

# US ENCRYPTION EXPORT CONTROL POLICY UPDATE 2002

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

The United States maintains export controls on military cryptographic products and technology under the Arms Export Control Act (AECA)<sup>1</sup> and the International Traffic in Arms Regulations (ITAR)<sup>2</sup> and on dual-use cryptographic products and technologies under the Export Administration Act (EAA)<sup>3</sup> and the Export Administration Regulations (EAR).<sup>4</sup> These export controls are coordinated with members of the Wassenaar Arrangement. The United States recently updated its export control regulations governing cryptographic products and technologies<sup>5</sup> in order to reflect changes made to the Wassenaar Arrangement List of Dual-use Goods and Technologies And Munitions List and to clarify other provisions of its policy with respect to cryptographic export controls.

In general, persons who export cryptographic products and technologies must submit them for a one-time technical review to the Bureau of Industry and Security (formerly the Bureau of Export Administration (BXA)) and the National Security Agency (NSA) prior to export. Some exports of cryptographic products and technologies require licenses issued by the Bureau of Industry and Security (BIS). In many cases, post-export reporting to BIS and NSA also is required.

Although the recent policy update is welcomed by industry, the cryptographic export control policy remains complex and still favors some products (particularly open source products) over others (including proprietary source products). Further reform is not currently a high priority of the US government. Concerted effort by industry will be required to achieve further reforms.

*Roszel C. Thomsen II and Antoinette D. Paytas are with Thomsen and Burke LLP.*

The laws and regulations governing the export of cryptographic products and technologies were quite simple when George H.W. Bush became president in 1988. All cryptographic products and technologies were regarded as "munitions" subject to the jurisdiction of the State Department's Office of Defense Trade Controls under authority of the AECA and the ITAR. The policies and procedures governing the issuance of export licenses were simple, too. All exports required licenses, and all applications for licenses were denied (unless the customer was either a subsidiary of a US company or a financial institution).

At the time, diplomats and the military were the primary users of cryptographic products. However, the population of users was beginning to increase and diversify. A number of factors precipitated these trends. The invention of public key cryptography by Diffie and Hellman made it easier to exchange cryptographic keys. The

## IN THIS ISSUE

**BROADBAND: WHERE COMMUNICATIONS  
AND INTERNET POLICY CONVERGE** ..... 8

*by Christy C. Kunin*

**EC COMPETITION LAW ASPECTS  
OF PEER-TO-PEER NETWORKING** ..... 12

*by Erik Vollebregt*

## COLUMNS



|                            |    |
|----------------------------|----|
| Case Law Update            | 16 |
| • Telecommunications Law   | 16 |
| • Internet Law             | 17 |
| • Trademark                | 22 |
| International Developments | 23 |



# JOURNAL OF INTERNET LAW

Copyright © 2002 by Aspen Law & Business, A Division of Aspen Publishers, Inc.  
A Wolters Kluwer Company

JOURNAL OF INTERNET LAW (ISSN# 1094-2904) is published 12 times per year by Aspen Publishers, Inc., 1185 Avenue of the Americas, New York, NY 10036. Telephone: 212-597-0200. One year subscription (12 issues) price: \$315. Single issue price: \$31.50. To subscribe, call 1-800-638-8437. For customer service, call 1-800-562-1973. Postmaster: Send address changes to JOURNAL OF INTERNET LAW, Aspen Publishers, Inc. 7201 McKinney Circle, Frederick, MD 21704. Periodicals postage paid at New York, New York 10036.

## BOARD OF EDITORS

### Founder

**David B. Rockower**

### Editor-in-Chief:

**Mark F. Radcliffe**

Gray Cary Ware & Freidenrich  
Palo Alto, CA

### Executive Managing Editor:

**William Reilly**

### Executive Editor:

**Maureen S. Dorney**

Gray Cary Ware & Freidenrich

### Associate Editors:

**James Cannon**

**David Dolkas**

**Elizabeth Eisner**

**Ian Feinberg**

**Jeffrey Harnes**

**Peter Leal**

**Val Luessenhop**

**Scott Pink**

**Ailyn Taylor**

**Jim Vickery**

**Joe Villela**

**Gabriele Walker**

**Mark Wicker**

Gray Cary Ware & Freidenrich

### Group Publisher

**Richard H. Kravitz**

Director, Newsletters

**Beverly F. Salbin**

Managing Editor

**Kathleen Brady**

Production Coordinator

**James M. Fraleigh**

### EDITORIAL OFFICES

400 Hamilton Avenue

Palo Alto, CA 94301

(650) 328-6561

1185 Avenue of the Americas

New York, NY 10036

(212) 597-0200

### EDITORIAL BOARD

**Constance Bagley**

Associate Professor of Business

Administration,

Harvard Business School

**Robert G. Ballen**

Schwartz & Ballen,

Washington, D.C.

