A STUDY OF THE INTERNATIONAL MARKET FOR COMPUTER SOFTWARE WITH ENCRYPTION

[NOTE: THIS IS A REDACTED COPY OF THE ORIGINAL SECRET DOCUMENT. BRACKETS [ ] ACCOMPANIED BY THE ORIGINAL CLASSIFICATIONS HAVE BEEN USED TO INDICATE LOCATION AND SIZE OF EXCISED CLASSIFIED TEXT]

Prepared by
the U.S. Department of Commerce and
the National Security Agency
for the
Interagency Working Group on
Encryption and Telecommunications Policy

TABLE OF CONTENTS

EXECUTIVE SUMMARY

BACKGROUND

- In late 1994, the President's National Security Advisor directed that an interagency report be prepared assessing the current and future international market for software products containing encryption and the impact of export controls on the U.S. software industry. The report was to include an assessment of the impact of U.S. encryption export controls on the international competitiveness of the U.S. computer software industry and a review of the types, quality, and market penetration of foreign-produced encryption software products. This paper presents the joint efforts of the Department of Commerce/Bureau of Export Administration and the National Security Agency to complete this tasking. (U)

EXPORT CONTROLS

- All countries that are major producers of commercial encryption products control exports of those products to some extent. Control methodologies and licensing practices vary, however, and a few countries, most notably France, Russia and Israel, also control imports and/or domestic use of encryption. There is a significant amount of international cooperation in controlling encryption exports. (U)

- Some European and other countries apparently treat exports to the United States of DES-based software more liberally than the United States treats DES exports to those countries. Some countries have stated that they generally restrict DES exports to financial end-uses. In general, no independent verification of these licensing practices was obtained. However, in some cases the U.S. was able to obtain DES products from them for non-financial end-uses. It is possible that some countries may allow these exports based on their political/economic/military relationship with the destination country (e.g., within the European Community, or former COCOM), for end uses that are considered legitimate commercial applications of the technology, or, in the case of exports to the United States, because DES is a national standard. (U)

- As the technology and the marketplace have evolved, the USG export control authorities have relaxed licensing constraints on cryptographic products several times over the past 10 years. These changes have usually been made after industry pressures and internal debate to balance national security and economic concerns. (U)

DOMESTIC AND INTERNATIONAL MARKETS

- While presently encryption software accounts for only a small percentage of the total software market (1-3%), according to numerous information security experts contacted in the course of the study, the future growth trend for this sector is expected to be great.

The market for encryption in distributed computation, databases, and electronic mail is beginning to expand exponentially as the U.S. and other countries develop and popularize electronic commerce, public networks, and distributed processing. (U)

- Encryption in these environments will often be implemented in software, as opposed to hardware, because it is generally less expensive and simpler to install and upgrade. Absent changes in government standards, for the next ten years, encryption software will primarily use DES and RSA-licensed encryption algorithms. Other non-standard and company proprietary algorithms will be used primarily for security-specific products for small niche markets. (U)

- Certain developments are promoting greater use by the general public of software-based network security features, including encryption, throughout the industrialized world. They include ever increasing use, fueled by well publicized "break-ins," of distributed databases, popular acceptance and usage of global networks, and the development and use of electronic commerce. (U)

- These developments are ongoing at one stage or another in practically all of the countries surveyed for this assessment. Less technologically advanced countries, where demand for encryption software is reportedly negligible, will soon undergo widespread development and computerization leading to increased demand for encryption software within the next 10 years. (U)

- The overwhelming majority (75%) of general-purpose software products (e.g., word processors, spread sheet programs, and database programs) available on foreign markets today are of U.S. origin. Commerce Department analyses indicate that the U.S. has few viable foreign competitors for such products, and of those general-purpose products with encryption features, all were found to be of U.S. origin. (U)

- In the security specific software market, however, U.S. manufacturers face competition in several foreign markets from such encryption exporting countries as the United Kingdom, Germany, and Israel. To a large extent, markets for these products tend to be "national." Not only do export controls affect sales, but local vendors of security-specific products are at a competitive advantage in that they are better situated to work closely with end-users and develop encryption solutions tailored to meet the conditions of the local environment. (U)

- NSA confirmed the existence of a significant number of foreign security-specific software products with encryption features, predominantly from Western European suppliers. Security-specific products are usually not available on the shelf at retail stores either in the U.S. or abroad, but can be purchased through direct contact with the manufacturer. (U)

- BXA attempted to quantify U.S. competitiveness and market share in 31 foreign countries where encryption is thought to have significant demand. While sources in the countries surveyed had limited access to import statistics or market literature on encryption software and encountered numerous difficulties in evaluating this complex market, definite conclusions may be drawn from the responses. (U)

    - Sources in 14 countries indicated that U.S. export controls limit U.S. market share in their countries. Sources in seven countries indicated that export controls have either no impact or no major impact. (U)

    - Sources in most countries indicated that the U.S. market share is keeping pace with overall demand despite the impact of U.S. export controls, which may promote indigenous production or reduce U.S. market penetration. In all known cases, the U.S. holds the majority of the general-purpose encryption software market. (U)

    - Three exceptions are Switzerland (where the U.S. market share reportedly declined in 1994, while the market shares of other European countries rose), Denmark, and the United Kingdom, which reported unspecified declines from previous years. Sources in all three countries attribute the decline to U.S. export controls, which they claim promote the development and sale of indigenous encryption products. (U)

    - In many countries surveyed, exportable U.S. encryption products are perceived to be of unsatisfactory quality. (U)

ANALYSIS OF FOREIGN PRODUCTS

- NSA used various methods to procure encryption software products from a variety of countries and companies, as reflected in the TIS database and other sources. Altogether, 28 products from 22 foreign producers in 10 countries were acquired for the purposes of this study. Of these, 21 purportedly use the DES algorithm, while the remaining 7 use proprietary algorithms. (U)

- [

] (S)

ECONOMIC IMPACT

- In the absence of significant foreign competition, the impact of U.S. export controls on the international market shares of general-purpose products is probably negligible. Customers are often unaware of the encryption features in these products and primarily base purchases on the features implementing the primary function of the product (e.g., word processing or database). (U)

- [

] (S)

- BXA attempted to quantify the economic impact of export controls on the U.S. software industry by forwarding a detailed voluntary questionnaire to 206 software vendors and other interested parties. Thirty six encryption software manufacturers provided completed surveys out of the 71 returned. By and large, the companies were unable or unwilling to quantify the costs of export controls, but did provide substantive explanations of how and why they believe they are adversely affected. (U)

    - Some general-purpose software companies claim that export controls have affected their plans to expand security features to meet anticipated growing demand. These companies believe that they could expand their domestic and international customer base with such features. (U)

    - The export licensing process itself is not a major obstacle to U.S. competitiveness. Only seven survey respondents use the Department of State licensing system. While they continue to have some complaints about the administrative burdens and time delays associated with State's process, several noted that there had been improvements in recent years. Only two of the survey respondents had been denied licenses by the Department of State. (U)

    - Numerous survey respondents indicated that they avoided applying for export licenses from the Department of State altogether. Some larger companies whose products tended to be general-purpose in nature either developed two versions of software, or incorporated an encryption algorithm they knew would qualify for Commerce general licenses. (U)

    - Many smaller, security-specific software firms, on the other hand, elected to limit their sales to the domestic market only. These companies indicated a high level of foreign interest in purchasing their products, and therefore lost potential sales. While it is difficult for them to quantify their potential market, they believe it to be sizeable. They claim their small size limited their ability to develop two versions of their products, and the fact that their products were for security purposes

specifically requires them to incorporate strong encryption. Only one company was able to provide specific examples where a foreign competitor obtained a sale due to an export license denied by U.S. authorities. (U)

- There is little evidence that U.S. export controls have had a negative effect on the availability of products in the U.S. marketplace. A broad range of products with secure algorithms exist in the U.S. market and availability of products is based principally on the level of customer demand. Export controls may have hindered incorporation of strong encryption algorithms in some domestic mass-market, general-purpose products, since some companies find developing and maintaining two versions of a product infeasible. (U)

- The existence of foreign products with labels indicating DES or other strong encryption algorithms, even if they are less secure than claimed, can nonetheless have a negative effect on U.S. competitiveness. Most encryption users base their purchasing decisions on the advertised product features, along with price, company reputation, etc. (U)

