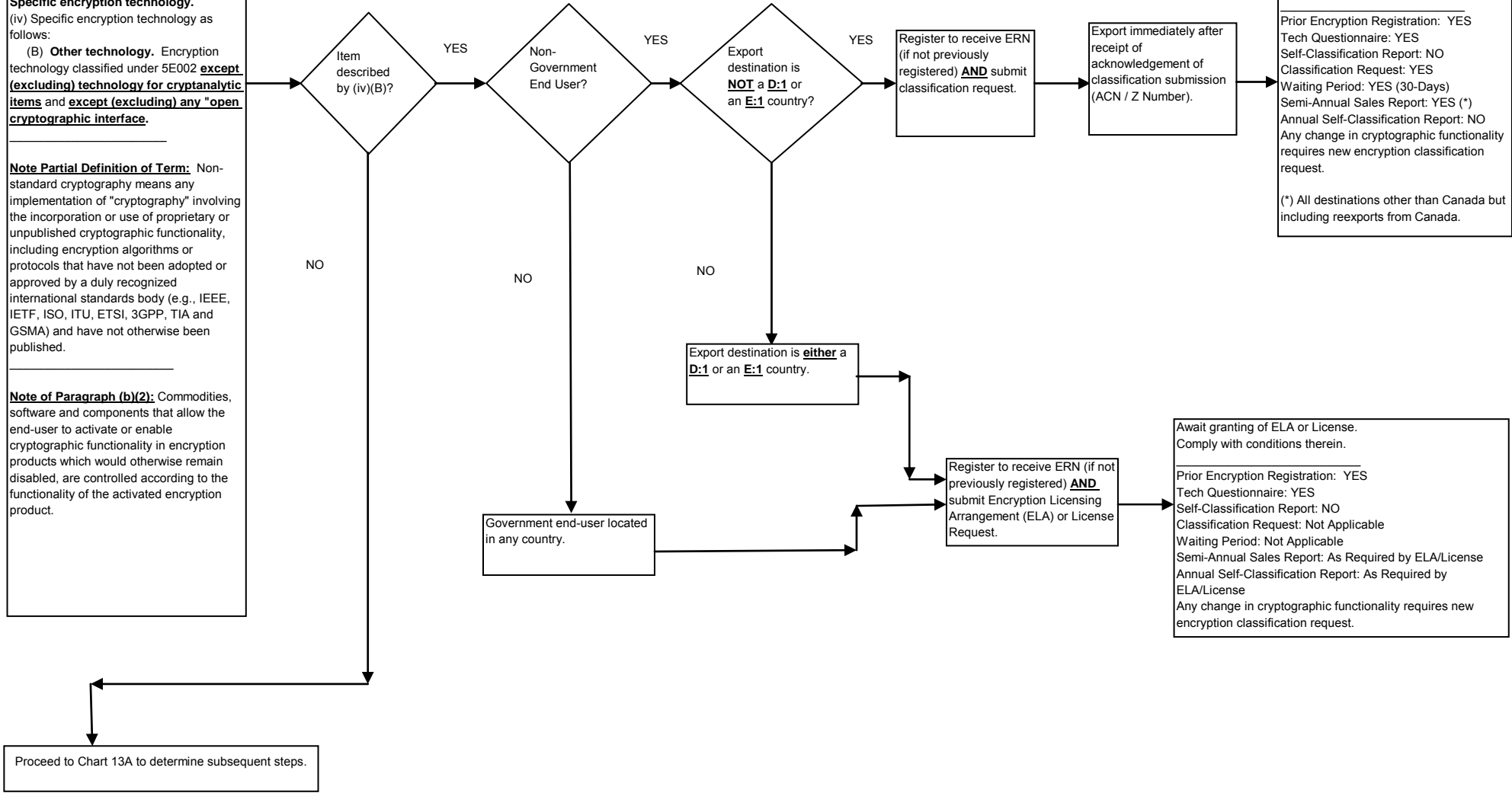


CHART 13A

PARTIAL LIST OF ITEMS CONTROLLED UNDER 5A002

This is **ONLY** a partial listing provided for immediate reference in training. Do **NOT** take export action based upon this information. Refer instead to the current version of Category 5, Part 2 of the EAR.

- a. Systems, equipment, application specific "electronic assemblies," modules and integrated circuits for "information security," as follows, and components therefor specially designed for "information security":
- a.1. **(E/NS/AT)** Designed or modified to use "cryptography" employing digital techniques performing any **cryptographic function other than authentication or digital signature and** having any of the following:
 - a.1.a. A "**symmetric** algorithm" employing a key length in **excess of 56-bits**; or
 - a.1.b. An "**asymmetric** algorithm" where the security of the algorithm is based on any of the following:
 - a.1.b.1. Factorization of integers in **excess of 512 bits** (e.g., RSA);
 - a.1.b.2. Computation of discrete logarithms in a multiplicative group of a finite field of size **greater than 512 bits** (e.g., Diffie-Hellman over Z/pZ); or
 - a.1.b.3. Discrete logarithms in a group other than mentioned in 5A002.a.1.b.2 in **excess of 112 bits** (e.g., Diffie-Hellman over an **elliptic curve**);
 - a.2. **(E/NS/AT)** Designed or modified to perform **cryptanalytic functions**;
 - a.4. **(NS/AT)** Specially designed or modified to reduce the compromising emanations of information bearing signals beyond what is necessary for health, safety or electromagnetic interference standards;
 - a.5. **(E/NS/AT)** Designed or modified to use cryptographic techniques to **generate the spreading code for "spread spectrum" systems**, not controlled in 5A002.a.6., including the **hopping code** for "frequency hopping" systems;
 - a.6. **(E/NS/AT)** Designed or modified to use cryptographic techniques to **generate channelizing codes, scrambling codes or network identification codes**, for systems using **ultra-wideband modulation** techniques **and** having any of the following:
 - a.6.a. A **bandwidth** exceeding **500 MHz**; or
 - a.6.b. A "**fractional bandwidth**" of **20%** or more;
 - a.7. **(NS/AT)** Non-cryptographic information and communications technology (ICT) security systems and devices evaluated to an assurance level exceeding class EAL-6;
 - a.8. **(NS/AT)** Communications cable systems designed or modified using mechanical, electrical or electronic means to detect surreptitious intrusion;
 - a.9. **(E/NS/AT)** Designed or modified to use '**quantum cryptography**.'