**Ian C. Ballon**

Manatt, Phelps & Phillips LLP

Palo Alto, CA

**Henry V. Barry**

Wilson, Sonsini, Goodrich & Rosati

Palo Alto, CA

**Jon A. Baumgarten**

Proskauer Rose

Washington, D.C.

**Michel Béjot**

Bernard, Hertz & Béjot

Paris, France

**Kevin J. Connolly**

Duval & Stachenfeld

New York, NY

**Stephen J. Davidson**

Leonard, Street and Deinard

Minneapolis, MN

**G. Gervaise Davis III**

Davis & Schroeder, P.C.

Monterey, CA

**Edmund Fish**

General Counsel

Intertrust, Sunnyvale, CA

**Prof. Michael Geist**

U. of Ottawa Law School

Goodman, Phillips & Vineberg,

Toronto, CA

**Morton David Goldberg**

Schwab Goldberg Price

& Darnay

New York, NY

**David Goldberg**

Cowan, Liebowitz & Lotman, P.C.

New York, NY

**Allen R. Grogan**

General Counsel,

Viacore, Inc.

Orange, CA

**Prof. Trotter Hardy**

School of Law

The College of William & Mary

**Peter Harter**

Security, Inc.

Mountain View, CA

**David L. Hayes**

Ferwick & West LLP

Palo Alto, CA

**Ronald S. Katz**

Coudert Brothers

San Francisco, CA

**Ronald S. Laurie**

Skadden, Arps, Slate,

Meagher & Flom, LLP

Palo Alto, CA

**Jeffrey S. Linder**

Wiley, Rein & Fielding

Washington, D.C.

**Charles R. Merrill**

McCarter & English

Newark, NJ

**Christopher Millard**

Clifford Chance

London, England

**Prof. Ray T. Nimmer**

Univ. of Houston Law Center

**Lee Patch**

General Counsel

Sun Microsystems'

JavaSoft Division

Mountain View, CA

**Hilary Pearson**

Bird & Bird

London, England

**MaryBeth Peters**

U.S. Register of Copyrights

Washington, DC

**David Phillips**

CEO

iCrunch Ltd.

London, England

**Michael Pollack**

General Counsel

Elektra Entertainment

New York, NY

**Thomas Raab**

Wessing Berenberg-Gossler

Zimmerman Lange,

Munich, Germany

**Lewis Rose**

Arent Fox Kintner Plotkin & Kahn

Washington, D.C.

**Judith M. Saffer**

Asst. General Counsel

Broadcast Music, Inc.

New York, NY

**Prof. Pamela Samuelson**

Boalt School of Law

University of California at Berkeley

**William Schwartz**

Morrison & Foerster

San Francisco, CA

**Eric J. Sinrod**

Duane, Morris & Hecksher LLP

San Francisco, CA

**Katherine C. Spelman**

Steinhart & Falconer, LLP

San Francisco, CA

**William A. Tanenbaum**

Kaye, Scholer, Fierman, Hays &

Handler, LLP

New York, NY

**Richard D. Thompson**

Bloom, Hergott, Cook,

Diemer & Klein, LLP

Beverly Hills, CA

**Roszel Thomsen, II**

Thomsen and Burke, LLP

Washington, D.C.

**Dick C.J.A. van Engelen**

Stibbe Simont Manohan Duhot

New York, NY

**Joel R. Wolfson**

Assoc. General Counsel

Blank Rome Connolly & McCauley LLP

Washington, D.C.

increasing power of personal computers made it feasible for ordinary folks to use sophisticated cryptographic algorithms. Software publishers began to implement cryptographic features into their products. As a result, industry and public interest groups began lobbying the government to relax the onerous export controls on cryptography.

