

US ENCRYPTION EXPORT REGULATION

US TO EU: ME TOO! - THE UNITED STATES AMENDS ITS EXPORT CONTROLS ON ENCRYPTION, RESPONDING TO RECENT DEVELOPMENTS IN THE EUROPEAN UNION

Roszel C. Thomsen II and Antoinette D. Paytas

This paper reviews the most recent changes to the US export controls on encryption items (referred to herein as the "US Regulations") that were published in the US Federal Register on 19 October, 2000.¹ It describes how the decision by the European Union (EU) Council of Ministers on 22 June 2000, to create a license free zone for exports of encryption (and other) items (referred to herein as the "EU Regulations") provided the initial stimulus for these changes. It also describes how the US Regulations fall short of matching the EU Regulations in some respects, while exceeding the EU Regulations in other respects. In addition, the authors offer recommendations for further reforms to the US encryption export control policy that might be addressed by the next administration in Washington. They conclude on a cautionary note, considering the possibility that the recent reforms to US encryption export control policy could be reversed in the future.

BACKGROUND

When the Clinton Administration came to Washington, encryption items were controlled for export from the United States as "munitions" under the Arms Export Control Act² and the International Traffic in Arms Regulations.³ Most applications for licenses to export strong encryption items were denied. Industry and public interest groups lobbied for liberalization, and the Clinton Administration reformed the outdated US export controls on encryption items in a series of graduated steps. Nevertheless, the US export controls on encryption items remain complex and onerous. American companies must submit encryption items for technical reviews by the intelligence authorities prior to export. Exports to some agencies of foreign governments require licenses, as do exports to telecommunications and Internet service providers wishing to provide services to some government agencies. Finally, post-export reporting requirements apply to many exports from the United States. Thus, US encryption export controls continue to impose a significant regulatory burden on American companies, retarding the worldwide deployment of strong cryptography, the protection of personal data, and the full flowering of Internet commerce.

THE EU'S LICENCE FREE ZONE INITIATIVE

When it amended the encryption export control regulations on 14 January 2000,⁴ the Commerce Department's Bureau of

Export Administration (BXA) anticipated that it might have to make further changes, in response to developments in the EU. Specifically, BXA said:

A number of companies have expressed concern that the European Union (EU) may implement a general authorization permitting encryption items to be exported freely within the EU and other specified countries. If and when the EU implements such an authorization, the Administration will take the necessary steps to ensure US exporters are not disadvantaged.⁵

On 23 June, the EU Council of Ministers adopted the new EU Regulations, designed to improve the existing system of export controls on dual use goods and technologies, including encryption. The EU Regulations create a harmonized EU General License (Community General Export Authorization) which covers the export of encryption items (except cryptanalytic items) within the fifteen EU member states and ten of its close trading and security partners: Australia, Canada, Czech Republic, Japan, Hungary, Norway, New Zealand, Poland, Switzerland and the United States. The text of the EU Regulation was published in the Official Journal on 30 June 2000.⁶

Washington responded quickly. On 17 July, White House Chief of Staff John Podesta gave a speech at the National Press Club in which he proposed new measures to assure the security and trust of Americans in cyberspace. His speech emphasized the themes of updating law enforcement authorities for the Internet age, harmonizing the rules that apply to different technologies such as telephones and E-mail, and balancing important values. He proposed legislation that would give

law enforcement important new tools to pursue criminals through cyberspace while also boosting citizens' fundamental rights to privacy in the electronic age. Mr. Podesta also announced new rules that will update encryption export controls. In a contemporaneous announcement, the White House Press Office said:

Today, the Administration is updating its policy for encryption exports to the European Union and other key trading partners, thus assuring continued competitiveness of US industry in international markets. Under the new policy, US companies can export under license exception (i.e., without a license) any encryption product to any end user in the 15 nations of the European Union as well as Australia, Norway, Czech Republic, Hungary, Poland, Japan, New Zealand and Switzerland. Previous distinctions between government and non-government end users are removed for these countries. Further, US exporters will be permitted to ship their products to these nations immediately after they have submitted a commodity classification request for their product to the Department of Commerce. Exporters no longer have to wait for a completed technical review or incur a 30-day delay to ship their encryption products to customers in these nations. These updates track with recent regulations adopted by the European Union that ease encryption exports to the same countries. Consistent with the Administration's January 2000 commitment, US companies can continue to compete effectively in these markets. The steps announced today continue our policy to serve the full range of national interests: promote electronic commerce, support law enforcement and national security, protect privacy, and maintain US industry leadership in security technologies.⁷