PARTIAL LIST OF ITEMS CONTROLLED UNDER 5B002

- a. **(NS/AT)** Equipment specially designed for the "development" or "production" of equipment controlled by 5A002 or 5B002.b;
- b. **(NS/AT)** Measuring equipment specially designed to evaluate and validate the "information security" functions of equipment controlled by 5A002 or "software" controlled by 5D002.a or 5D002.c.

PARTIAL LIST OF ITEMS CONTROLLED UNDER 5D002

- a. **(EI CONTROLS APPLY TO THIS ITEM IF FOR EQUIPMENT CONTROLLED FOR EI)** "Software" specially designed or modified for the "development", "production" or "use" of equipment controlled by 5A002 or "software" controlled by 5D002.c;
- b. **(NS/AT)** "Software" specially designed or modified to support "technology" controlled by 5E002;
- c. Specific "software" as follows:
 - c.1. **(EI CONTROLS APPLY TO THIS ITEM IF FOR EQUIPMENT CONTROLLED FOR EI)** "Software" having the characteristics, or performing or simulating the functions of the equipment, controlled by 5A002;
 - c.2. **(NS/AT)** "Software" to certify "software" controlled by 5D002.c.1.

PARTIAL LIST OF ITEMS CONTROLLED UNDER 5E002

(EI CONTROLS APPLY TO THIS ITEM IF FOR COMMODITIES/SOFTWARE CONTROLLED FOR EI) "Technology" according to the General Technology Note for the "development," "production" or "use" of equipment controlled by 5A002 or 5B002 or "software" controlled by 5D002.a or 5D002.c.

Proceed to Chart 13B to determine subsequent steps.

CHART 13B

MASS MARKET CRITERIA

Cat 5-2, Note 3: Cryptography Note:

ECCN's 5A002 and 5D002 do **NOT** control items that meet all of the following:

- a. Generally **available to the public** by being **sold without restriction** from stock at **retail selling points** (over-the-counter, mail order, electronic transactions, telephone transactions); AND
- b. **Cryptographic functionality** is **NOT** easily be **changed** by the user; AND
- c. Designed for **installation by the user** without further substantial support by the supplier; AND
- d. When necessary, **details are available** and will be provided upon request to the appropriate authority in the exporter's country to confirm compliance with the above.

742.15(b)(6)

EXAMPLES OF ITEMS WHICH **MAY BE ELIGIBLE** FOR MASS MARKET TREATMENT

Examples of Mass Market encryption items include **but are not limited to:**

General purpose operating systems;

Desktop applications designed for use with computers which are classified under ECCN 4A994 or designated EAR99 (such as e-mail, browsers, games, word processing, database, financial applications or utilities);

Laptops, hand-held devices;

Commodities and software for client internet appliances

Client wireless LAN devices;

Home use networking commodities and software (such as personal firewalls, cable modems for personal computers and consumer set top boxes);

Portable or mobile civil telecommunications commodities and software (such as Personal Data Assistants (PDA's), radios or cellular products);

Proceed to Chart 13C to determine subsequent steps.

CHART 13C

(i) Specified components under 5A002.a.1, a.5, a.6 and equivalent or related software under 5D002 NOT described under (b)(2) as follows:

(A) Chips, chipsets, electronic assemblies and field programmable logic devices;

(B) Cryptographic libraries, modules, development kits and toolkits including for operating systems and Cryptographic Service Providers (CSP);

(C) Application-specific hardware or software development kits implementing cryptography.

Item does **NOT** perform the functions or meet specifications of 740.17 (b)(2) items described in **Chart Series 11 or in Chart Series 12 above.**

740.17 (b) (3)(i) and
742.15 (b) (3)(i) and
Cat 5-2 Note 3: (Cryptography Note)