I. INTRODUCTION

BACKGROUND

Cryptography, once almost exclusively the domain of governments striving to maintain national security, has increasingly developed applications in the private sector.[1] This increase in demand can be traced to the proliferation of personal computers and global expansion in information exchange and electronic commerce, fueled by numerous accounts of computer hackers successfully invading government and commercial networks and concerns about industrial espionage. The use of encryption in some sectors, such as the banking industry, is now well developed, while in other areas it is nascent but expected to increase exponentially. (U)

U.S. software manufacturers assert that U.S. export control policy, as it applies to software products containing encryption, unfairly puts U.S. firms at a disadvantage in foreign markets. Chief among the industry's complaints is its allegation that software products providing strong encryption are widely available overseas from foreign vendors, while export controls prevent U.S. firms from selling equivalent products in the same markets. Industry also claims that the software export controls are ineffective and unenforceable, and that strong encryption algorithms can be easily downloaded by anyone with access to the Internet. Industry representatives have estimated that the current export control policy has resulted in billions of dollars annually in lost sales to U.S. firms subject to munition controls, and that future losses will be even greater as the demand for encryption is predicted to increase dramatically over the next five to ten years. (U)

In response to industry concerns and Congressional interest in this issue, in late 1994, the President's National Security Advisor directed that an interagency report be prepared assessing the current and future international market for software products containing encryption and the impact of export controls on the U.S. software industry. Specifically, Presidential Review Directive (PRD)/NSC-48 directed that the study be completed by July 1, 1995 and include:

- an assessment of the current and future international market for computer software with encryption;
- an assessment of the impact of U.S. encryption export controls on the international competitiveness of the U.S. computer software industry;
- an assessment of the economic consequences of U.S. encryption export controls, including their impact on exports and jobs in the U.S. computer software industry;

[1] A glossary of terms related to encryption used throughout this paper is included as Appendix A.

- a review of the types, quality, and market penetration of foreign-produced encryption software products; and

- a review of any controls that influence the international marketability of encryption software products. (U)

This paper presents the joint efforts of the Department of Commerce/Bureau of Export Administration and the National Security Agency to complete this tasking. The Department of Commerce was responsible for assessing current and future markets for encryption products and determining the impact of the controls on the U.S. industry, while the National Security Agency took the lead on the review of foreign encryption products and controls influencing the marketability of software products. A wide variety of government agencies, academic experts, commercial information sources, trade associations, and industry representatives were contacted in order to evaluate these issues. (U)

METHODOLOGY

To determine the extent to which regulatory controls influence the international marketability of encryption software products, the National Security Agency (NSA) and Bureau of Export Administration (BXA) reviewed U.S. and foreign export licensing regulations, practices and procedures, as well as domestic and international policies regulating the usage and importation of products containing encryption. Wherever possible, copies of relevant laws and regulations were obtained and in many cases face-to-face meetings were held with officials of foreign governments to discuss their policies and practices. In addition, information was collected from the Central Intelligence Agency (CIA), State Department, and non-government sources. This information is presented in Chapter II of this report. (U)

To assess the current and future international market for computer software with encryption as called for by the PRD, BXA asked U.S. embassies in 31 countries, where encryption software products are developed and sold, to determine the size of the encryption markets in their host countries and the estimated U.S. share of these markets. Embassy personnel queried encryption specialists, U.S. and foreign encryption producers and users, and government authorities in each of their respective countries. While in most instances, embassy officials were unable to determine exact figures, their efforts nonetheless resulted in rough estimates of the current market size, growth potential, and relative market shares in these countries. (U)

Similarly, no definitive statistics exist regarding the size and composition of the U.S. market for encryption software. BXA consulted with a number of computer security specialists in the private sector and academia, and utilized information amassed by market research firms to create a picture of the current and future domestic market for these products. We supplemented this information with an informal poll of information security professionals from ten diverse Fortune 500 companies to determine how these firms are currently using encryption software and

their plans for the future. The results of these market assessments are presented in Chapter III. (U)

Chapter IV presents information on types and quality of foreign software products with encryption. An extensive listing of 44 foreign encryption software producers compiled for the Software Publishers Association by Trusted Information Systems, Inc. (TIS) was used as a starting point for this review. NSA attempted to identify and confirm the existence of as many foreign software confidentiality products as possible.[2] This was accomplished by:

- Contacting the manufacturer or point of contact listed in the TIS database;
- Gathering brochures and product information at trade shows;
- Conducting an extensive search of software industry trade literature for references to products and manufacturers, and requesting USG representatives overseas to contact manufacturers for product information;
- USG representatives overseas searching local information sources such as telephone books for product vendors. Representatives also visited 50 foreign computer and software retailers and contacted an additional 25 by phone to inquire about the availability of software products with encryption in retail trade, and in some cases to purchase products;
- Contacting various foreign government agencies abroad and requesting they supply information about their domestic encryption products, and in some cases, copies of those products, and;
- Contracting with TIS to purchase foreign products. (U)

Overall 28 foreign encryption products were obtained by U.S. Government (USG) representatives overseas, Trusted Information Systems, or from foreign governments. Since it is impossible to judge the quality of these products based on their packaging, they were studied individually by NSA cryptanalysts to evaluate the strengths and weaknesses of their security features. The analyses of the security of these products are classified. (U)

In order to determine the impact of existing export controls on U.S. encryption software vendors, BXA developed an industry questionnaire (attached in Appendix C). The questionnaire was developed working closely with the Software Publishers Association, the Business Software Alliance, and other industry groups, and was distributed in mid-March, 1995 to approximately 206 encryption software vendors. The questionnaire mailing list was developed using association

---

[2] Products using encryption solely for non-confidentiality purposes (e.g., access control or authentication) were not included in this study as they are usually available under a Commerce General License. (U)

membership directories, listings in trade periodicals and directories, references in encryption-related press articles, and TIS's database of encryption producers (which included domestic as well as foreign vendors). The survey was also posted on the Internet in several locations. An additional 50 or so questionnaires were distributed to interested parties, including lawyers representing encryption software vendors, encryption hardware producers, and consultants. (U)

Completion of the survey, for which BXA received approval for distribution under the Paperwork Reduction Act, was voluntary. Thirty-six companies elected to respond. The majority of survey respondents were small firms producing specialized security software, rather than general-purpose software with an encryption element. By and large, the companies were unable to quantify the costs of export controls, but did provide useful qualitative explanations of how and why they believe they are adversely affected. A discussion of the ways in which U.S. software vendors are affected by these controls is presented in Chapter V. (U)

II. DOMESTIC AND INTERNATIONAL LAWS, REGULATIONS, AND POLICIES AFFECTING ENCRYPTION

UNITED STATES

Since one of the main purposes of this report is to determine the extent to which U.S. export controls affect the competitiveness of the software industry, it is first useful to review current and historical U.S. laws and policies that set the stage for the encryption industry. U.S. Government (USG) policies are also an important determinant of other governments' policies concerning commercial encryption markets. (U)

Import

The United States does not require a license for the import of cryptographic equipment or software. (U)

Domestic Use

The United States has no laws regulating the private use of encryption. The Arms Export Control Act however does require manufacturers of such products to register with the Department of State. The National Institute of Standards and Technology (NIST), by means of Federal Information Processing Standard 185, encourages government and private use of encryption products which incorporate a means for decryption by law enforcement under the appropriate lawful authority. (U)

Export

The United States regulates the export of certain hardware and software encryption products in order to protect national security interests. Two principal laws govern the imposition of export regulations pertaining to cryptographic products, the Arms Export Control Act (AECA) and the Export Administration Act (EAA). The AECA is the source of authority for the International Traffic in Arms Regulations and the EAA is the source of authority for the Export Administration Regulations. The control lists for cryptographic products included in these regulations parallel lists maintained by the U.S. and many Western allies in the New Forum, successor to the Coordinating Committee for Multilateral Strategic Export Controls (COCOM). (U)

The International Traffic in Arms Regulations (ITAR) are administered by the Department of State. The ITAR govern export licensing of most cryptographic products providing encryption for data confidentiality purposes. Under the ITAR, the Department of State requires licensing of exports of cryptographic hardware and software to any country other than Canada. License applications are referred to the Department of Defense (specifically the National Security Agency)

for an evaluation of the national security implications of the proposed export. In many cases, however, NSA and the Department of Defense have agreed that State may license specified encryption equipment without referral. Although the Department of State generally abides by the recommendation of NSA on specific export applications, State has final authority on all export decisions. (U)