THREE PILLARS OF US ENCRYPTION POLICY

The US encryption export control policy rests on three pillars. First, the US Government should have an opportunity to conduct a technical review of all cryptographic products prior to export. Second, the US Government should have the right to restrict exports of certain cryptographic products to governments through the export licensing process. Third, the US Government should receive post-shipment reporting with respect to some exports of cryptographic products. The US Regulations revise each of these requirements, in light of the EU Regulations.

Pre-Export Technical Reviews

Prior to publication of the US Regulations, American exporters had to submit their products to the Commerce Department's Bureau of Export Administration (BXA) and the National Security Agency (NSA) for review and approval under the Commodity Classification Request procedure, prior to commencing of exports. They generally could commence exporting on a limited basis thirty days after submission of a completed Commodity Classification Request, but BXA and NSA retained the right to deny exports of offending products if, for example, they included open cryptographic interfaces.

Under the new US Regulations, exporters may commence international shipments of cryptographic products promptly upon filing of a Commodity Classification Request with BXA and NSA.⁸ Preparation of a Commodity Classification Request is not a trivial task, as a properly completed submission must address a host of features in a level of detail in excess of that which customarily is disclosed in a vendor's product

literature. However, there is no time lag between filing of the application and receipt of approval to export to the EU and its partners. Equally importantly, there are no features that can render a decision that a product requires a license for export to the EU and its partners.

A checklist containing the information that must be supplied can be found at <www.t-b.com/cryptolist.htm>. Additional, special rules apply to Commodity Classification Requests for components and source code. Careful consideration must be given to the scope of disclosure required in applications for technical review, protection of information against unauthorized disclosure by US government employees who may review the application, and how best to expedite processing of applications by the relevant agencies.

In addition to technical disclosure, a properly completed Commodity Classification Request must address whether a cryptographic product meets either the "retail" or "mass market" criteria under the new US Regulations. These criteria are important, because products that qualify as either "retail" or "mass market" may be subject to less onerous restrictions governing their export to destinations outside the EU and its partners. Careful drafting also can optimize the likelihood of obtaining "retail" or "mass market" status.

Under the new US Regulations, some items are exempt from a technical review prior to export. Section 740.17(b)(3)(vi) states:

"Items which would be controlled only because they incorporate components or software which provide short-range wireless encryption functions may be exported without review and classification by BXA and without reporting under the retail provisions of *this section*."⁹

The Preamble to the new US Regulations provides the following additional guidance:

"In §740.17(b)(3) (Retail Encryption Commodities and Software), License Exception ENC is revised to authorize, without prior review and classification or reporting, those items which are controlled only because they incorporate components providing encryption functionality which is limited to short-range wireless encryption, such as those based on the Bluetooth and Home Radio Frequency (HomeRF) specifications. Examples of such products include audio devices, cameras and videos, computer accessories, handheld devices, mobile phones and consumer appliances (e.g., refrigerators, microwaves and washing machines)."

Unlike Bluetooth and HomeRF products, products developed according to IEEE 802.11b specifications are *not* eligible for this exemption, which is a source of lingering concern to US industry. The preamble is the only place in the new US Regulations where Bluetooth and HomeRF are specified by name. Experience with some test cases will determine the scope and effect of this new exemption.

In contrast with the new US Regulations, the EU Regulations do *not* specify that cryptographic products must be submitted for a technical review prior to export. At the same time, they do not prevent member governments from imposing technical review requirements in their national legislation. Some countries, notably France, historically have implemented technical review requirements more onerous than US Regulations. It is too soon to know whether governments in the EU and its partners will

require that cryptographic products be submitted for a technical review prior to export. However, consistent with prior practice, we anticipate that only a handful of countries are likely to do so.

