

ENCRYPTION EXPORT CONTROL POLICY 2000

by **Roszel C. Thomsen II**
and **Antoinette D. Paytas**

On Friday, January 14, 2000, the Commerce Department's Bureau of Export Administration (BXA) published an interim rule with request for comments that amends the export controls on encryption products in two important respects.¹ First, it implements the encryption export control reforms announced by the White House on September 16, 1999. Second, it implements changes to the encryption items that are subject to export controls under the Wassenaar Arrangement. By overlaying the new encryption export control policy on top of the Wassenaar control list, the new regulations are more liberal in their treatment of encryption exports, but remain fiendishly (and, arguably, unnecessarily) complex.

Overall, the White House has delivered on its promise to reform the onerous encryption export controls. The interim rule reflects numerous inputs received from industry over the past several months, and, as a result, it has been greatly improved from the discussion drafts that were circulated in November and December of 1999. In some respects, like the favorable treatment accorded to source code, the interim rule is even more liberal than the White House had promised. In other respects, like the remaining restrictions on network infrastructure products, it remains disappointing. These and other aspects of the interim rule are discussed in detail next.

Although the number of transactions requiring export licenses is reduced under the new policy, the administrative burden on companies to comply with the encryption export controls remains high. With few exceptions, every new product still must be reviewed by BXA and the National Security Agency (NSA) prior to export. In order to take advantage of the new liberalizations, many products

Roszel C. Thomsen II <roz@t-b.com> is a partner, and Antoinette D. Paytas <tpaytas@t-b.com> is an associate, in the law firm of Thomsen, Burke and Franke LLP <<http://www.t-b.com>>. Roz and Toni concentrate in the field of export controls, with particular emphasis on the laws and regulations governing cryptography.



must be reclassified, and companies will have to issue new instructions to their sales and marketing departments and channel partners. Many companies, particularly those in the networking industry, also will have to implement new customer screening and transaction reporting procedures.

The "bottom line," unfortunately, is that the new regulations are neither simple nor transparent. The provisions governing the classification of 56- and 64-bit products are far more complicated than they need to be. The new reporting requirements are an outright invitation to play "Let's Make a Deal" with BXA and the NSA.

"The good news is that consumers all over the world are going to have access to much stronger encryption. . . . The bad news is that if you want to send encryption out of the country, you have to hire a lawyer to do it. These regulations are very complicated."²

BACKGROUND

The interim rule has two primary objectives. It implements the three principles enunciated by the White House in its announcement of September 16, 1999, as the basis for its encryption export control policy, notably: (1) technical review of all encryption products prior to sale; (2) post-export reporting of sales; and (3) review of exports to foreign governments. It also implements changes agreed to by the Wassenaar members countries, by: (1) transforming Category 5, Part 2 of the Commerce Control List to a positive list; (2) creating a new Cryptography Note; (3) removing encryption software from the General Software Note; (4) removing controls on 64-bit mass market products; and (5) removing controls on 512-bit key management products. By blending these two objectives, the new regulations allow a greater scope of exports without case-by-case licensing, but at the same time introduce a higher level of complexity to the export control process.

STRONG ENCRYPTION PRODUCTS

Products and components implementing strong encryption are eligible for export under License Exception ENC to all customers (except government end users) in all destinations (except embargoed/terrorist countries) after a one-time technical review by BXA and the NSA. Strong encryption products and components that qualify as "retail" also may be exported to government end users. However, products incorporating open cryptographic interfaces are *not* eligible for export under License Exception ENC, with few exceptions.

TECHNICAL REVIEWS

Exporters must submit new products and components implementing (strong or weak) encryption to BXA and the NSA for a technical review, prior to export. This procedure is similar to what BXA and the NSA have used historically

to review encryption products for purposes of classification. The exporter prepares and submits a Commodity Classification Request that describes the product's functionality in general, and its cryptographic features in particular. A comprehensive description of the product's encryption algorithms and key lengths, key management mechanism, and key space is especially important. Thirty days after submission of a properly completed application, the exporter may commence exports, except to government end users.³

DEFINITION OF "RETAIL"

Products that qualify as "retail" also may be exported to government end users, so exporters will want to include in their Commodity Classification Requests information demonstrating that their products qualify as "retail."