The Export Administration Regulations (EAR), administered by the Department of Commerce, govern exports of cryptographic products providing encryption generally limited to purposes of data authentication, password protection, access control, and the like. Such products may be exported under a General License (with certain foreign policy exceptions), which requires no submission of paperwork by the exporter. Equipment providing confidentiality falls under EAR licensing if it is restricted to financial end-uses, e.g. automatic teller machines and point-of-sale terminals. In addition, other confidentiality products, including mass-market software products with encryption, may be transferred to Commerce licensing jurisdiction following a one-time review under Department of State auspices. Licenses for cryptographic products under the jurisdiction of Commerce, except in rare instances, are not referred to the Department of Defense for review. (U)

Special licensing procedures are in effect for some mass-market software products providing confidentiality. Mass-market software products implementing a particular encryption algorithm (RC2 or RC4) with a key length no more than 40-bits are transferred from the Department of State to the Department of Commerce licensing jurisdiction after a one-time review to ensure that the algorithm is implemented properly. Mass-market software products incorporating other algorithms may also be transferred to Commerce jurisdiction after a one-time review. Under the EAR, all mass-market software products, including those with encryption, as well as password, access control and authentication products containing encryption, are specifically exempt from control. Thus, once a mass-market product is transferred from State to Commerce jurisdiction, it may be freely exported under general licensing provisions. (U)

Policy

Within the United States Government, the National Security Agency has been primarily responsible for the development of export policy for encryption technologies. The objectives and policies developed by NSA in this regard are to a large degree consistent with those of most Western European nations due to international cooperation discussed later in this chapter. [

] (S)

In the early 1950's the United States and its major allies recognized the strategic importance of encryption and agreed through COCOM to control exports of all cryptography, regardless of function. At that time there was no significant business or private use of

cryptography; cryptographic equipment was primarily designed for and sold to government and military end-users. (U)

Since that time, and especially in the last decade, encryption technology and commercial applications for it have evolved. In the early 70s, the banking and financial communities recognized the importance of encryption to protect fund transfers. Applications for encryption also emerged in the industrial sphere. USG export control authorities have attempted to balance national security and economic concerns. Export licensing restrictions and procedures have been relaxed on several occasions in recent years in response to industry concerns and after interagency debate. Table 2.1 describes the major liberalizations in this area. (U)

Table 2.1 Changes in Export Policy (U)

YEAR	CHANGE
< 1983	All cryptography exports require individual State licenses
1983	Distribution licenses established allowing exports to multiple users under a single license
1987	Most non-confidentiality products moved to Commerce on case-by-case basis
1990	ITAR amended - all non-confidentiality products under Commerce jurisdiction
1990	Mass-market general-purpose software with encryption for confidentiality moved to Commerce on case-by-case basis
1992	SPA agreement providing for 40-bit RC4/2 based products under Commerce jurisdiction
1993	Mass-market hardware products moved to Commerce on case-by-case basis
1994	Reforms to expedite license processing at State; NSA person detailed to State

Until 1983, each export of cryptographic hardware and software required an individual validated license from the Department of State. In 1983, NSA and State responded to U.S. industry concerns by allowing industry the option of using distribution licenses to export cryptographic equipment to non-government end-users through foreign distributors. The use of distribution licenses, not then available for other commodities under State jurisdiction, delegated authority to the U.S. companies to issue individual licenses through their foreign distributors, thus obviating the need to apply to State for each export license and saving both time and money. (U)

In 1987 NSA, again in response to industry concerns, began a review to determine the effects on national security of relaxing the requirement for individual licensing for cryptographic

products whose function is limited to password encryption, access control and authentication. Industry argued that access control and authentication functions were, by far, the most important security features required in their products since such features prevent network and data from exploitation by hackers. This requirement was also emphasized by encryption users, most notably in the financial community, who noted their primary uses of encryption were to protect data from alteration and to authenticate users. Their concern was not that an unauthorized person could view a transaction but that such person could alter the data or masquerade as an authorized user. Government users also supported this thesis; their concerns were unauthorized access to information at rest in government databases as well as hackers interfering with the national communications infrastructure. These problems could be obviated by the use of strong access control mechanisms. (U)

The results of that study showed that these functions were becoming increasingly available in commercial products, especially software, such that continued licensing requirements on exports could disadvantage U.S. industry by causing an economic loss in U.S. exports. Weighing competing concerns of national security and industry, NSA's decision was to recommend decontrol of this class of security products. Ultimately in 1990, the Department of State amended the ITAR such that original jurisdiction for this category of encryption was moved to the Department of Commerce. (U)

[

] (C)

In 1990, the Department of State amended the ITAR to specifically address, for the first time, mass-market software containing encryption. Recognizing the need for streamlined licensing of such products and to maintain U.S. dominance of the worldwide software market, the Government recommended that "software packages designed to run on microcomputers, employing nonstandard cryptographic algorithms, not of strategic value and for which encryption is not the primary function of the package" could be moved on a case-by-case basis to Commerce jurisdiction. Within a short time, products were moved to Commerce jurisdiction, where licensing to most destinations was authorized without referral to the Department of Defense. (U)

In 1991, the Software Publishers Association (SPA) voiced concern about the time required for NSA to review mass-market software products using "non-standard cryptographic algorithms not of strategic value", especially in view of COCOM's recent agreement to exempt such software from control. Industry asked that a "standardized cryptographic algorithm not of strategic value" be specified such that vendors could build to this standard and be guaranteed export licensing relief. The SPA and NSA then negotiated an agreement which permits the license-free export of software containing encryption, using the RC2 or RC4 encryption

algorithms implemented with key lengths up to 40 bits. This liberalized treatment ensures transfer of licensing jurisdiction, after a one-time review by NSA, to the Department of Commerce, where the products are freely exportable. The one-time review by NSA is to verify that the product correctly implements the algorithm, and is to take a maximum of seven days. In addition, developers choosing to implement algorithms other than RC2/RC4 were accorded commodity jurisdiction review not to exceed fifteen days. Since this change, the overwhelming majority of commodity jurisdictions submitted for mass-market encryption products have been approved for Commerce jurisdiction. Of the 103 commodity jurisdictions requests for products submitted in 1994, 90 were transferred to Commerce jurisdiction. [

] Nevertheless, some in the software and computer security businesses worry that the 40-bit key length restriction is too short to provide reliable defense against the brute-force decryption assaults that advances in processor technology will yield in the near future. (PROPIN)

Since 1993, there have been several other minor liberalizations in encryption export control policies. For example, at NSA's behest, State transferred a number of cellular handsets with embedded cryptography to Commerce jurisdiction. Also, products specially designed for Electronic Data Interchange or electronic commerce applications (often using DES) have been transferred to Commerce jurisdiction. Additionally, a number of decryption-only products primarily used for software distribution and various decoder products intended for television entertainment purposes have been transferred to Commerce jurisdiction. (U)

In 1994, the Administration announced a number of new reforms to facilitate export licensing of cryptographic products. These reforms include: a new distribution arrangement, a personal use exemption, and an expedited license processing goal. Through a distribution arrangement, vendors can now distribute encryption products directly from the U.S. to foreign customers, without using a foreign distributor and without prior State Department approval for each export. This reform especially benefits the small companies which cannot afford a foreign distributor. The personal use exemption, once implemented, will allow U.S. citizens or U.S. companies to export temporarily, without prior approval, encryption products when intended for their own personal use. (Currently, every businessperson who travels abroad with a notebook computer equipped with Lotus Notes software or a secure telephone is theoretically in violation of the Arms Export Control Act unless they have a Department of State license.) Finally, the Administration announced a State Department goal to process export licenses for cryptographic products within two days. In order to meet this goal, an NSA employee is now integrated at the Department of State's Office of Defense Trade Controls (ODTC), an action which has resulted in a significantly faster response to vendors on their export license requests. NSA plans to place a second person at ODTC in 1995 to further speed license processing. (U)

[

] (FOUO)

Figure 2.1 Licensing Processing Times in Calendar Days (FOUO)

While the U.S. software industry by and large welcomed the liberalizations and procedural changes of the past several years, many assert that the USG has not done enough to remove controls that are unduly burdensome and costly to U.S. firms and prevent U.S. businesses from securing communications with overseas customers, suppliers, and partners. They claim that U.S. export control policy has not kept pace with increasing domestic and international demand for data confidentiality products incorporating strong encryption capabilities, such as DES or RSA. (U)