A trend toward the progressive relaxation of export controls on cryptography has proceeded for the last decade and a half. First, products that used cryptography for limited purposes, such as access control and authentication, were transferred from the "munitions" control regime to the jurisdiction of the Commerce Department's Bureau of Export Administration (as it was known at that time), which administers export controls on "dual-use" products under authority of the EAA and EAR.<sup>6</sup> Second, products using "weak" encryption for privacy of communications and stored data were transferred from the munitions to the dual-use control regime.<sup>7</sup>

Nevertheless, neither the government, industry, nor public interest groups were entirely satisfied with the state of encryption export controls at the end of the presidency of George H.W. Bush. The government continued to insist that widespread use of cryptography threatened its ability to conduct electronic surveillance. Despite tacit assurances from the government that the permitted standard for export of weak cryptography would increase over time, industry felt that weak cryptography was not likely to be competitive with stronger cryptographic products available from sources outside the United States. Public interest groups were concerned that Big Brother was using the export control laws and regulations to prevent the people from protecting themselves against threats to the security of their personal information.

In the early years of the Clinton administration, the public debate over the export controls on cryptography became increasingly rancorous. The Clinton administration attempted to reconcile the government's interest in surveillance with the public's interest in strong cryptography through a policy known over time as "key escrow," "key recovery," or "key management."<sup>8</sup> The basic premise was that the strong cryptographic products should be eligible for export, but only if they incorporated a feature allowing access to the keys required for the government to obtain access to plaintext. The Clinton administration's key escrow/recovery/management policy was an abject failure. The market resoundingly rejected products incorporating such key escrow/recovery/management features, and foreign competitors began to displace US companies in the marketplace.

Finally, in January 2000, the Clinton administration essentially abandoned its export control policy based on key escrow/recovery/management. It replaced the regime favor-

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other professional assistance is required, the services of a competent professional person should be sought. — From a Declaration of Principles jointly adopted by a Committee of the American Bar Association and a Committee of Publishers and Associations.

The opinions expressed are for the purpose of fostering productive discussions of legal issues. In no event may these opinions be attributed to the authors' firms or clients or to Gray Cary Ware & Freidenrich or its attorneys or clients.

ing key escrow with a policy supported by three pillars. First, the government would have the opportunity to conduct a technical review of most cryptographic products prior to export. Second, the government would retain the right to license certain types of particularly sensitive exports. Third, the government would receive reports of exports, after the fact.<sup>9</sup>

---

**The Clinton administration's key  
escrow/recovery/management policy  
was an abject failure.**

---

The government has modified the export controls on cryptography twice since January 2000. In October of 2000, the Clinton administration created a license-free zone for exports of cryptographic products between and among the 15 members of the European Union and eight other countries.<sup>10</sup> In June of 2002, the George W. Bush administration amended the export controls on cryptography to conform to the changed adopted by the Wassenaar Arrangement in December 2000.<sup>11</sup>

Although the export controls on cryptographic products are undoubtedly much more liberal than they have been in the past, they also have become far more complex. This unfortunate complexity, combined with a lack of transparency and still substantial pre-export review and post-export reporting requirements, remains a significant burden on industry, retarding exports of strong cryptographic products that are essential to protecting the privacy of businesses and consumers. The purpose of this paper is to describe the most recent changes to the export controls on cryptographic products, as well as to suggest further reforms that would reduce the regulatory burden without compromising legitimate national security and foreign policy interests of the United States.

**PURPOSES OF EXPORT  
CONTROL REFORMS**

The primary purpose of the recent encryption export control policy update is to implement the changes to the Wassenaar List of Dual-use Products and Technologies. In December 2000, the members of the Wassenaar Arrangement eliminated the 64-bit limitation on products meeting the requirements of the Cryptography Note. As a result of this change, none of the other members of the Wassenaar Arrangement imposed export controls on mass-market cryptographic products, regardless of algorithm, key length, or key management features they might implement, after the spring 2001. In order to avoid unilaterally disadvantaging US companies vis-à-vis their for-

eign competitors, the George W. Bush administration had to publish an implementing regulation in the Federal Register.

A secondary purpose of the recent encryption export control reforms is to update and clarify other provisions of the regulations governing encryption export controls. These changes certainly are welcomed, but they fall short of real simplification. Furthermore, the regulations still express a preference for certain types of software, notably so-called open source software, at the expense of proprietary software.

