#36

ICOTT INDUSTRY COALITION ON TECHNOLOGY TRANSFER
1400 L Street, N.W. Washington, D.C. 20005 Suite 800 (202) 371-5994

February 13, 1997

Ms. Nancy Crowe
Regulatory Policy Division
Bureau of Export Administration
Room 2705, U.S. Department of Commerce
14th Street & Pennsylvania Avenue, N.W.
Washington, D.C. 20230

2/13/97

Re: Encryption Items Transferred From the U.S. Munitions List to the Commerce Control List, 61 Fed. Reg. 68572 (Dec. 30, 1996)

Dear Ms. Crowe:

The Industry Coalition on Technology Transfer (ICOTT) is pleased to respond to the Department's invitation to comment on the new encryption regulations. ICOTT is a group of major trade associations (names listed below) whose thousands of individual member firms export controlled goods and technology from the United States. ICOTT's principal purposes are to advise U.S. Government officials of industry concerns about export controls, and to inform ICOTT's member trade associations (and in turn their member firms) about the U.S. Government's export control activities.

The regulations offer a two-year license exception (License Exception KMI) for the export of encryption products with key lengths of 56 bits or less to all except seven destinations.[1] Use of the exception, however, will be limited to firms that demonstrate a commitment to, and progress toward, the development of key recovery systems. Moreover, eligibility for this license exception will have to be renewed every six months. The regulations also transfer to the Commerce Control List all encryption items except those designed for military use.

The government's willingness to permit almost unrestricted exports of 56-bit encryption products demonstrates that such items no longer are of national security concern, are available abroad in substantial quantities, or are uncontrollable from a practical standpoint. Accordingly, ICOTT believes that limiting License Exception KMI to firms that assist the government on a separate project—the development of key recovery systems—is inappropriate. If an item does not need export controls, as plainly is the case with respect to 56-bit encryption technology, export controls should not be used to coerce industry cooperation on other fronts. We urge that the new regulations be amended to remove the requirement that engagement in the key recovery development effort is a prerequisite for the use of License Exception KMI.

---

1. These are Cuba, Iran, Iraq, Libya, North Korea, Sudan, and Syria.

There is growing evidence that 56-bit encryption can be overcome without undue expense, time, or difficulty. Experts indicate that 90-bit encryption is becoming the minimum standard for protection of sensitive commercial information. The government should consider whether to increase the 56-bit threshold accordingly.

As for the key recovery effort itself, ICOTT again expresses doubt that foreign governments or their citizens will embrace encryption products to which the United States government has access on demand. As Administration representatives candidly have acknowledged, no amount of bureaucratic pressure can overcome a market that votes with its pocketbook against key recovery products.

As for specific aspects of the regulations, ICOTT objects to the exclusion of "Encryption Items" (EI) from eligibility for the foreign availability, public availability, and de minimis exceptions to the Export Administration Regulations (EAR). If comparable products indeed can be shown to be available abroad without restrictions like those imposed by the United States, there is no justification for retaining United States controls on such items. The same is true for publicly available software. Further, as indicated in the recent *Bernstein* decision[2] and elsewhere, the imposition of controls on publicly available source code raises significant First Amendment issues.

ICOTT has been advised that where a particular encryption item is cleared by export by a particular exporter, other exporters seeking to export the identical item nevertheless will have to apply for and obtain their own clearances. ICOTT notes the inefficiency of this approach and asks that BXA consider whether—consistent with legal and policy considerations regarding confidentiality of business information—this multiplicity could be eliminated.

While ICOTT is pleased that 56-bit products will be eligible for sales after the two-year period has ended, we regret the restriction that "[t]he additional quantities sold may not be disproportionate to the customer's embedded base." If 56-bit technology is being permitted widespread export now, the case for restriction will be even less once two more years have passed. Manufacturers, exporters, and their customers need to plan ahead, and the use of six-month and two-year choke points makes if difficult to convince foreign customers of the reliability of United States suppliers. ICOTT also is pleased that United States firms will be permitted to service and support 56-bit items abroad after the two year period has ended.

---

2. *Bernstein v. U.S. Dep't of State*, No. C-95-0582 MHP (N.D. Cal. filed Dec. 9, 1996).

As an agency representative candidly conceded at a December 11, 1996 meeting with industry representatives, the two year goal for key recovery development is ambitious. ICOTT asks that the government be flexible about extending the deadline should bona fide development efforts not bear fruit by the end of 1998.

The regulations do not distinguish between software and hardware, focusing instead upon the encryption capability of items to be exported. This approach should be retained.

The regulations permit key recovery products to be made interoperable with non-key recovery products, so long as the interoperation does not prevent access to the encryption and decryption features of the key recovery product. The permission for interoperability is important to United States exporters and should be retained.

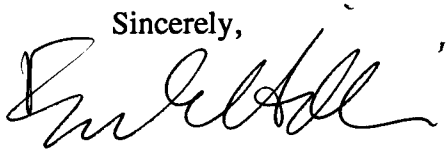
ICOTT is pleased that nonmilitary encryption items finally have been transferred to the Commerce Department but distressed at reports that license clearances may take longer there than at the Department of State. We urge BXA to give appropriate priority to processing encryption licenses and applications for License Exception KMI eligibility. Administration representatives indicated at the December 11 meeting that applications for encryption licenses under the new regulations would be subject to the general time limitations and appeal procedures for export licenses under Executive Order 12981. While the time periods in that executive order are unduly long, ICOTT prefers those limits to none at all and urges that the deadlines of Executive Order 12981 be complied with in the processing of encryption applications.

We understand that License Exception KMI is intended to be available for encryption products whose key lengths are less than *or equal to* fifty-six bits. By way of example, the Data Encryption Standard (DES) has a key length of fifty-six bits. New section 742.15(b)(3), however, refers to "encryption items *up to* 56-bit key length DES or equivalent" (emphasis added). The phrase "or including" should be inserted between "up to" and "56-bit".

Supplement 5 to part 742 requires key recovery agents to give BXA "prompt notice of a compromise of a security policy or of the confidentiality of key(s) or other escrowed information required to decrypt ciphertext." Lest this be construed to require reporting of *de minimis* breaches (e.g., door to security office inadvertently left unlocked on one occasion by last employee to leave for the day), a materiality threshold like that found in other reporting rules (e.g., §§ 748.6(f) and 764.2(g)(2)) should be included in the final regulations.

Sincerely,

Boyd J. McKelvain
Chairman



Eric L. Hirschhorn
Executive Secretary

ICOTT Members

American Electronics Association (AEA)
American Association of Exporters and Importers (AAEI)
Electronic Industries Association (EIA)
Semiconductor Equipment and Materials International (SEMI)
Semiconductor Industry Association (SIA)