[

]

(FOUO)

[

]

(FOUO)

Figure 2.2 ITAR Permanent License Applications for Confidentiality Products (FOUO)

[

] (FOUO)

In addition, export policy takes into account both national and international standards. A prime example involves the exportability of products compliant with the European Global System for Mobile Communications (GSM) cellular standard. U.S. firms are able to compete and receive license approval to export GSM systems to foreign GSM customers, where, importantly, many European firms also compete. This policy attempts to ensure that U.S. firms are on a level

[

]

(FOUO)

Figure 2.2 ITAR Permanent License Applications for Confidentiality Products (FOUO)

[

] (FOUO)

In addition, export policy takes into account both national and international standards. A prime example involves the exportability of products compliant with the European Global System for Mobile Communications (GSM) cellular standard. U.S. firms are able to compete and receive license approval to export GSM systems to foreign GSM customers, where, importantly, many European firms also compete. This policy attempts to ensure that U.S. firms are on a level

[

] (C)

Until 1989, the COCOM controls for cryptography remained relatively straightforward: all cryptographic products were controlled regardless of function, including password protection, authentication, and confidentiality. After that, the increasing commercial demand for products incorporating encryption led to a proposal that products used exclusively for password encryption or for authentication no longer require full COCOM approval but may be authorized for export at the national level, including those using DES. This proposal was accepted and subsequently implemented in 1991, [

] These functions are now exported from the U.S. under General License, as discussed in the previous section. (C)

In 1991, during its rewrite of the Industrial List, COCOM expanded the decontrols on mass-market software by adopting the General Software Note (GSN) which effectively decontrolled all mass-market software regardless of function. Some governments, including the U.S., France and Australia, agreed to the GSN but continued to control exports of mass-market encryption products having confidentiality. (U)

[

] (C)

[

] (C)

National Laws and Regulations

In order to present as complete and accurate a picture as possible of the international export control situation, NSA and Commerce attempted to obtain and analyze copies of the laws and regulations from as many encryption-producing nations as possible during the time allotted. Several nations' laws and regulations have been received to date and are described below. In

addition, a number of other countries, including some former COCOM members, are known to have controls, but their laws and regulations have not been analyzed. (U)

To obtain the information in this section, a variety of sources was consulted. A study dated January 1994 by Professor James Chandler, then of George Washington University, as well as the CIA's Office of Scientific and Weapons Research (OSWR) report on foreign laws and policies provided excellent references for this paper. In addition, a series of State Department cables in 1993-1994 provided pertinent information on foreign laws and policies. Finally, the Department of Commerce/BXA attempted to supplement this information for those countries that are believed to be producers of encryption software via a request to the Foreign Commercial Service representative in each country. (U)

The most valuable input to this report came from personal interviews with representatives of the various ministries and departments of foreign governments involved in the export control of encryption equipment. These interviews allowed us to probe actual government policies and practices in this area. In most cases we found that either the intelligence agencies or the information security agencies determine whether exports of these products are approved or denied, although in many cases these agencies had little expertise on the intricacies of the licensing process. Discussions with officials of foreign or trade ministries, alone, often proved disappointing as they were not fully aware of the policies of their intelligence or defense agencies in this arena. Also of use in determining how foreign governments implement their export control regulations regarding encryption were our experiences in attempting to obtain various foreign products for analysis -- whether licenses were required, denied, or granted for export to the United States. (U)

Although this report documents existing national laws and regulations of some European countries, national laws for European Union (EU) members may be superseded to some extent by EU regulations which were adopted on July 1, 1995. Therefore, EU regulations in this area also were examined. (U)

[

] (C)

Encryption software products were obtained from ten countries, including products purportedly incorporating the DES algorithm from seven countries: Denmark, Germany, Israel, Japan, New Zealand, South Africa, and the United Kingdom. In some cases, foreign export licenses may have been required. In other cases, export licenses may not have been required, or products may have been illegally exported. In any event, the fact that purportedly DES products were purchased indicates that such products can be obtained for end-uses other than financial. It may be that some licensing decisions were made based on the fact that the exports were for the United States, where DES is a federal standard (although no country stated that this was their policy). It may also indicate that licensing policies of some other encryption producing countries are more lenient than that of the United States and are not limited to financial applications. (U)

In addition to export controls, some of these nations have adopted or have pending legislation regulating the import and/or domestic use of cryptography. (U)

All nations surveyed, including the U.S., have homologation laws which regulate the connection to and use of communications equipment on their national telecommunications networks. Often U.S. businesses cite import or domestic use restrictions on cryptography for denial of encryption use in foreign countries, whereas in many cases the use may in fact be denied because the equipment has not been certified to interface to the national network. However, there have been unconfirmed reports that several governments do in fact use homologation laws as a pretext to restrict the use of cryptography on their telecommunications networks, and in bilateral consultations one government implied its use of this practice. (U)

Detailed discussions of each of the countries for which information was obtained are provided below:

Australia

Export

Australian legislation controlling the export of cryptographic products has existed since at least 1987 when Australia became a member of COCOM. However, unlike COCOM controls, Australian regulations include all cryptographic products under a separate category rather than distinguish them as either dual-use or military. These products require Ministry of Defence approval for export under Regulation 13B and the associated Schedule 13 of the Customs (Prohibited Exports) Regulations. As such, Australian control regulations exceeded the COCOM guidelines in some areas, most notably in requiring individual export licensing for mass-market applications software and other mass-market software performing cryptographic functions. (U)

[

]

[

] (C)

[[1]

] (S)

Import

There are no import controls on cryptographic products. (U)

Domestic Use

At present, private use of encryption devices in Australia is limited only by the requirement to obtain Public Switch Telephone Network regulator Austel's approval for any equipment to be attached to the network. Approval is generally granted provided the equipment does not harm the network. Australia does not appear to use homologation laws to control private use of encryption. (U)

[

[2]] (S)

---

[1] State: Canberra 03283-93. (S)

[2] State: Canberra 04846-94. (S)

Austria[3]

Export

The Austrian Government controls all encryption software as a dual-use item, and special licenses are required for its export, transit, or re-export. The legislation governing dual-use items is the Aussenhandelsgesetz 1995 Bundesgesetzblatt 172, as well as the accompanying Bundesgesetzblatt 180/1995. Licenses are denied to destinations where an armed conflict is ongoing, to countries of concern, and to those countries against which there are international sanctions. (U)

Canada

Export

The Export and Import Permits Act (EIPA), the Export Control List (ECL) and the Area Control List (ACL) are the mechanisms by which Canada controls exports. The EIPA authorizes the Government to exercise export controls to ensure that military or strategic goods are not exported to destinations representing a strategic threat to Canada. Implementation of the Act is the responsibility of the Ministry of Foreign Affairs. (U)

[

] (S)

[

] (C)

[3] Commerce: Vienna 004611, June 7, 1995. (U)

The Canadian Government is concluding an analysis of the worldwide availability of encryption products, and the export controls governing their shipment. The information is to be used to determine if Canadian export policy toward encryption should be liberalized. (U)

Import

Canada does not require import licenses for cryptographic products although the COCOM IC/DV procedures are supported. (U)

Domestic Use

Canada has no statute regulating private use of cryptography. Like most nations, Canada does have homologation regulations which control and validate equipment attached to the public network. Cryptographic equipment must conform to these regulations. (U)

[

] (C)

Denmark

Export

Denmark controls the export and re-export of encryption software pursuant to international agreements and de facto existing COCOM regulations. There is no evidence as to whether Denmark adheres to the COCOM exemption for mass-market software. A validated license is required for exports. So far none have been denied. Denmark does not differentiate between encryption algorithms. The same regulations apply for DES as for other algorithms.[4] (U)

Denmark presently regulates the export of strategic goods under a Ministry of Industry executive order dated 12 November 1993. The central element in the executive order is the list of strategic goods that are subject to export control policy and may be exported only when the Business Policy Ministry has issued a license. This list originally included only products that were under embargo due to Danish cooperation in COCOM, however, it is now composed of products from four international control systems which Denmark supports. These are the New Forum Group, the Missile Technology Control Regime, the Nuclear Nonproliferation Treaty, and the Australia Group. The executive order, however, is to be abolished now that the EU regulation