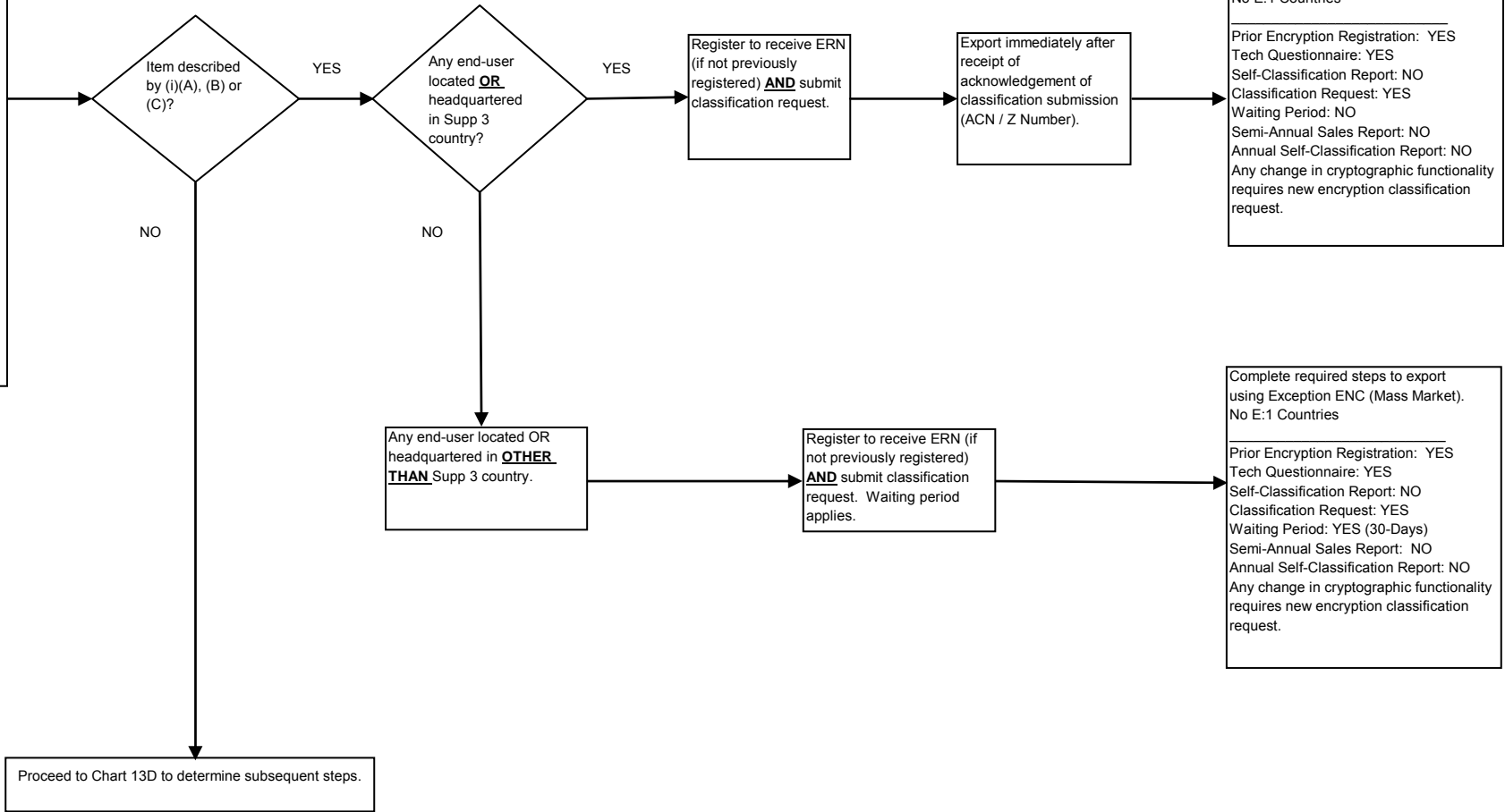


CHART 13D

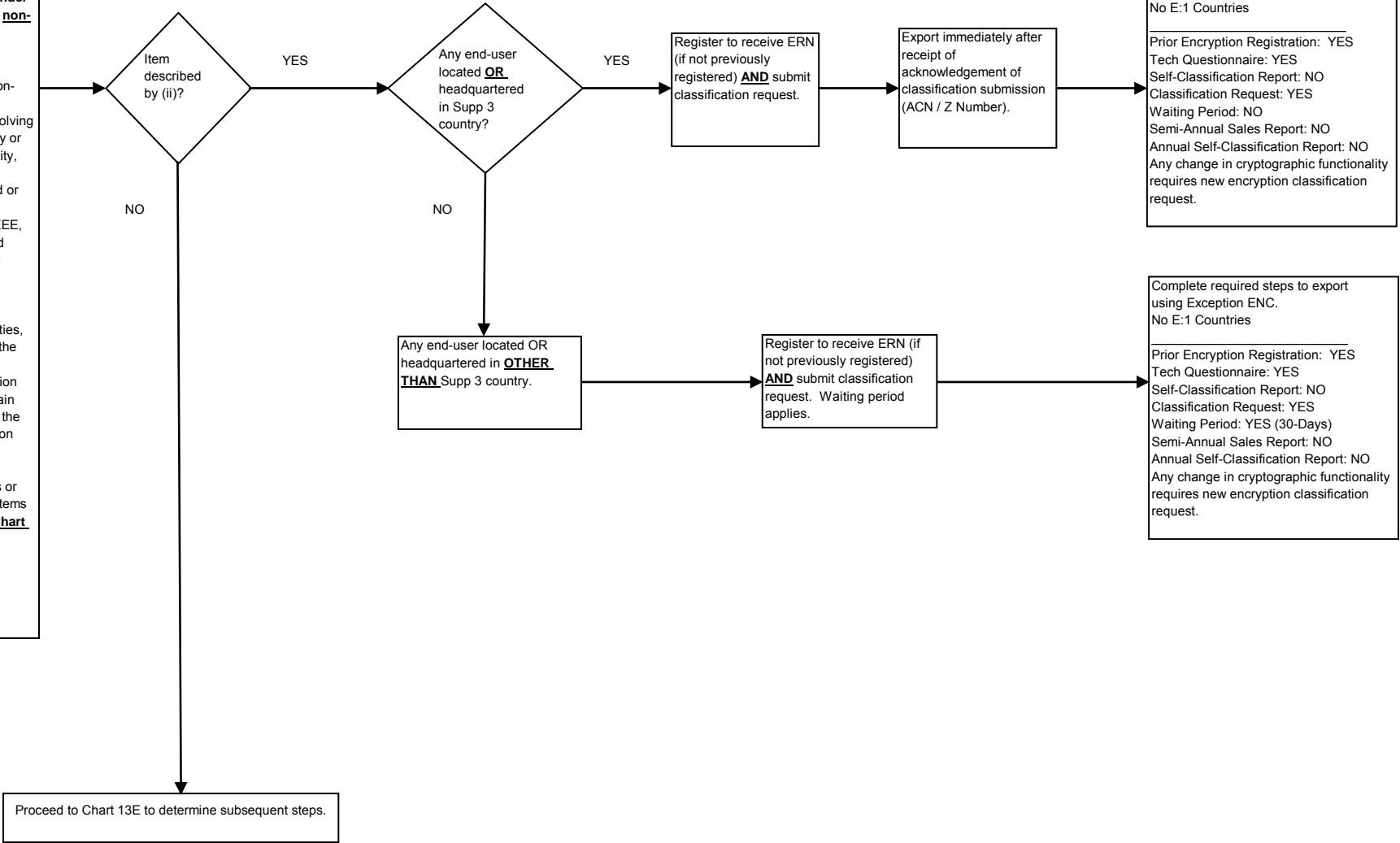
740.17 (b) (3)(ii) and
742.15 (b) (3)(ii) and
Cat 5-2 Note 3: (Cryptography Note)