Licensing of Exports to Governments

Prior to publication of the new US Regulations, BXA divided strong cryptographic products into two categories. So-called "retail" products could be exported after technical review without further licensing to governments. Products that did not qualify as "retail" required a license for export to governments.

The new US Regulations eliminate the distinction between "retail" and other strong encryption products, for purposes of sales to governments in the EU and its partners. All cryptographic products may be exported to governments in qualifying countries without further review or approval.¹⁰ In this respect, exporters in the United States and EU will compete on a level playing field. However, the distinction between "retail" and other strong encryption products remains important for Americans who export to countries beyond the EU and its partners.

The new US Regulations define "retail" strong encryption products as follows:

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

- (i) Sold in tangible form through retail outlets independent of the manufacturer;
- (ii) Specifically designed for individual consumer use and sold or transferred through tangible or intangible means; *or*
- (iii) Which are or will be 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:

- (i) Cryptographic functionality can be easily changed by the user;
- (ii) Requires substantial support for installation and use;
- (iii) Cryptographic functionality has been modified or customized to customer specifications; *and*
- (iv) Network infrastructure products such as high-end routers or switches designed for high volume communications.¹¹

The definition of "retail" bears a striking resemblance to the definition of "mass market" in the Cryptography Note under the Wassenaar Arrangement¹². However, there are two important differences between the new definition of "retail" and the definition of "mass market". The first difference is the inclusion of the words "large volume" in "positive" test number three. This change makes 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. This change makes it more difficult for exporters of routers, switches and firewalls, for example to qualify their products as "retail" and to compete on a level playing field with foreign suppliers of similar network infrastructure products.

Inextricably intertwined in the new US Regulations are the definition of "retail" and the definition of "government

end-user", because products that do not qualify as "retail" require a license for export to a "government end-user" outside the EU and its partners. For purposes of the new US Regulations, the definition of "government end-user" is as follows:

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 ... 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.¹³

Screening of customers to determine whether they fall within the definition of "government end-user" is the bane of US exporters' existence, requiring judgment calls and careful guidance to channel partners, so that strong encryption products are licensed properly.

In addition, telecommunications and Internet service providers outside the EU and its partners must obtain a license prior to providing services specific to government end-users using products that have not been granted "retail" status.¹⁴ Covered services include wide area network, local area network, virtual private network, voice and dedicated link services, application specific and electronic commerce services, and public key infrastructure encryption services specifically for government end-users only.

In comparison with the new US Regulations, EU member governments are free to devise licensing policies and procedures governing exports to countries outside the EU and its partners, at their national discretion under the EU Regulation and the Wassenaar Arrangement. The United States has "bulk" licensing mechanisms, known as *License Exception ENC* and *Encryption Licensing Arrangements* that have analogues in other countries, like the United Kingdom's *Open General Export License* and *Open Individual Licenses*¹⁵. However, it is hazardous to speculate as to whether US encryption licensing policy will be broadly similar to the policies of the various EU member countries, because of the broad national discretion afforded to member governments under the Wassenaar Arrangement and the EU Regulations.

Post-Export Reporting Requirements

Post-export reporting requirements in the new US Regulations do not have an analogue under the EU Regulations. In general, US exporters must file a biannual report including the name and address of the recipient of every cryptographic product (and the end-user, if known) unless one of the following exemptions applies:

- (i) any encryption to US subsidiaries for internal company use;

- (ii) finance-specific products;
- (iii) encryption commodities or software with a symmetric key length not exceeding 64 bits or otherwise classified as qualifying for mass market treatment;
- (iv) Retail products exported to individual consumers;
- (v) Items exported via free or anonymous download;
- (vi) Encryption items from or to a US bank, financial institution or their subsidiaries, affiliates, customers or contractors for banking or financial operations;
- (vii) Items which incorporate components limited to providing short-range wireless encryption functions;
- (viii) Retail operating systems, or desktop applications (e.g. E-mail, browsers, games, word processing, data base, financial applications or utilities) designed for, bundled with, or pre-loaded on single CPU computers, laptops or hand-held devices;
- (ix) Client Internet appliance and client wireless LAN cards;
- (x) Foreign products developed by bundling or compiling of source code.¹⁶

Recognizing that the reporting requirements are burdensome on US exporters, the Clinton Administration introduced several new exemptions in the new US Regulations.