[4] Copenhagen 2717, 31 May 1995. (U)

has come into effect on 1 July 1995, and the main legal basis for export controls will be the EU regulation. (U)

[

] (C)

In response to a Commerce questionnaire,[5] an official from the Confederation of Danish Industry Board stated that individual validated licenses are required for the export of cryptographic equipment and software. The official noted that no such licenses have been denied. (U)

Import

Denmark does not control the import of encryption software. (U)

Domestic Use

[

]

(S)

European Union

Export

In 1992, the European Commission proposed a dual-use regulation as part of the progression to a Free Market. However, problems immediately arose as to whether this was a matter of national or Commission competence. Since military exports were clearly linked to member states' essential security interests connected with the production of, or trade in, arms, munitions and war materials, control of such exports was deemed to be a matter for individual

[5] Commerce: Copenhagen 2717, 31 May 1995. (U)

states. With dual-use goods it could be argued that their military potential was a national interest, whereas their civil potential was a Commission one. (U)

Inevitably, the final outcome was a compromise. A procedure was devised to reflect the split competence between member states and the Commission; there would be a Dual-Use Regulation , the legal basis for which is Article 113 of the Treaty of Rome, and a Maastricht-based Common Foreign and Security Policy Joint Action with a series of Annexes. As it now stands, the Dual-Use Regulation (EC No. 3381/94) contains 24 Articles and entered into force on 1 July 1995. It has appended to it Council Decision No. 94/942/CFSP which is comprised of 8 Articles and 5 Annexes. (U)

The overall effect of the regulation is broadly that:

a. all member states recognize the same list of dual-use goods (generally based on the COCOM list), destinations and guidelines;
b. the majority of dual-use goods may require, at most, only a general authorization for shipment between member states (and for favored destinations outside the community - Australia, Canada, Japan, Norway, Switzerland and the United States);
c. a common level of export control should exist throughout the community;
d. an export license issued in one member state shall normally be valid for the shipment of goods from another member state. (U)

Most cryptographic equipment is excluded from the provisions of the Regulation for an "interim period" likely to be at least three years, based on their inclusion in Annex IV. During this interim period, most cryptography equipment (except for that decontrolled by COCOM) will still require individual licensing between member states as well as all other destinations. With the expiration of the interim period, the requirement for licensing of cryptographic equipment will remain for all destinations outside the member states and the favored destinations. (U)

[

] (S)

Finland

Export

Finland controls encryption software as a dual-use item requiring an individual validated license. The governing legislation is the Foreign Trade and Economic Growth of Finland, Treaty Series 506/92, Amendment 731/93 and 331/94. (U)

U.S. embassy sources indicate that export and import regulations on encryption software are not rigorously enforced in Finland.[6] (U)

Import

An individual validated license is required to import encryption software. (U)

Domestic Use

Finland regulates the domestic use of cryptography. (U)

France

Export

It has often been stated, and is certainly true, that France has the most comprehensive cryptologic control and use regime in Europe, and possibly worldwide. Although French law on the export of cryptographic devices has existed in some form for over 40 years, until 1990 it was based principally on the export control regimes imposed by COCOM, of which France is a member. On December 29, 1990, a new law (90-1170) was enacted regulating the telecommunications industry. Article 28 of this law specifically addresses encryption and adopts a control and export regime far more restrictive than that applied by COCOM. The new French law, in order to "preserve the interests of national defense and of internal or external State security," regulates the "supply, export, or use of cryptologic methods or devices." Thus, although foreign cryptologic products may be imported into France without a license, they may not be supplied to French users nor used in France without authorization by the Prime Minister. (U)

The French law separates cryptographic equipment into two categories based upon the Decree 92-1358 of December 28, 1992, a follow-on to the earlier decree. The first category, equipment which "can have no other purpose than authenticating a communication or ensuring the integrity of a transmitted message," requires the submission of a statement or declaration to the Central Service for Information Systems Security (SCSSI). In practice, the supply and use of authentication equipment is routinely allowed within France and for export with a minimum of paperwork, regardless of the cryptographic algorithm employed. However, the statement or declaration submitted for supply, use or export of these devices must provide a "description of the security functions or mechanisms, including a detailed description of the cryptologic algorithm(s) (mathematical formulae) used and the system for the creation, development, and protection of the secret conventions; the software must be provided . . . in the source language." (U)

---

[6] Helsinki 3313, May 26, 1995. (U)

The second category embraces cryptographic methods or devices which provide for the confidentiality of data or transmissions and cryptologic analysis methods. Supply, use or export of devices in this category require prior authorization. The authorization, if provided, will either be a general authorization (that is, an authorization to supply or export devices to any user) or a private use authorization which restricts supply, export or use to specifically named individuals or communities. Data submitted by the supplier, user or exporter in order to obtain such authorization is extensive. In general, the information submitted must "describe not only the algorithm for generating a sequence or pseudo-random block, but all the hardware or software facilities, transforming an intelligible plain signal into an unintelligible cryptogram, including generating keys, storing them, managing them, etc." (U)

It is important to note that for both categories French law makes no distinction among software, firmware or hardware products. Software products, including mass-market software, are treated identically to hardware products. (U)

Import/Domestic Use

[

]7 (S).

Germany

Export

Germany regulates the export of cryptographic products based on the Foreign Trade Regulations (most recent publication of July 7, 1994). The list of commodities controlled under German law is published in "The Export of Embargoed Goods - German Export Control's Handbook" dated 1993 and essentially follows the COCOM guidelines. This document is quite extensive and lists export procedures, commodities controlled and countries requiring licenses. (U)

Germany requires a license for the export of cryptographic equipment to all destinations. The George Washington University (GWU) study determined that "Germany has specifically exempted encryption software from the General Software Note of the COCOM Industrial List. Therefore, Germany maintains control of both public domain and mass-market encryption software." This was confirmed in State: Bonn 12499-93 and in the CIA OSWR report on Foreign Laws and Policies. (U)

---

7 Paris 22932, August 22, 1994. (U)

[

]

[

] (S)

[

] (S)

Import

Germany does not require licenses for the import of cryptographic equipment. (U)

Domestic Use

[

][8] (S)

India

Export

[8] CIA: OSWR, *Foreign Laws and Policies on Secure Civilian Communications (U)*, SW M 94-20056, December 6, 1994. (S NF)

India is a major producer and exporter of software. India's software industry grew by 52 percent in 1994 and is expected to grow by a similar amount in 1995. Exports of all software exports rose by 50 percent by mid-1995 and are expected to reach $677.4 million (U.S.) by 1996.[9] By the year 2000 export revenues may reach $1 billion.[10] U.S. government officials and sources in India identified several Indian producers of encryption software products, although neither TIS nor NSA was able to identify any specific encryption software products. Quantitative information on Indian exports of software with encryption was not available. (U)

[

]" (C)

[

] (C)

Import/Domestic Use

[

] (C)

[

] (FOUO)

---

[9] "Indian Software Firms Record 51 Percent Growth," The Reuter Asia-Pacific Business Report, June 6, 1995. (U)

[10] "Software Industry Growing," The Ethnic Newswatch, March 17, 1995. (U)

[11] New Delhi 8364, May 24, 1994; New Delhi 5852, May 3, 1995. (U)

Israel

Israel, like France, has comprehensive regulations regarding the export, import, and domestic use of encryption products under a Court Order entitled "The Supervision On Products and Utilities (Dealing With Encryption Means), 1974, based upon the Supervision on Products and Utilities Law of 1957." This court order states that a person will not engage in encryption activities, to include import, export, production or use, unless he is licensed by a national manager appointed by the Minister of Defense (MOD). (U)

[

] (S)

[[12]

] (S)

Italy

Export

Italy has two distinct laws regulating the export of cryptographic equipment. The first, Number 185 of July 9, 1990, regulates the export of cryptographic equipment as an armament of war and requires approval for all such equipment. This law requires the company wishing to export equipment to seek approval from the Ministry of Foreign Affairs as well as the Ministry of Defense/Chief of Staff for Defense. Law Number 222 of February 27, 1992, and its supplement, Number 114 of May 18, 1994, also control the export of cryptographic equipment; they are essentially the Italian implementation of the COCOM guidelines. Although the Ministry of Foreign Trade has principal administrative authority in this area, decisions on export are made by an inter-Ministry commission which includes members from the Ministry of Foreign Affairs, the Ministry of Defense, the Ministry of the Interior, and the Intelligence agencies. Licenses are

