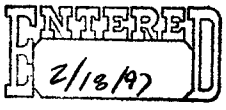
#33

DEWEY BALLANTINE

1775 PENNSYLVANIA AVENUE, N.W.
WASHINGTON, D.C. 20006-4605
TELEPHONE 202 862-1000 FACSIMILE 202 862-1093

February 14, 1997



W. CLARK MCFADDEN II
202 429-2333

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

Re: Semiconductor Industry Association Comments on Interim Rule, Encryption Items Transferred from the U.S. Munitions List to the Commerce Control List, Docket No. 960918265-6366-03

Dear Ms. Crowe:

The Semiconductor Industry Association ("SIA") welcomes this opportunity to comment on the Commerce Department's new encryption controls. SIA represents 30 U.S.-based semiconductor manufacturers who account for approximately 85% of U.S. semiconductor shipments.

SIA has an active interest in the encryption regulations because its member companies participate in a world economy that is increasingly dependent on globalized information systems and related networks. Without robust security, the development of the Global Information Infrastructure ("GII") will be seriously impeded.

I. SPECIFIC ISSUES RELATING TO THE INTERIM COMMERCE REGULATIONS

At a minimum, the interim encryption regulations deserve improvement in several areas.

A. License Processing Under the New Encryption Regime

The Administration should work to ensure that the Commerce-administered regime for encryption provides substantial improvements for exporters. For example, processing times under the Commerce regime should be significantly shorter than those that existed under the State Department regime. SIA is concerned that the licensing of encryption exports could be an even longer process with the transfer of jurisdiction to the Commerce

Department. The unbridled involvement of the Energy, Justice, State, and Defense Departments, and the Arms Control & Disarmament Agency in the process may add only unnecessary levels of review and cause unwarranted delays in licensing decisions. To prevent this outcome, SIA urges Commerce to quickly obtain delegations of authority from those agencies that do not have a significant interest in encryption exports.

The processing of applications for licenses to export encryption items should be straight-forward and timely under the new system. In practice, qualification for License Exception KMI should be similar to that for other license exceptions. The qualification for an exception should not be comparable to the process for obtaining a license.

B. Inapplicability of De Minimis Standard and Mandatory Foreign Availability Procedures

Under the interim rule, the encryption items transferred from the State Department's Munitions List ("ML") to the Commerce Department's Commerce Control List ("CCL") will not be afforded any protection by the Export Administration Regulations' ("EAR") de minimis standard[1/] or mandatory foreign availability procedures.[2/] Disallowance of the de minimis standard will cause confusion and impose costs far exceeding any benefits. It will conflict with the existing de minimis rule (which applies broadly to reexports of dual-use items) and will be difficult to manage.

The rationale for the de minimis standard -- that the presence of a slight amount of controlled content is inconsequential for the transaction as a whole -- applies equally to encryption. The denial of this fundamental protection to the transferred encryption items runs counter to the Export Administration Act ("EAA").[3/] Inevitably it will result in the

---

1/ See 61 Fed. Reg. 68578 (Dec. 30, 1996)(to be codified at 15 C.F.R. § 734.4(b)(2) & (h)).

2/ See id. at 68585 (to be codified at 15 C.F.R. § 768.1(b)).

3/ See 50 U.S.C.A. App. § 2404(a)(5)(A)([N]o authority or permission may be required under this section to reexport any goods or technology subject to the jurisdiction of the United States from any country when the goods or technology to be reexported are incorporated in another good and--
(i) the value of the **controlled** United States content of that other good is 25 percent or less of the total value of the good....(emphasis added).

same procedure that led to establishment of the de minimis standard in the first place -- creation of a major incentive for foreign manufacturers to "design-out" U.S. components.

Disallowance of mandatory foreign availability procedures similarly concerns SIA because, in addition to other features of the interim regulations, it conflicts with existing practice for virtually all dual-use goods subject to U.S. controls. The recent transfer in jurisdiction underscores that encryption should be treated as a dual-use item, not as a munition. As with the de minimis standard, the exclusion of these procedures is also inconsistent with the three-year effort to simplify the EAR.

C. Treatment of Components

The interim regulations are ambiguous with respect to their treatment of components with encryption capabilities. This ambiguity extends to both nonkey and key recovery encryption.