(ii) Encryption commodities, software and components NOT described under (b)(2) AND that provide or perform non-standard cryptography.

Note Partial Definition of Term: Non-standard cryptography means any implementation of "cryptography" involving the incorporation or use of proprietary or unpublished cryptographic functionality, including encryption algorithms or protocols that have not been adopted or approved by a duly recognized international standards body (e.g., IEEE, IETF, ISO, ITU, ETSI, 3GPP, TIA and GSMA) and have not otherwise been published.

Note of Paragraph (b)(2): Commodities, software and components that allow the end-user to activate or enable cryptographic functionality in encryption products which would otherwise remain disabled, are controlled according to the functionality of the activated encryption product.

Item does **NOT** perform the functions or meet specifications of 740.17 (b)(2) items described in **Chart Series 11 or in Chart Series 12 above.**



Proceed to Chart 13E to determine subsequent steps.

Complete required steps to export using Exception ENC (Mass Market). No E:1 Countries

Prior Encryption Registration: YES
Tech Questionnaire: YES
Self-Classification Report: NO
Classification Request: YES
Waiting Period: NO
Semi-Annual Sales Report: NO
Annual Self-Classification Report: NO
Any change in cryptographic functionality requires new encryption classification request.

Complete required steps to export using Exception ENC. No E:1 Countries

Prior Encryption Registration: YES
Tech Questionnaire: YES
Self-Classification Report: NO
Classification Request: YES
Waiting Period: YES (30-Days)
Semi-Annual Sales Report: NO
Annual Self-Classification Report: NO
Any change in cryptographic functionality requires new encryption classification request.