Unfortunately, the definition of "retail" is narrower than the definition of "mass market" which has a decade of interpretation in export control practice. This narrow definition of "retail" is intentional. BXA specifically intends to exclude from the definition of "retail" certain networking products implementing strong encryption that previously qualified as "mass market." As a result, exports of these networking products to government end users, or to telecommunications and internet service providers to provide services to government end users, requires a license.

"POSITIVE" AND "NEGATIVE" TESTS

In order to qualify as "retail," a product must meet at least one of the following "positive" tests:⁴

1. Sold in tangible form through retail outlets independent of the manufacturer;
2. Specifically designed for individual consumer use and sold or transferred through tangible or intangible means; or
3. Sold in large volumes without restriction through mail order transactions, electronic transactions, or telephone call transactions.

In addition, the product at issue must *not* meet any of the following "negative" tests:⁵

1. Cryptographic functionality can be easily changed by the user;
2. Requires substantial support for installation and use;
3. Cryptographic functionality has been modified or customized to customer specifications; and
4. Network infrastructure products such as high-end routers or switches designed for high volume communications.

Thus, there are two important differences between the new definition of "retail" and the old definition of "mass market." The first difference is the inclusion of the words "large volume" in "positive" test number three. This change may make it more difficult for smaller companies to qualify their products as "retail" than as "mass market." The second

difference is the inclusion of the prohibition on network infrastructure products in "negative" test number four. Obviously, this will make it more difficult for router and switch vendors to qualify as "retail" and to compete with foreign suppliers of network infrastructure products.

EXAMPLES

As the debate over the definition of "retail" raged during the fall of 1999, the following examples were inserted into the definition at the behest of certain vocal constituencies:

1. General purpose operating systems and their associated user-interface client software and general purpose operating systems with embedded networking and server capabilities (Microsoft);
2. Non-programmable encryption chips and chips that are constrained by design for retail products (Intel);
3. Low-end routers, firewalls, and networking or cable equipment designed for small office or home use (Cisco);
4. Programmable database management systems and associated application servers (Oracle);
5. Low-end servers and application-specific servers (including client-server applications, *e.g.*, secure socket layer (SSL)-based applications) that interface directly with the user (Sun); and
6. Encryption products distributed without charge or through free or anonymous downloads (numerous companies).

However, this is an illustrative list, not an exclusive list. Additional products that meet one of the "positive" tests and none of the "negative" tests described previously, or that meet one of the other tests described hereafter, may qualify as "retail."⁶

"FUNCTIONAL EQUIVALENCY" TEST

The interim rule also provides that "encryption products and network-based applications which provide functionality equivalent to other encryption products classified as retail will be considered retail." This provision is designed to level the playing field in two respects. It allows a product that competes directly with a retail product, but is not sold through retail channels, to receive "retail" export treatment. It also allows companies to offer network services, such as calendaring, scheduling, and email, to any subscriber, including government end users, even though the "server" product itself may not qualify as "retail."⁷

"Financial-Specific" Test

A carry-over from the prior encryption export control policy, products that are restricted by design to secure financial communications are given "retail" status, regardless of whether they meet the "positive" and "negative" or "functional equivalency" tests. In order to meet the "finance-specific" test, a product must be highly field format-

ted with validation procedures and not easily diverted to other end uses. For example, products implementing the Secure Electronic Transactions protocol developed for credit card transactions may qualify as "financial specific."⁸

56-Bit "Retail" Products

The drafters of the interim rule had a problem. They wanted to conform the Commerce Control List to the Wassenaar Arrangement, but did not want to "roll back" the broad eligibility of export for 56-bit products with key exchange mechanisms up to and including 1,024 bits or equivalent that may not be classified as "mass market." To prevent such a rollback, the interim rule treats such products as "retail" whether or not they meet any of the tests described previously.⁹

DEFINITION OF "GOVERNMENT END USERS"

One of the primary objectives of the new encryption export control policy is to allow BXA and the NSA to review applications requesting authorization to export non-retail products to government end users, which presumably are high-priority targets of the NSA's surveillance efforts. To this end, the interim rule includes the following definition of "government end user":