[12] State: Tel Aviv 11049-93. (S)

approved or denied based upon economic considerations, Italian national security and international commitments. (U)

[

]

[

] (S)

[

][13] (S)

Import

No import laws were discovered although Italy does comply with the COCOM IC/DV system. (U)

Domestic Use

Italy has no law governing the domestic use of encryption. However, in the recent past, regulation governing civil sale, purchase and use of encryption was considered (and rejected) by the Italian parliament and a new proposal may be forthcoming.[14] (U)

---

[13] State: Rome 08436-93. (S)

[14] State: Rome 012823-94 (U)

Japan

Export

[

]

[

] (S)

Import

MITI officials state there are no import restrictions on cryptographic equipment in Japan. (U)

Domestic Use

The Ministry of Posts and Telecommunications has primary responsibility for regulating private or commercial encryption usage. These officials state there are no domestic restrictions on the private use of cryptography in Japan. (U)

Netherlands

Export

[[15]

[15] State: The Hague 03519-93. (S)

] (S)

[

] (S)

[

] (S)

Import

Dutch officials have confirmed that there are no import restrictions for cryptographic products, although the Netherlands conforms to the COCOM IC/DV system. (U)

Domestic Use

[[16]

] (S)

[

[16] CIA: OSWR, *Foreign Laws and Policies on Secure Civilian Communications (U)*, SW M 94-20056, December 6, 1994. (S NF)

] (S)

New Zealand

Export

The New Zealand Government treats encryption software as a dual-use item and requires an export license. The governing legislation is the Export Prohibition Regulations of 1953 and the Customs Act of 1966. Export permits are issued by the Customs Department on the advice of the Ministry of Foreign Affairs and Trade. [17] (U)

[

] (S)

Import/Domestic Use

New Zealand has no controls on the importation or domestic use of encryption software. (U)

Norway

Export

[

] (S)

[17] Aukland 240, May 24, 1995. (U)

Import

Foreign Affairs, as well as Defense officials, confirmed that there are no restrictions on the import of encryption equipment into Norway. (U)

Domestic Use

[

] (S)

Poland

Trade in encryption software is controlled as a military item by the Special Turnover Department of the Ministry of Foreign Economic Relations (MFER). The Department issues special concessions in coordination with the Export Control Department of the MFER, which is responsible for dual-use commodities. Polish authorities do not use DES or any other standard for control. Encryption software is evaluated on a case-by-case basis.[18] (U)

Russia

Export

[

[19]] (S)

With the disintegration of the former USSR, the President of Russia issued at least five decrees of February 22, March 27, April 11, May 12, and July 5, 1992 (Nos. 179,312,388, 469 and 507), which, together with the Law on Defence Industry Conversion, laid down certain legal foundations for a national armaments and military technologies export control system. These decrees were consolidated in 1994 by the "Statute on Controls of Exports from the Russian Federation of Certain Types of Raw and Processed Materials, Equipment, Technology, Scientific

---

[18] Warsaw 7649, June 2, 1995. (U)

[19] State: Moscow 14697-93. (S)

and Technical Information Which Can Be Used in the Production of Weapons or Military Equipment" as ratified by the President of the Russian Federation under Decree 74 dated February 11, 1994. Included in this statute is a list of commodities which require an individually approved license issued by the Ministry of Foreign Economic Relations for export from Russia. (U)

[

] (S)

[

] (S NF)[20]

Import

Section 5 of Edict Number 334, dated April 3, 1995, issued by the President of Russia prohibits the import of cryptographic products without a license. (U)

Domestic Use

Section 4 of Edict Number 334, dated April 3, 1995, issued by the President of Russia prohibits all activities in the development, sale and use of cryptography in Russia without a license issued by the Federal Agency for Governmental Communications and Information. (U)

South Africa

Export

The South African government controls encryption as a dual-use item on the General Armaments Control Schedule. Exports of encryption require an individual validated license. The control of encryption is under the jurisdiction of the South African Department of Defense Armaments Development and Protection Act, 1968, No. R.888, published on May 13, 1994.[21] (U)

---

[20] [ ](C NF), OSE IR 94-401758, November 8, 1994. (C NF)

[21] Johannesburg 000951, June 23, 1995. (U)

Import/Domestic Use

An individual validated license is required for the import of encryption software. A valid permit from the Armaments Control Division is required for the import or transportation of cryptographic equipment or software. (U)

Spain

Export

As a member of COCOM and the New Forum, Spain adopted export regulations which mirror the COCOM control lists. Spanish law in this area is codified in Royal Decree 824/1993 dated May 28, 1993, and its annexes dated September 21, 1993. This legislation establishes an inter-governmental committee to review export license applications as well as establish necessary policies in this area. This commission, the Junta Interministerial Reguladora del Comercio de Material de Defensa y de Doble Uso (JIMDDU), is presided over by the Secretary General for Commerce and includes representatives of the Defense Directorates and the Foreign Affairs and Economic Ministries. Licenses are approved or denied on an individual basis dependent upon the effects on Spanish foreign policy or national defense as well as international commitments. (U)

Most exports from Spain require an individually validated license for all destinations, although the law does make provision for general licenses and distribution licenses. Security products containing confidentiality features require individual licensing, even for EU and New Forum member nations. Exceptions may be granted for mass-market software products conforming to the COCOM General Software Note. (U)

The formulation of national cryptographic policies for Spain is under the authority of the Director General of the Centro Superior de Informacion de la Defensa (CESID), a department of the Ministry of Defense. The role and functions of the CESID are legislated in Royal Decree 1/1987, dated December 30, 1986. (U)

[

] (S)

[

] (S)

Import

Import authorizations are also addressed by RD 824/1993 and licenses are required for articles listed in Annex 6 . Cryptographic products do not require import licenses although Spain does comply with the COCOM IC/DV system and will supply import certificates for cryptographic products if required by the exporting country for delivery verification. (U)

Domestic Use

No Spanish laws specifically regulating the public use of cryptography in Spain could be found. Government use is under the control of the CESID by RD 1/1987. (U)

[

] (S)

[

]

[

] (S)

Sweden

Export

[

] (S)

Import

There are no restrictions on the import of encryption equipment into Sweden. (U)

Domestic Use

[

] (S)

Switzerland

Export

[

[22]] (S)

In response to a recent inquiry from the U.S. Department of Commerce, an official at the Swiss Federal Office of Foreign Economic Affairs stated that Switzerland controls the export of

[22] Bern 1371, August 18, 1994. (U)

encryption software. This official stated that up to the present the Swiss government has received no export license applications for encryption software (according to the Swiss, firmware, i.e. hardware/software combinations do not count as software).[23] Notwithstanding the above, sources in Argentina and South Africa state that Switzerland is a supplier of encryption software to their respective countries. (U)

Import

The import of encryption software is not subject to control in Switzerland. (U)

Domestic Use

Switzerland has no laws regulating the private use of encryption. (U)

United Kingdom

Export

[

] (S)

[

[24]] (C)

---

[23] Bern 2664, June 7, 1995. (U)

[24] State: London 08412-93. (C)

Import

There are no import controls on cryptologic products in the United Kingdom. (U)

Domestic Use

[

] (C)

III. WORLDWIDE MARKET FOR ENCRYPTION SOFTWARE: PRESENT STATE AND FUTURE PROSPECTS

One industry consulting firm recently estimated[1] current worldwide annual demand for encryption products at $1 billion.[2] The total world market for hardware and software confidentiality products was estimated at $695 million in 1991 and is expected to grow to $1.8 billion by 1996, with over half of the demand in the U.S.[3] Industry analysts indicate that a major portion of this market is for controlled encryption products (data and file encryption products comparable to DES or equivalent algorithms). They estimate annual demand for such products at several hundred million dollars.[4] A major portion of this demand is for hardware products, but software is growing rapidly in popularity and usage.[5] (U)

The term that best describes future growth trends for demand for encryption software is "explosive". Most encryption experts contacted during the course of this study agree on the following. The market for encryption software in distributed computation, databases, and electronic mail is beginning to expand rapidly as the U.S. and other countries develop and popularize electronic commerce, public networks, and distributed processing applications requiring encryption.[6] The direction this demand will take - hardware or software - will be determined by a number of factors, including cost, processing speed, and ease of implementation and installation. National and industry standards will play a key role, as will the pace of the development of trusted computer operating systems, without which software encryption is viewed as generally less secure than hardware-based encryption. Yet, most experts contacted for this study concur that encryption in the largest potential market, PC-based networking environments, will predominantly be implemented in software, which is generally less expensive than hardware, more flexible and simpler to install and upgrade. For these reasons businesses generally view encryption software as a cost-effective alternative to hardware devices in certain environments. According to one market research firm, for the next ten years, encryption software will primarily use DES and RSA-licensed encryption algorithms. A smaller percentage of software products