CHART 13E

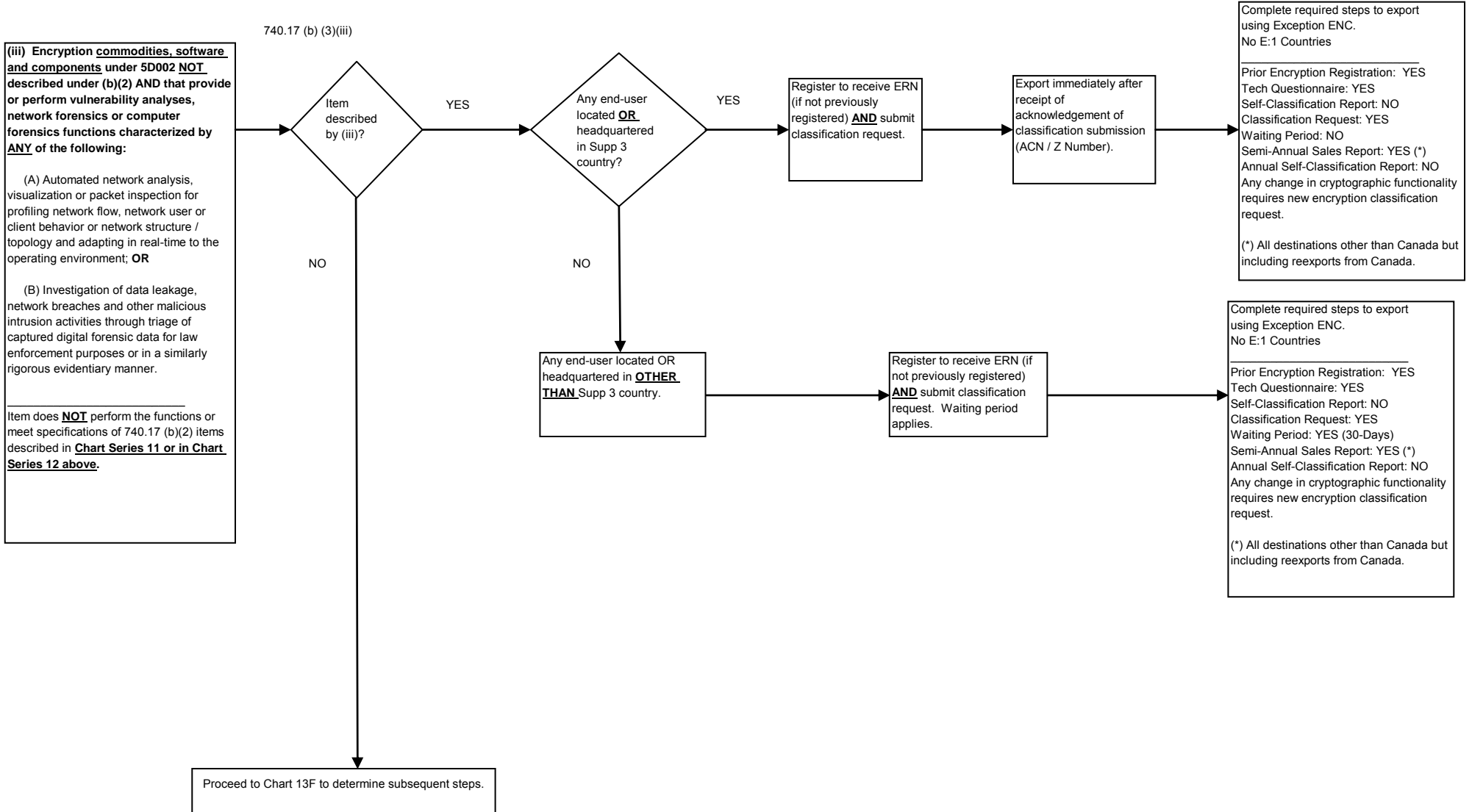


CHART 13F

740.17 (b) (3)(iv) and
742.15 (b) (3)(iv) and
Cat 5-2 Note 3: (Cryptography Note)

(iv) Cryptographic enabling commodities and software.
Commodities and software and components that activate or enable cryptographic functionality in encryption products which would otherwise remain disabled **AND** where the product or cryptographic functionality is not otherwise described in (b)(2) **OR** (b)(3)(i).

Note Partial Definition of Term: Non-standard cryptography means any implementation of "cryptography" involving the incorporation or use of proprietary or unpublished cryptographic functionality, including encryption algorithms or protocols that have not been adopted or approved by a duly recognized international standards body (e.g., IEEE, IETF, ISO, ITU, ETSI, 3GPP, TIA and GSMA) and have not otherwise been published.

Item does **NOT** perform the functions or meet specifications of 740.17 (b)(2) **OR** (b)(3)(i) items described in **Chart Series 11, Chart Series 12** or in **Chart 13C** above.