Government End user (as applied to encryption items). A government end user is

- (a) any foreign central, regional, or local government department, agency, or other entity performing governmental functions; including governmental research institutions, governmental corporations or their separate business units (as defined in part 772 of the EAR) which are engaged in the manufacture or distribution of items or services controlled on the Wassenaar Munitions List, and international governmental organizations;
- (b) this term does not include the following public entities: utilities (including telecommunications companies and Internet service providers); banks and financial institutions; transportation; broadcast or entertainment; educational organizations; civil health and medical organizations; retail or wholesale firms; and manufacturing or industrial entities not engaged in the manufacture or distribution of items or services controlled on the Wassenaar Munitions List.¹⁰

Thankfully, this definition was narrowed considerably during the drafting process. For example, telecommunications and Internet service providers (ISPs) were added to the list of excluded entities in (b) in the second discussion draft. Nevertheless, screening of customers to determine whether they fall within the definition of "government end user" promises to be an export manager's nightmare.

SPECIAL RULES FOR TELCOS AND ISPS

The provisions governing telcos and ISPs provoked some of the most contentious discussions between govern-

ment and industry during the drafting process leading up to the interim rule. Like the definition of government, the scope of services that require a license before telecommunications and internet service providers can offer them using non-retail encryption items was narrowed considerably during the drafting process. At the very end, a restriction against providing encryption of the telecommunications backbone was removed, and replaced with a new, and more onerous, reporting requirement. As published, the interim rule requires telcos and ISPs to obtain a license if they want to use non-retail products to provide "services specific to government end users, e.g., WAN, LAN, VPN, voice and dedicated-link services; application specific and e-commerce services and PKI encryption services specifically for government end users only."¹¹

In short, national PKIs, and in fact any service that is offered on a non-discriminatory basis to subscribers at large, is permitted without a license. Only services that are specific to governments require a license. In addition, there are special reporting requirements for sales to telecommunications and ISPs, described next.

EXPORT LICENSING OPTIONS

For exports to governments, and to telcos and ISPs wishing to provide services to governments, there are two licensing options. The first option is to apply for licenses case by case. This approach is cumbersome, but it does allow each specific transaction to be evaluated on its own merits. The second option is to apply for Encryption Licensing Arrangements that allow exports to classes of end users for specified end uses in a territory. Although they are quite flexible, Encryption Licensing Arrangements generally are more restrictive than the case-by-case licensing policy.

BXA has indicated in the interim rule that certain types of civil end uses will receive "favorable consideration." In the past, such assurances often have been hollow. However, BXA officials have offered assurances of their sincerity that will be put to the test, quickly. The civil end uses that should receive favorable consideration are as follows:¹²

1. Social or financial services to the public;
2. Civil justice;
3. Social insurance;
4. Pensions and retirement;
5. Taxes; and
6. Communications between governments and their citizens.

SOURCE CODE AND GENERAL PURPOSE TOOL KITS

In the past, cryptographic source code and general purpose tool kits required a license for export to all destinations (except Canada). One of the pleasant surprises in the

interim rule is the relaxation of controls on these items. Sections hereafter referring to Open Source, Community Source, and Other Source Code and General Purpose Toolkits refer to such items incorporating strong cryptography (*i.e.*, controlled under 5D002). Source code for weak cryptography is addressed in a separate section, entitled "Weak Cryptography."

UNRESTRICTED (OPEN) SOURCE

Source code for strong cryptography that is generally available to the public, without payment of a licensing fee or royalty, is released from "Encryption Item" controls and is eligible for export without prior review under License Exception TSU. This type of source code sometimes is referred to as "open source" and may include open cryptographic interfaces that generally require a license. The only pre-qualification is that that exporter must submit advance notification to BXA of the Internet location where the source code is available, or a copy of the source code, prior to export. The exporter does not have to block downloads to embargoed countries, but it cannot knowingly export to such countries. The exporter does not have to report downloads, nor must it report the derivative use of the source code by parties outside the United States.¹³