There are several reasons why the George W. Bush administration's first attempts to reform the encryption export controls took so long and are so modest, especially when compared with prior changes. The export controls on cryptography have been reformed to such an extent that, quite frankly, they are no longer the politically charged issue of yore. As a result, the National Security Council under George W. Bush did not take the leadership role that it had during the Clinton administration. Political appointees at the Bureau of Export Administration focused on other priorities, including attempts to re-new the EAA, which has lapsed. Finally, the new regulations were nearing publication when the tragedy of September 11, 2001, occurred. There were suggestions that the terrorists had used cryptography to hide evidence of their crimes, and Senator Judd Gregg (R-NH) even suggested that the government should revert to its (failed) key escrow policy.<sup>12</sup> Under the circumstances, a decent interval had to elapse before it would be politically acceptable to relax the export controls on cryptography.

**WASSENAAR CRYPTOGRAPHY NOTE**

For more than a decade, Wassenaar member countries (and their predecessors at COCOM) had recognized that products available through mass-market channels simply were not susceptible to effective export controls. However, until December 2000, the Wassenaar Cryptography Note placed a limitation of 64 bits on products with symmetric algorithms that qualified for decontrol under the note.

Conforming US regulations to the Wassenaar changes, mass-market products today are classified under Export Control Classification Number (ECCN) 5A992 and 5D992, after a one-time review by BIS and NSA, and are eligible for export to most destinations under No License Required (NLR). In addition, such products are exempt from the post-export reporting requirements and are automatically eligible for consideration under the *de minimis* provisions of the EAR.

Despite this important change, the basic structure of the cryptographic export controls remains essentially

intact. There are some clarifications and updates to the technical review, licensing, and reporting requirements, but they are modest.

#### **TECHNICAL REVIEW REQUIREMENT**

BIS and NSA still conduct a technical review of most cryptographic products prior to their initial export from the United States. However, the mechanism for administering this review and the scope of products requiring review have changed.

#### **TECHNICAL REVIEW MECHANISM**

BIS no longer conducts technical reviews under the Commodity Classification Request procedure. The information that exporters must supply to BIS and NSA has not changed, however. The reason for this change is that legislation to renew the EAA currently pending before Congress contains a provision that will allow other agencies, in addition to BIS and NSA, to review Commodity Classification Requests.<sup>13</sup> Neither the George W. Bush administration nor the public perceive benefit in having other agencies, notably the Defense, Energy, Justice and State Departments, involved in the technical review of cryptographic products. Therefore, the technical review of cryptographic products was removed from the Commodity Classification Request procedure.

In addition, exporters should be aware of three other initiatives that will change the way they file technical review requests. The SNAP electronic filing system will be modified to reflect the new technical review procedure. The SNAP system also will become mandatory for all filings. In addition, the SNAP system will be upgraded to allow electronic submission of supporting documents.

One might hope that these changes to the technical review mechanism will expedite the processing of new applications. In 2001, exporters filed approximately 1,900 Commodity Classification Requests, of which approximately 1,300 were for products classified under ECCN 5A002 and 5D002 (approximately 81 percent of which received the most favorable "retail" treatment). An additional 600 applications were filed for products classified under 5A992 and 5D992. The average processing time was 56 days in 2001.<sup>14</sup>

#### **NEW ELIGIBILITY FOR TECHNICAL REVIEW**

BIS created a new class of products that are eligible for export after the required technical review for cryptographic test equipment classified under ECCN 5B002. Note, however, that this new eligibility does not extend to cryptanalytic equipment, which remains subject to licensing requirements to all destinations.<sup>15</sup>

#### **NEW EXEMPTION FROM TECHNICAL REVIEW**

BIS has created a new exemption from the technical review requirement, for products implementing the WiFi wireless encryption standard (also known as IEEE 802.11b). The purpose of this change is to create a level playing field for various wireless encryption products. Prior to this change, only products implementing Bluetooth and HomeRF standards, but not 802.11b, were exempt from the technical review.<sup>16</sup>

#### **EXPORT LICENSING REQUIREMENT**

The export licensing requirements for cryptographic products have been modified in several minor respects. In 2001, the Commerce Department received approximately 200 applications for export licenses. It approved all of these applications, except for 36, which were returned without action (either because the application was unnecessary or was deficient in some respect), and one that was denied. One-quarter of these applications authorized exports of technology outside the United States. One-quarter of these applications were for Encryption Licensing Arrangements. The remaining one-half of these applications were for licenses authorizing exports to a specific end user.<sup>17</sup>

BXA did not receive any applications requesting authorization for a service provider to offer cryptographic services to government end users. This requirement has been eliminated, which should represent a reduction in regulatory burden for suppliers of network infrastructure equipment and software.<sup>18</sup>

#### **POST-EXPORT REPORTING REQUIREMENT**

Industry had recommended a number of significant reductions in the post-export reporting requirements. Unfortunately, many of these recommendations have not been implemented. However, there are two important new relaxations of reporting requirements.