---

[1] All monetary values given in this section are in U.S. dollars. (U)

[2] According to Winn Schwartau, executive director of Interpact, an information security consulting firm in Seminole, Florida, as reported by Jill Gambon in *Information Week*, April 10, 1995. (U)

[3] "Cryptography Policy", *Communications of the ACM*, September 1994. (U)

[4] To place this figure in perspective, trade analysts in the Department of Commerce estimated the world market for packaged software at $77 billion in 1994. (U)

[5] Conversation with Tom Venn, president, Information Security Corporation, April 12, 1995. (U)

[6] Conclusion reached based on comments expressed by Ed Roback of NIST; Lynn McNulty , formerly of NIST; Dr. Dorothy Denning, Mathematics Department, Georgetown University; Dr. Steve Kent of BBN; and Tom Venn, President of Information Security Corp.

will employ company proprietary algorithms, primarily for security-specific products for small niche markets.[7] (U)

The applications for encryption software are extensive and increasing rapidly. As noted above, they include uses in general-purpose software products and security-specific products. Many general-purpose software products-particularly those that offer business and financial applications and communications products-include security features, such as encryption, as standard components. In general, interviews with a number of encryption experts led to the following conclusion.[8] In the near future, the greatest demand upsurge, in dollar terms, will be for mass-market higher-end networking software packages containing encryption features. In unit terms, the greatest near-term demand will be for mass-market, low-end add-on's for electronic mail (E-mail) and Internet software packages. (U)

Current trends suggest that civil use of software-based encryption will significantly increase in the next five years, with corporate customers dominating this new marketplace. Additionally, government and military customer demands for software encryption will increase due to its potentially lower cost and easier installation than hardware. Although in the near term the majority of the demand will continue to be in the area of network access protection and authentication of data, the requirement for data confidentiality, especially in archival applications and E-mail, will grow. (U)

Certain technological developments are promoting greater use by the general public of software-based network security features, including encryption, throughout the industrialized world. They include ever increasing use, fueled by well publicized "break-ins," of distributed databases, popular acceptance and usage of global networks, and the development and use of E-mail and electronic commerce. These developments are ongoing at one stage or another in practically all of the countries surveyed for this assessment. Market estimates from sources queried in some less technologically advanced countries, where demand for encryption software is reportedly negligible, indicate that these nations will soon undergo widespread development and computerization leading to increased demand for encryption software within the next ten years. (U)

The potential for electronic commerce using emerging technologies is expected to greatly increase demand for encryption software in the 21st Century. Total business transactions conducted over the Internet in 1994 have been estimated at $100 million and are expected to

---

[7] *Data Encryption Devices: Overview*, Datapro, March 1993. (U)

[8] Conclusion reached based on comments expressed by Ed Roback of NIST; Lynn McNulty , formerly of NIST; Dr. Dorothy Denning, Mathematics Department, Georgetown University; Dr. Steve Kent of BBN; and Tom Venn, President of Information Security Corp.

grow dramatically in the coming years. One market research firm estimates that more than $300 billion worth of goods and services will be traded over the Internet in the year 2000.[9] (U)

Some industry analysts foresee widespread demand for embedded encryption capability in such futuristic applications as electronic voting, digital cash, and network-based gambling.[10] In other words, the potential demand for encryption software is as unlimited as the need for risk-free, uninterrupted telecommunication. By all accounts, the mid-term to long-term potential demand for encryption software is so great that it defies any attempt to quantify it, particularly since much of the demand will be generated by consumer applications, such as electronic voting, digital cash, and network-based gambling, that do not yet exist outside of research environments.[11] These applications may generate demand for a wide range of security features including encryption functions currently under Commerce Department and State Department jurisdictions. (U)

Past experience suggests that the availability of cryptographic equipment in the domestic market was until recently based principally on the level of customer demand. Export controls had little, if any, effect on such availability. For example, government and industry panels found no evidence that the removal of access control equipment from the Munitions List in 1990, which rendered it freely exportable, had any significant positive impact on the availability of access control products or the development of this technology. In light of vendor assertions that export controls were not only affecting foreign sales but also domestic development of the technology and its availability for use in the United States, a significant improvement in the technology and its commercial availability were expected. This did not occur. While today there exists considerable concern among experts over the availability of secure technology to prevent unauthorized network access, market forces have not sufficed to make it widely available. (U)

E-mail applications are already beginning to generate widespread consumer demand for security-specific mass-market software products in the U.S. E-mail is one of the most popular features of the Internet and one of the most powerful technologies driving the Internet's exponential expansion in recent years. Security functions such as password protection and access control are a standard built-in feature of many commercial general-purpose software packages. Yet, the public's concerns about the security of its transmissions over public networks are generating unprecedented consumer demand for more advanced data confidentiality tools for E-mail packages: (U)

---

[9] " GTSI Announces New Electronic Commerce System for Government Use." *PR Newswire*, Financial News Section, April 4, 1995. (U)

[10] "Networking." *Computerworld*, January 23, 1995, P. 61. (U)

[11] "Networking," *Computerworld*, January 23, 1995, p. 61. (U)

- The American Lawyer News Service, which reviewed security on several public networking services, recommends using data encryption for all sensitive E-mail communications.[12] (U)

- The author of the current standard for E-mail header formats considers the lack of good off-the-shelf encryption as the main limitation of Internet mail applications today and views Pretty Good Privacy (PGP) as a promising solution to the problem of confidentiality.[13] (U)

- A recent review of several new Internet E-mail programs in a popular computer magazine noted their lack of confidentiality support and recommended that users implement their own "security plan" using programs such as PGP.[14] (U)

In general, many industry analysts contend that today's mass-market E-mail software lacks the embedded security features which the public demands. Critics of U.S. export controls attribute the absence of robust confidentiality encryption in today's mass-market networking software packages to controls on encryption software. They contend that some U.S. software companies are unwilling to include advanced cryptographic technology in mass-market products even for the U.S. market due to the realization that no company can control the distribution of its products with any certainty. They contend that the risk of civil liability or criminal proceedings is quite high for companies whose controlled products wind up overseas without proper licenses.[15] (U)

One example often raised is the case of the firm Viacrypt, a U.S. company which produces a commercial version of the embargoed PGP. The company was reportedly served with a subpoena requesting information related to the international distribution of its encryption software, even though the company disavowed any knowledge of the alleged exports and has no plans to export its product.[16] The end result of liability concerns, some critics of U.S. export control policy contend, is the availability of very few products containing advanced cryptographic

---

[12] "Protecting Privilege in E-mail Systems," *American Lawyer News Service*, September 5, 1994. (U)

[13] "Internet Off-The-Shelf Authentication and Privacy Found Lacking," *Electronic Messaging News*, April 19, 1995. (U)

[14] "Internet E-mail Front Ends," Editor's Choice; Overview of Nine Evaluations of Internet Mail Tools, *PC Magazine*, April 25, 1995. (U)

[15] [

] (FOUO)

[16] *Export Controls on Encryption Software*, by Ira S. Rubenstein (of Microsoft Corporation). (U)

technology on the domestic market.[17] However, this contention has been disproved by the TIS study, which has identified approximately 240 such U.S. software products advertised as containing DES and equivalent algorithms. (U)

A number of other factors may help to explain the lack of encryption in many commercial E-mail products. E-mail for most applications requires interoperability between software packages from different producers. Without a common encryption algorithm and key-exchange mechanisms and a de facto interoperability standard, users of different E-mail packages cannot communicate securely. To date, demand for secure E-mail has not been sufficient to drive industry to develop these necessary standards. (U)

A number of assessments undertaken in recent months indicate that user demand for data encryption software is extremely high among corporate end-users. For example, a recent survey of 151 U.S. corporations conducted by the Business Software Alliance, which represents U.S. software publishers, found that 37 percent would consider buying foreign software if it had better encryption than an otherwise superior domestic product. (U)