COMMERCIAL (COMMUNITY) SOURCE

Source code that is generally available to the public, but requires payment of a licensing fee or royalty for commercial use, is eligible for export without prior review under License Exception ENC. This type of source code sometimes is referred to as "community source" and may include open cryptographic interfaces that generally require a license. The only pre-qualification is that the exporter must submit advance notification to BXA of the Internet location where the source code is available, or a copy of the source code, prior to export. The exporter does not have to block downloads to embargoed countries, but it may not knowingly export to such countries. However, the provider does have to report non-proprietary information describing foreign products offered for commercial sale (unless the foreign product is developed merely by bundling or compiling of the source code). The foreign products do not have to be reviewed and classified by BXA, yet they remain subject to the EAR.¹⁴

OTHER SOURCE CODE AND GENERAL PURPOSE TOOL KITS

Source code for strong cryptography that does not qualify as either Open Source or Community Source is eligible for export under License Exception ENC, to any non-government end user.¹⁵ Unlike Open Source and Community Source, such other source code and general purpose tool kits must be reviewed and classified by BXA prior to export, and they may not include open cryptographic in-

terfaces.¹⁶ The exporter must block downloads not only to embargoed countries, but also to <.gov>, <.mil> and other similar addresses. The exporter also has to report non-proprietary information describing foreign products offered for commercial sale (unless the foreign product is developed by merely bundling or compiling of the source code).¹⁷ The foreign products do not have to be reviewed and classified by BXA, but they remain subject to the EAR.

REPORTING REQUIREMENTS

The reporting requirements are among the most complex sections of the interim rule. First, we look at whether a product is exempt from the reporting requirements. Second, we examine the type of information that must be reported. Third, we consider the special rules applicable to telecommunications and internet service providers.

EXEMPTIONS FROM REPORTING REQUIREMENTS

Based on Type of Product

Some exemptions from the reporting requirements are based on the type of product being exported. For example, finance-specific products, and products not exceeding 64 bits, are not subject to reporting.¹⁸

Based on the Type of Recipient

Other exemptions are based on the type of recipient. For example, exports to subsidiaries of US companies, and to US banks, financial institutions, their subsidiaries, affiliates, customers or contractors, are not subject to reporting.¹⁹

Based on the Type of Product and Type of Recipient

Still other exemptions are based not only on the type of product, but also the type of recipient. For example, exports of retail products to individual consumers are not subject to reporting.²⁰

Based on Method of Distribution

The final exemption is based on the method of distribution. Any export that is made by free or anonymous download is exempt from reporting.²¹

INFORMATION REPORTED

The information that one must report depends on whether the sale is through "direct" or "indirect" channels.

Direct Sales

For finished products, the exporter must report the name and address of the recipient and the quantity exported. (Note that direct sales of retail products to individual consumers are exempt from the reporting requirements.)

For components, community source code and general purpose encryption tool kits, the exporter must submit the names and addresses of the manufacturers using such encryption components, commercial source code, or general

purpose encryption toolkits and a non-proprietary technical description of the products for which the component, source code, or toolkit are being used (e.g., brochures, other documentation, descriptions or other identifiers of the final foreign product; the algorithm and key lengths used; general programming interfaces to the product, if known; any standards or protocols that the foreign product adheres to; and source code, if available).²²

Indirect Sales

For items exported through indirect sales channels, the exporter must report the name and address of the distributor or reseller and the quantity exported. In addition, the exporter must report the end user's name and address, if such information is collected in the ordinary course of business.²³

SPECIAL RULES FOR EXPORTS TO TELCOS AND ISPS

There is a special rule governing exports and re-exports of network infrastructure products (e.g., high-end routers or switches designed for large volume communications) to telcos and ISPs. All such reports are due "by the time of export." Exporters may request other reporting arrangements with BXA to better reflect their business models. However, it remains to be seen how receptive BXA will be to requests for reporting that deviate from this model.²⁴

ELECTRONIC DOWNLOAD SCREENING

In the past, companies that wanted to make strong cryptography available for electronic download in the United States and Canada had to implement certain precautions to prevent unauthorized downloads without a license. The new regulations are substantially less restrictive, although they arguably are more complex.