One important secondary benefit of implementing the Wassenaar changes of December 2000 is that exporters no longer have to report transfers of mass market software, regardless of cryptographic strength.

BIS has removed the requirement for post-export reporting of "community" source code (i.e., source code that is available to the public free of charge for non-commercial use but requires payment of fees for commercial use). Community source now is eligible for export on the same terms as "open" source.<sup>19</sup>

#### **OTHER CLARIFICATIONS**

There are several other clarifications to the export controls on cryptography that are worthy of note.

## PRODUCTS QUALIFYING AS "RETAIL"

BIS has clarified and expanded the list of products that qualify as retail encryption items. Please note that network infrastructure products are still not eligible for retail treatment.<sup>20</sup> The list of examples of retail items now includes the following:

1. Retail eligibility criteria. Retail encryption commodities and software are products and components:
  - A. Generally available to the public by means of any of the following:
    - (1) Are sold in tangible form through retail outlets independent of the manufacturer;
    - (2) Are specially designed for individual consumer use; or
    - (3) Are sold or will be sold in large volume, without restriction, through mail order transactions, electronic transactions, or telephone call transactions; and
  - B. Meeting all of the following:
    - (1) The user cannot easily change the cryptographic functionality;
    - (2) Substantial support is not required for installation and use; and
    - (3) The cryptographic functionality has not been modified or customized to customer specification.
2. Additional types of retail encryption products. The following products will also be considered to be retail encryption products:
  - A. Encryption commodities and software (including key management products) with key lengths not exceeding 64 bits for symmetric algorithms; 1024 bits for asymmetric key exchange algorithms; and 160 bits for elliptic curve algorithms. (You may immediately export or reexport such encryption commodities and software as retail items upon submitting a completed review request to BIS and the ENC Encryption Request Coordinator, in accordance with the requirements described in paragraph 2D of this section);
  - B. Encryption products and network-based applications that provide equivalent functionality to other mass-market or retail encryption commodities and software (refer to the Cryptography Note (Note 3) to part II of Category 5 of the CCL for the definition of mass-market encryption commodities and software);
  - C. Encryption products that are limited to allowing foreign-developed cryptographic products to operate with US products (*e.g.*, signing). No review of the foreign-developed cryptography is required;
  - D. Encryption commodities and software that activate or enable cryptographic functionality in retail encryption products that would otherwise remain disabled.
3. Examples of eligible retail encryption products: Subject to the retail eligibility criteria in paragraph (b)(3)(i) of this section, retail encryption items include, but are not limited to, the following:
  - A. General purpose operating systems that do not qualify as mass market;
  - B. Non-programmable encryption chips and chips that are constrained by design for retail products;
  - C. Retail networking products, such as low-end routers, firewalls, and virtual private networking (VPN) equipment designed for small office or home use;
  - D. Desktop applications (*e.g.*, email, browsers, games, word processing, database, financial applications, or utilities) that do not qualify as mass market;
  - E. Programmable database management systems and associated application servers;
  - F. Low-end servers and application-specific servers (including client-server applications, *e.g.*, Secure Socket Layer (SSL)-based Web applications and applets, servers, and portals);
  - G. Network and security management products designed for, bundled with, or pre-loaded on single CPU computers, low-end servers, or retail networking products; and
  - H. Short-range wireless components and software that do not qualify as mass market. Products that would be controlled under ECCN 5A002 or 5D002, only because they incorporate components or software that provide short-range wireless encryption functions, may be exported or reexported under the retail provisions of License Exception ENC without review or reporting.

The most important changes are to the treatment of certain networking products, the use of encryption for network management, and components for wireless encryption products.

### Certain Networking Products

Although network infrastructure products are not eligible for retail treatment, BIS has issued a clarification with respect to network equipment designed for "small office or home office use" that may qualify as retail. In the past, the government had used an informal three-part test, designating as retail items that had a line speed not exceeding 2.1 Mbps, encrypted throughput not exceeding 5 Mbps, or supporting no more than 100 concurrent encrypted tunnels.