Exemption (vii), which governs "short range wireless" functions, is new and notable. Intended initially to remove reporting from products that implement so-called *Bluetooth* standard with a range of 30 meters or less, it probably also probably exempts products based upon the HomeRF standard.

Exemption (viii) is an important victory for American exporters, as it exempts from reporting most shrink wrap software. However, it is also problematic, as it is limited to software designed for "single CPU computers". This language may exclude operating systems like UNIX, designed for multiple CPU computers, as well as shrink wrap software for server applications.

Exemption (ix) is a modest victory for makers of wireless networking products implementing the IEEE 802.11b standard, exempting NIC cards and PC cards, but not access points, from reporting. Note that products implementing the IEEE 802.11b standard are not exempt under (vii) above.

Exemption (x) appears on the surface to be attractive to persons outside the United States who may incorporate US-origin source code in their products. However, it is really just a clarification, rather than an extension, of the prior practice under regulations in effect before 19 October 2000.

Looking at the exemption for short range wireless products and software for single CPU computers, laptops and hand-held devices, NICs and PC cards it appears that the regulators are searching for a clean way of describing "consumer" products that should be exempt from reporting. Further efforts in this regard are highly desirable.

In addition, BXA issued an important clarification in the US Regulations governing reporting by subsidiaries of US companies located outside the United States. Previously, US companies reported exports from the United States, and subsidiaries abroad reported their exports and re-exports. This requirement made it difficult to collect information for consolidated filing of reports and placed subsidiaries abroad at a disadvantage *vis-à-vis* local distributors who did not have to report. BXA has clarified the situation in the new US Regulations, so that US companies are required to report exports from the United States, but they are not required to collect information from their

subsidiaries abroad, nor are the subsidiaries required to file separate reports.

BXA also eliminated a particularly onerous reporting requirement that applied only to a handful of companies exporting network infrastructure equipment. Under the old regulations, exporters had to file contemporaneous reports describing network infrastructure equipment sold to telecommunications and Internet service providers outside the United States. These reporting requirements were eliminated in the new US Regulations.

OTHER IMPORTANT CHANGES

At the request of various industry trade associations, BXA also made a number of changes that, although not directly responsive to the EU's initiative, should improve the competitiveness of American companies. These changes involve the regulations governing cryptographic application programming interfaces (APIs), source code, beta test software, technical assistance, the so-called *de minimis* rule, and rules governing weak cryptography.

Cryptographic APIs

Under the prior regulations, products incorporating "open" cryptographic APIs generally were not eligible for export, except under license. "Open" cryptographic APIs allow a third party to substitute cryptographic libraries of their choosing for the libraries supplied by the vendor. The rationale for restricting exports of products incorporating "open" cryptographic APIs was that BXA and NSA could not conduct a thorough technical review of products, if the recipient was able to insert the cryptographic library of preference and replace the cryptographic provider supplied initially by the developer.

As a result of this restriction on exports of products with open cryptographic APIs, American companies resorted to various mechanisms to restrict the ability of third parties to replace the cryptographic service provider supplied with the product. Most of these mechanisms involved some kind of digital signature mechanism, so that only cryptographic providers approved and signed by the developer would interoperate with the developer's cryptographic infrastructure. These products were referred to as having "closed" cryptographic APIs.

The new US Regulations change the rules with respect to both "open" and "closed" cryptographic APIs. Products with "open" cryptographic APIs may be exported to all destinations in the EU and its partners, like other cryptographic products.¹⁷ In addition, vendors of products with "closed" cryptographic APIs are permitted to "sign" cryptographic providers developed by third parties outside the United States, without prior review by BXA or NSA.¹⁸

The EU Regulations do not contain special rules governing exports of products with "open" cryptographic APIs. US industry had urged that the restrictions on cryptographic APIs be removed entirely in the new US Regulations. One can anticipate that such requests will be renewed, when the next administration comes to Washington.