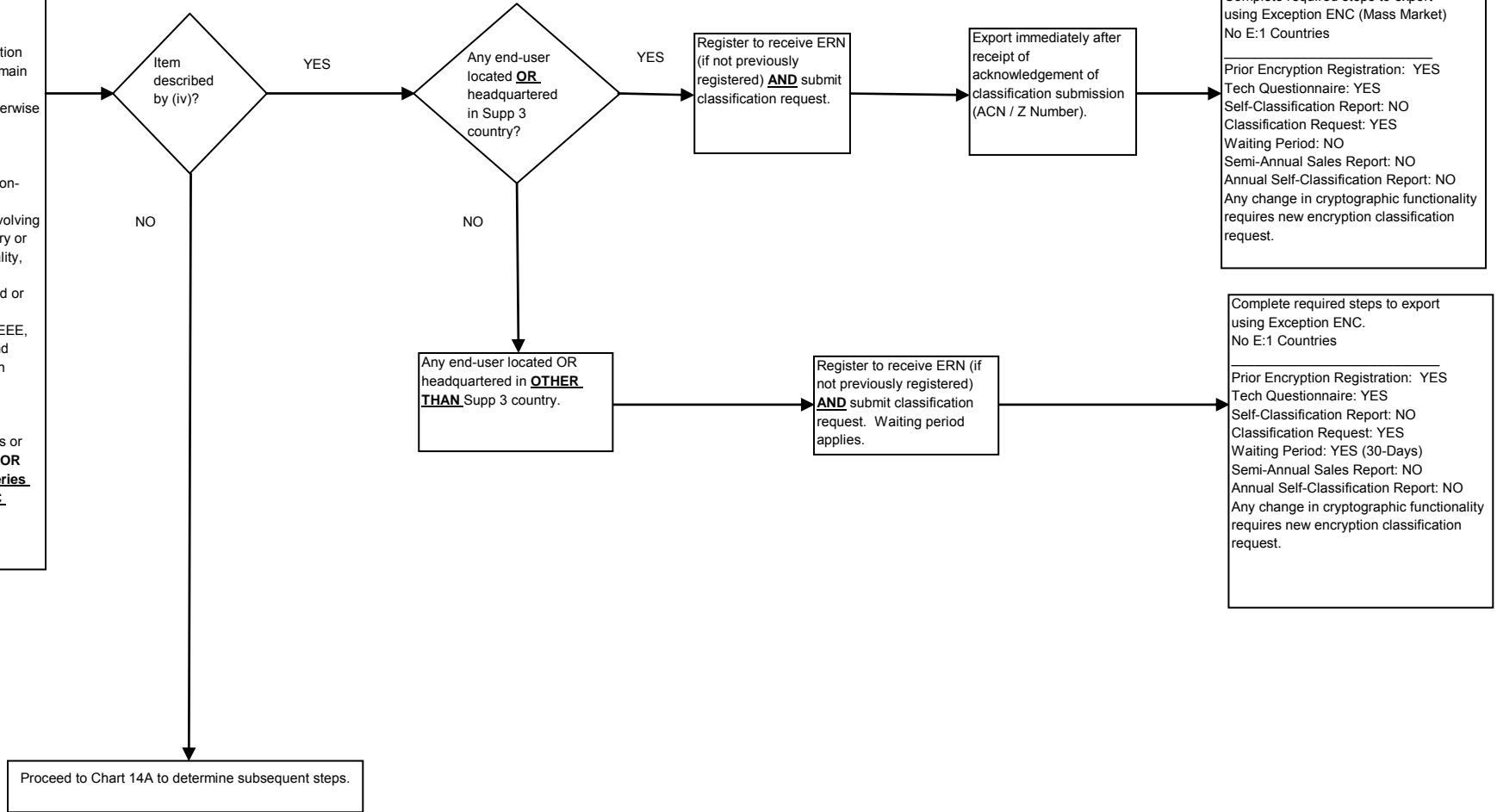


CHART 14A

PARTIAL LIST OF ITEMS CONTROLLED UNDER 5A002

This is **ONLY** a partial listing provided for immediate reference in training. Do **NOT** take export action based upon this information. Refer instead to the current version of Category 5, Part 2 of the EAR.

- a. Systems, equipment, application specific "electronic assemblies," modules and integrated circuits for "information security," as follows, and components therefor specially designed for "information security":
- a.1. **(E/NS/AT)** Designed or modified to use "cryptography" employing digital techniques performing any **cryptographic function other than authentication or digital signature and** having any of the following:
- a.1.a. A "**symmetric** algorithm" employing a key length in **excess of 56-bits**; or
- a.1.b. An "**asymmetric** algorithm" where the security of the algorithm is based on any of the following:
- a.1.b.1. Factorization of integers in **excess of 512 bits** (e.g., RSA);
- a.1.b.2. Computation of discrete logarithms in a multiplicative group of a finite field of size **greater than 512 bits** (e.g., Diffie-Hellman over Z/pZ); or
- a.1.b.3. Discrete logarithms in a group other than mentioned in 5A002.a.1.b.2 in **excess of 112 bits** (e.g., Diffie-Hellman over an **elliptic curve**);
- a.2. **(E/NS/AT)** Designed or modified to perform **cryptanalytic functions**;
- a.4. **(NS/AT)** Specially designed or modified to reduce the compromising emanations of information bearing signals beyond what is necessary for health, safety or electromagnetic interference standards;
- a.5. **(E/NS/AT)** Designed or modified to use cryptographic techniques to **generate the spreading code for "spread spectrum" systems**, not controlled in 5A002.a.6., including the **hopping code** for "frequency hopping" systems;
- a.6. **(E/NS/AT)** Designed or modified to use cryptographic techniques to **generate channelizing codes, scrambling codes or network identification codes**, for systems using **ultra-wideband modulation** techniques **and** having any of the following:
- a.6.a. A **bandwidth** exceeding **500 MHz**; or
- a.6.b. A "**fractional bandwidth**" of **20%** or more;
- a.7. **(NS/AT)** Non-cryptographic information and communications technology (ICT) security systems and devices evaluated to an assurance level exceeding class EAL-6;
- a.8. **(NS/AT)** Communications cable systems designed or modified using mechanical, electrical or electronic means to detect surreptitious intrusion;
- a.9. **(E/NS/AT)** Designed or modified to use '**quantum cryptography**.'

PARTIAL LIST OF ITEMS CONTROLLED UNDER 5B002

- a. **(NS/AT)** Equipment specially designed for the "development" or "production" of equipment controlled by 5A002 or 5B002.b;
- b. **(NS/AT)** Measuring equipment specially designed to evaluate and validate the "information security" functions of equipment controlled by 5A002 or "software" controlled by 5D002.a or 5D002.c.

PARTIAL LIST OF ITEMS CONTROLLED UNDER 5D002

- a. **(EI CONTROLS APPLY TO THIS ITEM IF FOR EQUIPMENT CONTROLLED FOR EI)** "Software" specially designed or modified for the "development", "production" or "use" of equipment controlled by 5A002 or "software" controlled by 5D002.c;
- b. **(NS/AT)** "Software" specially designed or modified to support "technology" controlled by 5E002;
- c. Specific "software" as follows:
- c.1. **(EI CONTROLS APPLY TO THIS ITEM IF FOR EQUIPMENT CONTROLLED FOR EI)** "Software" having the characteristics, or performing or simulating the functions of the equipment, controlled by 5A002;
- c.2. **(NS/AT)** "Software" to certify "software" controlled by 5D002.c.1.

PARTIAL LIST OF ITEMS CONTROLLED UNDER 5E002

(EI CONTROLS APPLY TO THIS ITEM IF FOR COMMODITIES/SOFTWARE CONTROLLED FOR EI) "Technology" according to the General Technology Note for the "development," "production" or "use" of equipment controlled by 5A002 or 5B002 or "software" controlled by 5D002.a or 5D002.c.

Proceed to Chart 14B to determine subsequent steps.

CHART 14B

MASS MARKET CRITERIA

Cat 5-2, Note 3: Cryptography Note:

ECCN's 5A002 and 5D002 do **NOT** control items that meet all of the following:

- a. Generally **available to the public** by being **sold without restriction** from stock at **retail selling points** (over-the-counter, mail order, electronic transactions, telephone transactions); AND
- b. **Cryptographic functionality** is **NOT** easily be **changed** by the user; AND
- c. Designed for **installation by the user** without further substantial support by the supplier; AND
- d. When necessary, **details are available** and will be provided upon request to the appropriate authority in the exporter's country to confirm compliance with the above.