OPEN AND COMMUNITY SOURCE

Open and Community Source code may be made available for electronic download without notifying the recipient that the software is subject to US export controls, requiring acknowledgment of such controls, or blocking Internet sites in the embargoed countries.²⁵

RETAIL PRODUCTS

Exporters should ensure that retail products are not exported to end users in embargoed countries, by blocking the Internet addresses for the embargoed countries. However, it does not appear that exporters have to do any additional screening, and downloads of retail products are exempt from the reporting requirements if they are free and/or anonymous.²⁶

NON-RETAIL PRODUCTS, COMPONENTS, SOURCE CODE, AND TOOLKITS

Exporters must implement a more elaborate procedure in order to authorize the electronic download of non-retail

products, components, source code (other than open and community source), and general purpose tool kits. Specifically, the exporter must: (1) notify the party requesting the download that the product is subject to US export controls; (2) obtain affirmative acknowledgment from the party requesting the download that the software is subject to US export controls; and (3) ensure that the system requesting the download does not have a domain name or internet address of a foreign government end user (e.g., <.gov>, <.gouv>, <.mil>, or similar addresses).²⁷

INTRA-COMPANY TRANSFERS

The interim rule also make several significant changes with respect to intra-company transfers, for US-based companies and foreign-based companies that have US subsidiaries.

EXPORTS BY US PARENTS TO FOREIGN SUBSIDIARIES

US companies may export strong encryption hardware, software, and technology to their foreign subsidiaries without review under the Commodity Classification Request procedure. The only limitations are that the products and technologies are limited to internal use and that foreign-origin products produced using the US-origin items remain subject to US export controls.²⁸

FOREIGN NATIONALS HIRED BY US COMPANIES

The so-called deemed export rule, which requires US companies to obtain a license prior to sharing cryptographic technology with employees who are neither American citizens nor "green card" holders, has been modified. Under the new regulations, exporters must apply for licenses only for nationals of Taliban-occupied Afghanistan, Cuba, Iran, Iraq, Libya, North Korea, Serbia, Sudan, and Syria.²⁹

EXPORTS BY US SUBSIDIARIES TO FOREIGN PARENTS

US subsidiaries of foreign companies that want to export US-origin encryption technology to their parent and sister companies will have to obtain Encryption Licensing Arrangements in order to do so.³⁰

OPEN CRYPTOGRAPHIC INTERFACES

Cryptographic interfaces remain subject to a license requirement if they are "open"—that is, if a user may substitute cryptographic libraries and the like in place of the features supplied by the developer without the developer's support. The important exceptions to this rule are exports of open and community source code, and exports to US subsidiaries.³¹

BUG FIXES AND UPDATES

Bug fixes that merely make a product operate in accordance with its specifications may be exported under Li-

cense Exception TSU.³² Upgrades that do not affect a product's cryptographic features may be exported under License Exception ENC.³³ In neither case is a second one-time review required prior to export of the bug fix or update.

GRANDFATHERING

As a general rule, strong encryption products that have been reviewed by BXA and the NSA through the classification and licensing procedures will be eligible for export as non-retail products. There is one small, but potentially important, exception, however. Licenses authorizing export only to subsidiaries of US companies will not qualify, because such licenses were "rubber stamped" in the past without in depth review.

Again, as a general rule, companies that want to qualify their products as "retail" will have to submit new commodity classifications. Again, however, there is an important exception. Products with encryption key lengths not exceeding 56 bits and asymmetric key exchange modulus in the range of 512 to 1,024 that have been reviewed by BXA and NSA through the classification and licensing procedures will be eligible for export as retail products.³⁴

WEAK CRYPTOGRAPHIC PRODUCTS

Considering the more liberal licensing treatment of strong encryption products, why would anyone export a weak cryptographic product? Actually, there are a number of reasons that companies may want to continue development of weak cryptographic products, among them:

1. Weak cryptographic products that are "publicly available" are not subject to US export controls at all.
2. Weak cryptographic products that are proprietary may be exported to governments without a license, even if they do not qualify as "retail."
3. Weak cryptographic products that are proprietary are released from "EI" controls. Therefore, incorporation of weak cryptographic products into foreign-made products does *not* result in the foreign-made products becoming subject to US export controls.
4. Weak cryptographic products may be eligible for export into certain foreign markets, whereas strong cryptographic products may not.