Now, the line speed no longer is regarded as a limiting characteristic; the encrypted throughput has doubled to 10 Mbps; and the 100 concurrent tunnel limitation remains unchanged.<sup>21</sup>

#### Certain Network Management Products

BIS has added a new example of retail products, including those that provide network and security management for single CPU computers, low-end servers, and retail networking products. This would include, for example, an implementation of the Secure Shell protocol for network management.<sup>22</sup>

#### Short-Range Wireless Products

Short-range wireless products, such as encryption chips designed for retail wireless products with ranges typically not exceeding 100 meters, would qualify as retail. This category would include chips that implement the popular Bluetooth, HomeRF, and Wi-Fi standards.<sup>23</sup>

### PRODUCTS QUALIFYING AS MASS MARKET

Note that the definition of "mass market" is essentially identical to the definition of "retail eligibility criteria" set forth above. However, BIS intends that products qualifying as mass market will be a sub-set of those that qualify as "retail". Examples of mass-market products include the following:

- General purpose operating systems and desktop applications (*e.g.*, email, browsers, games, word processing, database, financial applications, or utilities) designed for, bundled with, or pre-loaded on single CPU computers, laptops, or hand-held devices;
- Commodities, software, and components for client Internet appliances and client wireless LAN devices; home use networking commodities and software (*e.g.*, personal firewalls, cable modems for personal computers, and consumer set top boxes);
- Portable or mobile civil telecommunications commodities and software (*e.g.*, personal data assistants (PDAs), radios, or cellular products); and
- Commodities and software exported via free or anonymous downloads.<sup>24</sup>

Note that the list of products that might qualify as mass market is a subset of those that might qualify as retail because the "equivalent functionality" test for retail does not have an equivalent under the mass market definition.

### PRODUCTS WITH "DORMANT" CRYPTO

For several years, Commodity Classifications have been issued confirming that products with "dormant" encryption are classified under ECCNs 5A992 and 5D992.

In the new encryption policy update, BIS has incorporated this informal policy into the regulations. Only the software or authorization code that "activates" the "dormant" encryption is controlled under 5A002 or 5D002.<sup>25</sup>

### FINANCE SPECIFIC PRODUCTS

In the past, some finance specific products have been given retail treatment, including products implementing highly formatted fields as specified in the Secure Electronic Transactions protocol, whereas other finance specific products, such as Automated Teller Machines, have been exempt from review. The new policy specifically exempts all encryption products that are "finance specific." Note, however, that this definition does not include products that may have end uses related to financial operations (*e.g.*, supply chain management) but that are not limited by design to financial transactions.

### SUMMARY

There are a number of areas where further reform of the encryption export controls is highly desirable, from industry's perspective. Real simplification is one example. Leveling the playing field between open source (open crypto APIs permitted) and proprietary source (open crypto APIs restricted) is another. Clarifying the gray area between network infrastructure products (excluded from retail) and small office/home office products (eligible for retail) is a third. However, further reform currently is not at the forefront of the George W. Bush administration's agenda. Industry will have to develop proposals that have market justification and do not unnecessarily impair the national security and foreign policy interests of the United States in order to achieve further reform of the encryption export controls.

### NOTES

1. 22 U.S.C. § 2778.
2. 22 C.F.R. 120, *et. seq.*
3. 50 U.S.C. App 2401-2411.
4. 15 C.F.R. 730, *et. seq.*
5. 67 Fed. Reg. (2002).
6. 56 Fed. Reg. 24824 (1991).
7. 57 Fed. Reg. 32148 (1993).
8. Executive Order 13026 of November 15, 1996; 61 Fed. Reg. 58767 (1996).
9. 65 Fed. Reg. 2492 (2000).
10. 65 Fed. Reg. 62600 (2000).
11. 67 Fed. Reg. (2002).
12. See <http://www.wired.com/news/politics/0,1283,46816,00.html>.
13. Senate EAA (S. 149) and House EAA (H.R. 2581).
14. Norman LaCroix at March 2002 RAFTAC.
15. 15 C.F.R. 740.17.

16. *Id.* at 740.17(b)(3)(iii)(H).

17. Norman LaCroix at Match 2002 RAPTAC.

18. *Id.*

19. 15 C.F.R. 740.13(e)(2).

20. *Id.* at 740.17(b)(2)(i).

21. 67 Fed. Reg. 38858.

22. 15 C.F.R. 740.17(b)(3)(G).

23. 67 Fed. Reg. 38856.

24. 15 C.F.R. 742.15(b)(5).

25. *Id.* at 742.15(b)(4).