742.15(b)(6)

EXAMPLES OF ITEMS WHICH MAY BE ELIGIBLE FOR MASS MARKET TREATMENT

Examples of Mass Market encryption items include **but are not limited to**:

General purpose operating systems;

Desktop applications designed for use with computers which are classified under ECCN 4A994 or designated EAR99 (such as e-mail, browsers, games, word processing, database, financial applications or utilities);

Laptops, hand-held devices;

Commodities and software for client internet appliances

Client wireless LAN devices;

Home use networking commodities and software (such as personal firewalls, cable modems for personal computers and consumer set top boxes);

Portable or mobile civil telecommunications commodities and software (such as Personal Data Assistants (PDA's), radios or cellular products);

Proceed to Chart 14C to determine subsequent steps.

CHART 14C

742.15 (b) (1) Mass Market

Associated **commodities** under **5A002.a.1, a.2, a.5, a.6, a.9, 5B002** and equivalent or related **software** under **5D002**.
MEETING MASS MARKET (MMKT) CRITERIA
 Item does **NOT** perform the functions or meet specifications of 740.17 (b)(2) OR (b)(3) items described in **Chart Series 11, Chart Series 12 or Chart Series 13** above.

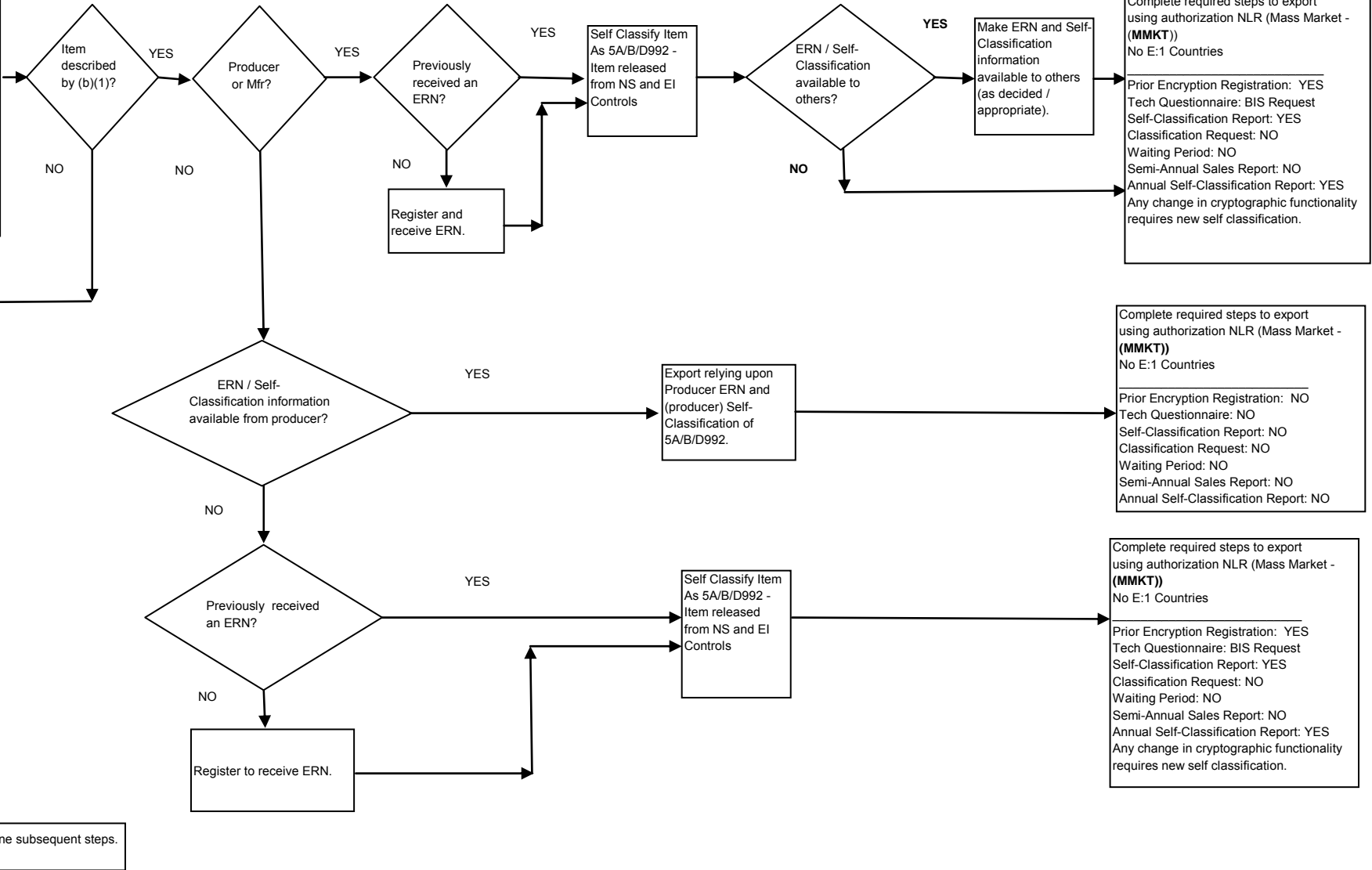


CHART 14D

740.17 (b) (1) ENC

Associated **commodities** under **5A002.a.1, a.2, a.5, a.6, a.9, 5B002** and equivalent or related **software** under **5D002**.
NOT MEETING MASS MARKET CRITERIA

Item does **NOT** perform the functions or meet specifications of 740.17 (b)(2) OR (b)(3) items described in **Chart Series 11, Chart Series 12 or Chart Series 13** above.