Nevertheless, it is important to note that exporters must submit weak cryptographic products for review by BXA and the NSA prior to export. Exporters may NOT self-classify weak cryptographic products.

"MASS MARKET" PRODUCTS NOT EXCEEDING 64 BITS

Mass market encryption hardware, software and technology with key lengths not exceeding 64 bits may be classified under 5A/D/E/992, after a one-time review. The definition of "mass market" is broader than the definition of

"retail," as there is no "large volume" test for sales via mail order, telephone transactions, and electronic downloads.³⁵

PRODUCTS THAT ARE NOT "MASS MARKET"

Encryption hardware, software, and technology with key lengths up to and including 56 bits with an asymmetric key exchange mechanism not exceeding 512 bits may be classified under 5A/D/E/992. Products that only provide key management with asymmetric key exchange mechanisms not exceeding 512 bits also may be classified under 5A/D/E/992. In addition, other products of similar strength will be considered case by case.³⁶

NOTIFICATION OF INTENT TO UPGRADE

Mass-market encryption products that have been reviewed and approved for export under License Exception TSU or ENC may be upgraded without an additional review. The exporter must submit a letter from a corporate official to BXA stating that the only change to the product is the encryption key length.³⁷

CONCLUSION

The new encryption regulations are more liberal, but also more complex, than the regulations they replace. Industry will have an opportunity to file comments in the next 120 days. Nevertheless, it appears that we are going to have to live with these new regulations, at least for the foreseeable future, because the prospects for legislation are not good. Representative Zoe Lofgren, who was one of the original co-sponsors of the SAFE Act, perhaps said it best: "It's not perfect, but it's not bad. Much of what we hoped to achieve through SAFE has been achieved through these regulations. It would be a mistake to move that bill, because we have gotten so much of what we'd hoped to achieve."³⁸

NOTES

1. 65 FR 2492 (Jan. 14, 2000).
2. Alan Davidson, Center for Democracy and Technology, quoted in David E. Sanger & Jeri Clausing, "U.S. Removes More Limits on Encryption," *N.Y. Times*, Jan. 13, 2000.
3. 15 C.F.R. § 740.17(e)(1).
4. *Id.*, § 740.17(a)(3)(i).
5. *Id.*, § 740.17(a)(3)(ii).
6. *Id.*, § 740.17(a)(3)(iii).
7. *Id.*, § 740.17(a)(3)(iv).
8. *Id.*, § 740.17(a)(3)(vi).
9. *Id.*, § 740.17(a)(3)(vii).
10. *Id.*, § 772.
11. *Id.*, § 740.17(a)(4).
12. *Id.*, § 742.15(b)(3).
13. *Id.*, § 740.13(e).
14. *Id.*, § 740.17(a)(5)(i).
15. *Id.*, § 740.17(a)(5)(ii).
16. *Id.*, § 740.17(a)(5)(iii).
17. *Id.*, § 740.17(g)(3).

18. *Id.*, § 740.17(g)(1)(ii), § 740.17(g)(1)(iii).
19. *Id.*, §§ 740.17(g)(1)(i), § 740.17(g)(1)(vi).
20. *Id.*, § 740.17(g)(1)(iv).
21. *Id.*, § 740.17(g)(1)(v).
22. *Id.*, § 740.17(g)(2)(ii).
23. *Id.*, § 740.17(g)(2)(i).
24. *Id.*, § 740.17(g)(5).
25. *Id.*, § 734.2(b)(9)(ii).
26. *Id.*
27. *Id.*, § 734.2(b)(9)(iii).
28. *Id.*, § 740.17(a)(1).
29. *Id.*
30. *Id.*, § 742.15(b)(3).
31. *Id.*, § 740.17(f).
32. *Id.*, § 740.13.
33. *Id.*, § 770.2(n).
34. *Id.*, § 770.17(e)(2).
35. *Id.*, § 742.15(b)(1)(iii).
36. *Id.*, §§ 742.15(b)(1)(i), 742.15(b)(1)(ii).
37. *Id.*, § 740.17(e)(3).
38. John Schwartz, "U.S. Eases Encryption Export Rules," *Wash. Post*, Jan. 13, 2000, at E1.