Source Code

Cryptographic source code controls fall into three categories: (a) open source, (b) community source, and (c) proprietary

source. The rules governing exports of each type of source code are different, and the have been amended in important respects in the new US Regulations. Open source refers to software that is available to the public without restriction free of charge, under a GNU-style license agreement. Linux is an instructive example of open source. The old regulations allowed the export of open source to any end-user without a technical review, provided that the person making the open source available filed a contemporaneous notification with BXA and NSA. However, the prior regulations were silent with respect to restrictions (if any) on the export of compiled executable software derived from open source. Under the new US Regulations, compiled executable software derived from open source is eligible for export under the same conditions as the open source itself, provided that the compiled executable is available without restriction and free of charge.¹⁹ Unfortunately, if you include the compiled executable software into a product that you distribute for a fee, then the resulting product must be submitted for a one-time technical review, described above.

Community source refers to software that is available to the public free of charge for non-commercial use but that contains further restrictions on commercial use. Community source may be exported under essentially the same conditions as open source, but community source remains subject to more detailed reporting requirements.²⁰

Proprietary source refers to all source code that is neither "open" nor "community" source. Exporters may provide proprietary source code to any end-user in the EU and its partners, and to any non-government end-user in other countries, promptly upon filing of a technical review with BXA and NSA.²¹ The same reporting requirements applicable to community source also apply to proprietary source.

Beta Test Software

The new US Regulations revise the export controls applicable to beta test software in several important respects. Strong encryption software is eligible for export without prior technical review and classification, provided that the exporter submits a pre-export notification to BXA and NSA describing the cryptographic features and provides a post-export report of the names and addresses of the recipients (except individual end-users) bi-annually.²²

The regulators deliberated at length regarding the scope of products that should be eligible for export under the beta test software provisions. In the end, they determined that only products meeting the Wassenaar Cryptography Note or Mass Market Note should be eligible. The next Administration in Washington will face pressure to extend the beta testing authorization to additional classes of cryptographic products.

Technical Assistance

When the State Department transferred the jurisdiction to control exports of encryption items to the Commerce Department on 30 December 1996, BXA essentially replicated an especially controversial aspect of the State Department's regulations purporting to require a license for the transfer of "technical assistance" to parties outside the United States with the intent to assist such parties in the design and development

of encryption products. This provision was controversial, because it purported to control such transfers, even if all of the information transferred were in the public domain or otherwise generally available. Whether such a provision would survive free speech protections of the First Amendment to the United States Constitution is problematic, and the issue has never been litigated to a final judgment by a court of competent jurisdiction. In order to remove sources of potential challenge, BXA has amended this provision, so that it does *not* apply to participation in standards development, such as efforts by the Internet Engineering Task Force and other, similar groups.²³ BXA also has exempted all transfers to the EU and its partners from the license requirement.

De Minimis Rule

One of the more controversial aspects of the new US Regulations is the so-called *de minimis* rule. In order to understand the *de minimis* rule and changes thereto, one first must recognize that the United States asserts jurisdiction extraterritorially with respect to products and technologies that are of US-origin. For example, Germany may take the position that it controls the export of products from Germany to Singapore, but only the government of Singapore has jurisdiction to license the re-export of the same product from Singapore to India. By comparison, the United States takes the position that it has jurisdiction to control not only the export of products from the United States to Singapore, but also the re-export from Singapore to India. The same rules apply where a US-origin part or component is incorporated into a foreign end-product. One can easily understand that many governments view the US extraterritorial assertion of controls beyond its borders as overreaching!

The *de minimis* rule states that if the US-origin content in a foreign-origin end-product falls below a specified threshold, then the foreign-origin end-product is exempt from US export controls. The new US Regulations provide that encryption items *may* be eligible for *de minimis* treatment *if* approved under the technical review process.²⁴ The preamble to the new US Regulations provide only limited guidance with respect to what products may be eligible, nor does it provide any "grandfathering" for products that already have been through the technical review process, despite repeated requests from industry. As a result, BXA will have to re-review a number of products that already have been through the one-time technical review, causing a significant backlog to develop at BXA and NSA.