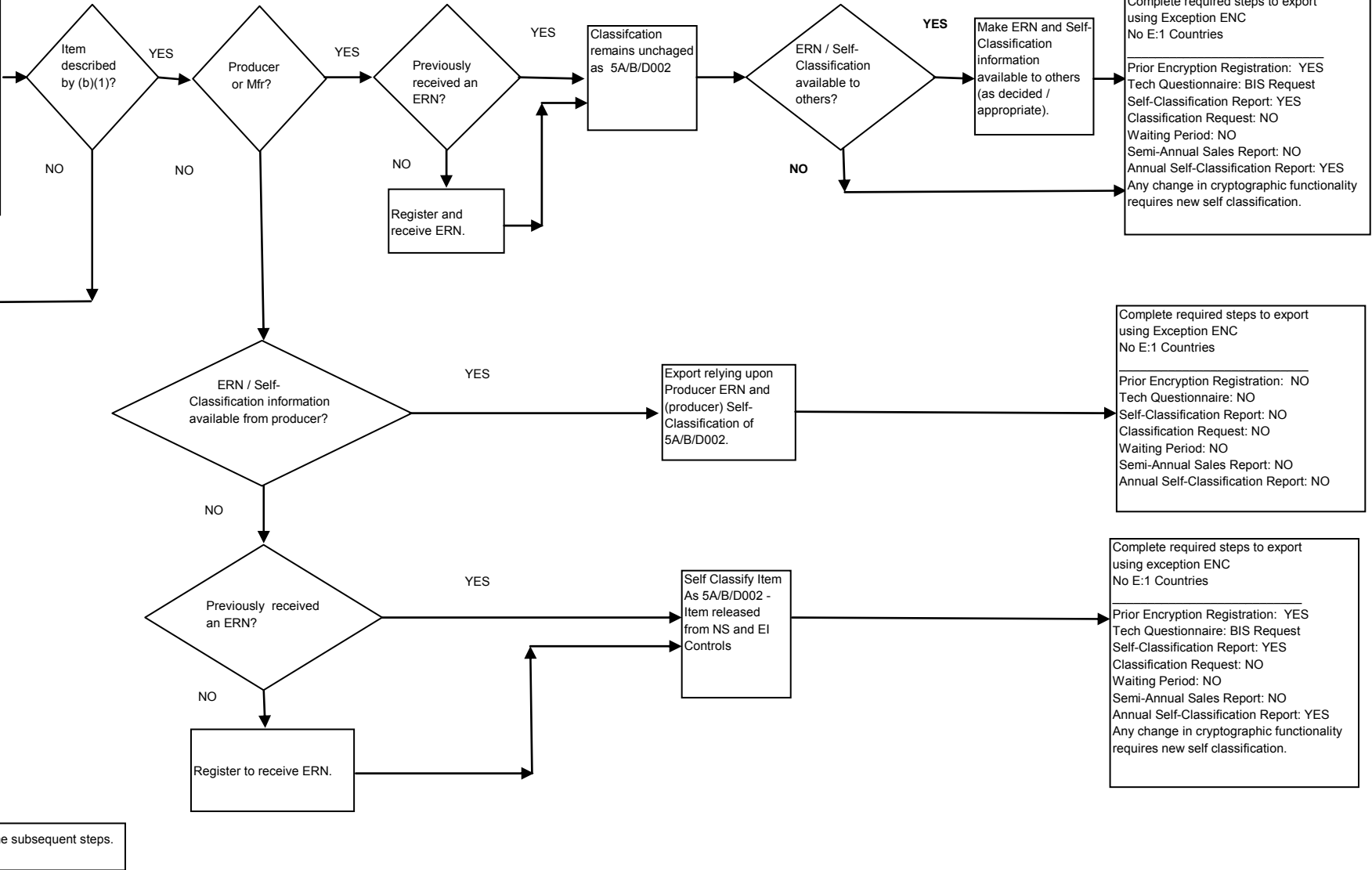


CHART 15A

Item or situation has not been specifically addressed in Chart Series 1 through 14 or item is a newly developed encryption concept / idea / function / item or employs encryption or encryption functionalities, commodities, software or technology in manners not anticipated or otherwise addressed in Chart Series 1 through 14.

Contact:
Information Technology Controls Division for direction. Likely course of action or instructions will be Registration to receive ERN (if not previously registered) **AND** submission of an Encryption Classification Request and/or Encryption Licensing Arrangement (ELA) or License Request.

Information Technology Controls Division

Randy Pratt Director 202-482-5303 cpratt@bis.doc.gov	Joe Young Senior Engineer 202-482-4197 jyoung@bis.doc.gov
Judith Currie Senior Export Policy Analyst 202-482-5085 jcurrie@bis.doc.gov	Michael Pender Senior Engineer 202-482-2458 mpender@bis.doc.gov
Sylvia Jimmison Export Policy Analyst 202-482-2342 sjimmiso@bis.doc.gov	Aaron Amundson Export Policy Analyst 202-482-5299 aamundso@bis.doc.gov
Anita Zinzuvadia Electrical Engineer 202-482-3772 azinzuva@bis.doc.gov	

Contact :
BIS Western Regional Office for general guidance and assistance with the EAR and for questions other than those relating to encryption.

BIS Western Regional Office
Irvine, CA
T: 949-660-0144
F: 949-660-9347

Michael Hoffman Director mhoffman@bis.doc.gov	John Bushnell Industry Analyst jbushnel@bis.doc.gov
Richard Sylvestri Export Administration Specialist rsylvest@bis.doc.gov	Joseph Tosto, Jr. Export Administration Specialist jtosto@bis.doc.gov

Northern California Branch
San Jose, CA

Larry Sullivan
T: 408-998-8806
F: 408-998-8677