1. Nonkey Recovery Encryption With Key Lengths Up to and Including 56 Bits

In the context of recovery encryption up to and including 56 bits, the requirements on producers of semiconductors should be clarified in three important respects:

- First, the regulations should be amended to provide explicitly for the full eligibility of semiconductors for License Exception KMI;

- Second, the key recovery development plans submitted by semiconductor producers should be sufficient if they contain in a 1-2 page letter: (a) an explanation of the steps taken or to be taken to develop, produce, distribute, and market key recovery products and (b) benchmarks and milestones for incorporating key recovery features into products; and

- Third, renewal of License Exception KMI should be available by forwarding a letter to BXA every six months reporting on the chipmaker's good-faith efforts to meet milestones. Processing of renewal documentation should be expeditious.

2. Key Recovery Encryption

The operational features of encryption are generally determined by the nature of an overall system, not the individual components of the system. Therefore, in cases where encryption

functionality is tied to an integrated system, the applicant should be able to procure an appropriate end-use certification from a buyer in lieu of directly satisfying the requirements that are set forth in Supplement No. 5[4/] to Section 742 of the interim rule. Such a certification would contain an undertaking from a buyer that the device(s) would be utilized only in systems that permit access to the plaintext of encrypted information.

D. Inappropriate Distinction Between Encryption Software and Encryption Hardware

There is no compelling reason to impose more burdensome procedures on mass market encryption hardware than on mass market encryption software. Accordingly, the interim regulations should be modified to provide for the mass market treatment of encryption hardware that is comparable to that extended to encryption software under Sections 734.4(b)(2) & 742.15(b)(1) of the interim rule. Such treatment should include eligibility for the expedited procedures provided to software and the applicability of the de minimis standard.

E. Treatment of Encryption Exports to Reliable End-Users

SIA supports the Commerce Department's decision to recognize the validity of existing State Department encryption licenses. Under the previous regime which treated encryption items as a munition, the State Department was willing to approve exports of encryption products using the Data Encryption Standard ("DES") in cases where the proposed end-user was a bank or a subsidiary of a U.S. company. While not requiring regulatory codification, SIA understands that the Commerce Department will continue such practice. SIA supports the maintenance of this practice by the U.S. Government and recommends its extension to all legitimate commercial end-users that have demonstrated their reliability.

F. Definition of "Encryption Object Code"

The Commerce Department should confirm that the definition of "encryption object code" in Section 772 of the interim rule does not include software applications or systems software as referenced under that portion of Section 772 describing "encryption software." SIA believes that the rationale for such a distinction is compelling since application software should be treated differently than encryption object code.

4/ This supplement is titled "Key Escrow or Key Recovery Agent Criteria, Security Policies, and Key Escrow or Key Recovery Procedures."

G. Modernization of Controls on Low-Level Encryption Items

In addition to raising the ceiling for data encryption exports from 40 to 56 bits, the Commerce Department should also implement reform of controls on low-level encryption items. Such items are controlled under Export Control Classification Number ("ECCN") 5A995 and generally can be exported anywhere in the world except for terrorist-supporting or embargoed destinations.[5/] Data encryption generally does not fall within ECCN 5A995.

SIA proposes the extension of ECCN 5A995 to include data encryption items with key lengths that are no more than 40 bits (e.g., components for smart cards). Such items are already widely available overseas.

II. CONCLUSION

The recent jurisdictional transfer of encryption items demonstrates a recognition by the Administration that such items have predominant commercial uses. SIA believes that dual-use encryption should be accorded the full benefits provided to products controlled under Section 5 of the EAA, including the de minimis and foreign availability provisions. Further, the unique circumstances that surround semiconductors, as discussed herein, need to be taken into account in Commerce's encryption regulations. To the extent that SIA's proposed modifications are incorporated into the new controls, the capability of U.S. semiconductor producers to compete on a level playing field worldwide will be enhanced.

If you have any questions or comments about SIA's views on encryption, please contact me at (202) 429-2333.

Sincerely,

W. Clark McFadden II
Counsel to the Semiconductor
Industry Association

5/ Products within ECCN 5A995 include, among others, certain "personalized smart cards" and components therefor, mobile radiotelephones with link encryption, data authentication equipment, and cryptographic equipment designed for use in machines for bank or money transactions.