Weak Encryption Items

The new US Regulations revise the controls on weak encryption items, permitting their export immediately upon submission of a notification that describes the relevant cryptographic features. The information that applicants must submit is substantially similar to that which is required for Commodity Classification Requests for strong encryption products.²⁵

CONCLUSION

The Clinton Administration implemented significant changes in the export controls on encryption items incrementally and

reluctantly, only after its attempts to influence the market to adopt key escrow failed. Over the years, its ability to convince the Congress to support stringent export controls ebbed away, to the point where a majority of Members of the House of Representatives supported legislation to remove the export controls in the form of the Security and Freedom through Encryption (SAFE) Act.²⁶ It lost a crucial First Amendment challenge to the validity of the export controls on cryptographic source code, *Bernstein v United States*²⁷ at both the trial court and the initial appellate review. Driven by the EU's decision to create a license free zone for encryption products, the Clinton Administration once again revised its encryption export control policy, only weeks before the Presidential election.

The authors have pointed out that there are areas where further revisions may be warranted. Nevertheless, it is worth considering the possibility that the pendulum, which has swung in the direction of liberalization for almost a decade, might swing back in the direction of further tightening of the export controls on encryption items. An instructive example is the US export controls on commercial satellites.

As in the case of encryption, reacting to pressure from the affected industry, the Clinton Administration transferred jurisdiction with respect to export controls on commercial satellites from the Department of State to the Department

of Commerce.²⁸ However, the Congress, responding to incidents featured in the so-called Cox Report, passed legislation transferring jurisdiction back to the Department of State,²⁹ resulting in an enormous loss of market share on the part of American satellite manufacturers, according to industry representatives.

It is not difficult to anticipate possible events that could trigger a reconsideration of the trend toward liberalization of encryption export controls. A domestic terrorist incident or other heinous crime in which cryptography was employed by the perpetrators could serve as the catalyst. An international incident caused by the inability to decrypt signals intelligence in a timely manner likewise could trigger a re-assessment of the current export controls on cryptographic products. The debate over the appropriate export controls on encryption in the United States likely will enter an hiatus during the next six months or so, until after the elections, but it is not over.

Roszel C. Thomsen II roz@t-b.com is a Partner, and **Antoinette D. Paytas** tpaytas@t-b.com is an Associate, with the law firm of Thomsen and Burke LLP <www.t-b.com>. Roz and Toni concentrate in the field of export controls, with particular emphasis on the laws and regulations governing information technology.

FOOTNOTES

¹65 Fed. Reg. 62600 (2000).

²22 USC. 2778.

³22 C.F.R. 120 *et. seq.*

⁴65 Fed. Reg. 2492 (2000).

⁵*Id.*

⁶2000 O.J. (L 159) 1.

⁷See <http://www.pub.whitehouse.gov/uri-res/12R?urn:pdi://oma.eop.gov.us/2000/7/17/16.text.1>

⁸15 C.F.R. § 740.17(d)(1)(i).

⁹*Id.* at § 740.17(b)(3)(vi).

¹⁰*Id.* at § 740.17(a).

¹¹*Id.* at § 740.17(b)(3).

¹²See <http://www.wassenaar.org>

¹³*Id.* at § 772.

¹⁴*Id.* at § 740.17(b)(2)(ii).

¹⁵See <http://www.dti.gov.uk/export.control/>

¹⁶*Id.* at § 740.17(e)(1).

¹⁷*Id.* at § 740.17(a)(5)(i).

¹⁸*Id.* at § 740.17(a)(5)(ii).

¹⁹*Id.* at § 740.13(e)(2).

²⁰*Id.* at § 740.17(b)(4)(i).

²¹*Id.* at § 740.17(b)(4)(ii).

²²*Id.* at §740.9(c)(3).

²³*Id.* at § 744.9(a).

²⁴*Id.* at § 734.4(b).

²⁵*Id.* at § 742.15(b)(1).

²⁶H.R. 850.

²⁷See <http://www.epic.org/crypto/export_controls/bernstein_decision_9_cir.html>

²⁸61 Fed. Reg. 56894 (1996).

²⁹Pub. L. 105-261.