In order to assess how encryption is currently being used in the corporate sector, BXA contacted by telephone information security experts at ten diverse Fortune 500 companies. We spoke to security managers in the financial services, manufacturing, petrochemical, and insurance businesses. All companies polled considered encryption essential to their operations, and were currently using it (implemented in both hardware and software) for communicating and exchanging information with overseas customers, suppliers, and subsidiaries. Five out of the ten companies stated that they required encryption at least as strong as DES, while two expressed no preference for algorithms, and two said DES was not strong enough (prefer triple DES or IDEA). One company uses a variety of encryption solutions, including Lotus Notes, RC2/4, and PGP, depending on the sensitivity of the information being transmitted. Currently, three of the companies contacted were using foreign-origin encryption because they believe it offered better protection than U.S. products and could be freely used to communicate with international joint venture partners, suppliers, customers, etc. An additional three firms said that they would consider buying foreign encryption products should U.S. products be unable to meet their increasing demands for secure communications. (U)

All companies believe that their needs for encryption will increase dramatically over the next five to ten years. Several cited the spread of the National/Global Information Infrastructure, and the fact that their businesses were becoming more international as reasons for the ensuing rise in encryption demand. Most mentioned that they anticipate doing much more electronic commerce via the Internet, which is increasing the need for good public key encryption (e.g., RSA). One thought that computer hackers and other intrusions were becoming more and more common, thus increasing the need for computer security measures such as encryption. All ten

---

[17] Statement of Dr. Blaise W. Liffick, Mid-Atlantic Regional Director, Computer Professionals for Social Responsibility, at hearings of the National Research Council on Government Regulation of Cryptographic Technology, April 12, 1995. (U)

corporate encryption users expressed dissatisfaction with existing export controls on encryption software. This dissatisfaction ranged from mild inconvenience, in the case of two firms that received approval to export encryption software to subsidiaries, to a major cost factor, in the case of several firms using multiple, incompatible encryption packages to comply with export controls. Several also indicated that export controls are a significant obstacle to future development of electronic communications and commerce within their business. (U)

The demand for software with confidentiality features and the perceived lack of such features in much of today's general-purpose consumer software will promote the development and use of mass-market and custom-made security-specific encryption software products, such as PGP, in the U.S. and abroad. The existence of U.S. and, to some extent, foreign export controls on security-specific encryption software will promote the formation of markets shaped along national boundaries that resist penetration by foreign suppliers of products with exportable versions of encryption products. (U)

UNITED STATES

The U.S. data encryption market (hardware and software) reached an estimated $384 million in 1991 and will jump to $946 million by 1996.[18] As recently as 1993 the single largest user of data encryption equipment in the U.S. was the U.S. government. Within the business community, encryption was until recently used primarily by the banking and financial industries. Currently, over one-third of Fortune 500 companies specifically require encryption capability in their hardware and software purchases.[19] Confidentiality encryption (as opposed to other forms of cryptographic services) has become particularly important to industry due to recent publicity given to security threats. (U)

According to the market research firm Datapro, a major factor promoting the use of encryption is the publicity given to breaches of security by hackers. Another is the recent spate of warnings from government sources to industry regarding the threat from foreign intelligence services that have reportedly targeted U.S. firms for industrial espionage. (U)

NATIONAL MARKETS

One goal of this report is an assessment of the current and future market for computer software with encryption in foreign countries and the U.S. share of the market in these countries. Toward this end, the Bureau of Export Administration (BXA) attempted to quantify the U.S. market share in each of 31 foreign countries where encryption was thought to be in great demand,

---

[18] According to International Resource Development, as reported in "Cryptography Policy," *Communications of the ACM, September, 1994. (U)*

[19] According to a survey conducted by the Business Software Alliance. (U)

based on evidence of the development of indigenous encryption software products. BXA asked U.S. embassies abroad to determine the U.S. share of the overseas encryption market in those countries. Embassy personnel queried encryption specialists, U.S. and foreign encryption producers and users, and government authorities in 31 foreign countries where encryption software was thought to be commercially developed and sold. Their efforts resulted in rough estimates of market shares in 13 foreign countries. No substantive information was available from sources in several countries for a variety of reasons. (U)

No sources in the countries surveyed had access to import statistics or market literature on encryption software. The task of quantifying market shares was further complicated by the marketing activity of subsidiaries of U.S. companies and other third-country vendors in many of the countries examined. The complexity is heightened by the sourcing practices of software developers which may license a foreign-origin encryption algorithm for incorporation into a software product employing key management subroutines of yet a different origin. Royalty fees make up a considerable portion of the retail value of mass-market software. Many foreign encryption producers license encryption algorithms from the U.S. (U)

In many cases local producers and acknowledged experts had no idea themselves of the demand, in dollar terms, for software with encryption. Others (in Germany, for example) were reluctant to provide information for fear of inviting U.S. competition in a lucrative local market. Apparently some countries (Argentina and the Czech Republic, for example) have not yet advanced to the stage of developing a significant market for encryption software (as opposed to hardware). In these countries (as was the case earlier in the U.S.), the development and use of dedicated hardware encryption devices by the government and military may eventually lead to wider use of mass-market software products. Yet, despite the absence of precise trade data, definite conclusions may be drawn from the responses from several countries. (U)

In dollar terms encryption software currently comprises a very small portion of the overall market for computer software, according to reporting from some U.S. embassies. For example, encryption software accounts for only one percent of software demand in Austria and India. In Norway the figure is three percent. In Taiwan encryption software comprises less than 0.1 percent of overall software imports. The figures are probably similar for other countries. (U)

U.S. and foreign industry and government sources in Argentina, Finland, France, the Netherlands, Norway, South Africa, and Taiwan reported that the U.S. holds the majority of the general-purpose encryption software market in their respective countries. The U.S. dominance in the worldwide market is supported by evidence from other sources as well, including research by NSA. (U)

The U.S. share of the encryption software market is keeping pace with overall demand for encryption in most of the countries that were examined during this assessment. The three exceptions are Switzerland (where the U.S. market share reportedly declined in 1994, while the market shares of European countries reportedly rose), Denmark, and the United Kingdom, which

reported unspecified declines from previous years. Sources in all three countries attribute the decline to U.S. export controls, which they claim promote the development and sale of indigenous encryption products. (U)

Sources in a number of other countries indicated that the U.S. market share is keeping pace with overall demand despite the impact of U.S. export controls, which some sources claim tend to promote indigenous production or reduce U.S. market penetration. Such countries include Argentina, the Czech Republic, France, Germany, Israel, The Netherlands, New Zealand, Sweden, and Taiwan. (U)

One major drawback of this information is that very few sources provided estimates that made a distinction between markets for mass-market and custom encryption software, or between general-purpose software and dedicated encryption software. However, the results of a major research effort undertaken by NSA enable us to draw certain conclusions about these market segments. (U)

NSA attempted to identify foreign data encryption products through a variety of sources and verify their existence by purchasing the products. The NSA analysis followed the example of the TIS study in dividing mass-market encryption software into two categories: "general-purpose" products and "security-specific" products. General-purpose products were defined as those products containing encryption as an added feature but not the primary purpose of the product. This would include, for example, word processing, spreadsheet, and database software. These products, in most cases, do not advertise the encryption capability on the shrink-wrapped package. Security-specific software products have data security as their principal purpose and can often be recognized by titles such as "Datalock" or "Safeguard." Here, the security features of the product are broadly described on the outer package. Further analysis in this report reflects this distinction. (U)

GENERAL-PURPOSE SOFTWARE WITH ENCRYPTION

In 1993 (the latest year for which data are available), the U.S. held approximately 75 percent of the world market for mass-market software products, 91 percent of the systems software market, 77 percent of the applications tools market, and 63 percent of the applications solutions market. Of the world's top 10 software suppliers, six were American.[20] The overwhelming majority of general-purpose products with encryption available on foreign markets today are, according to NSA and TIS, of U.S. origin. They include word processors, spread sheet programs, data base programs, and the like. Other U.S.-dominated mass-market product segments expected to generate demand include: personal computer operating systems and a broad

---

[20] *US. Global Trade Outlook, 1995-2000,* International Trade Administration, U.S. Department of Commerce, March 1995. (U)

range of PC applications software. Commerce Department analyses indicate that the U.S. has few viable foreign competitors for such products. (U)

Several factors contribute to the competitive strength of the U.S. packaged software industry. Foremost is the leading role U.S. vendors played in developing the software industry. This has given U.S. firms a technological edge and made the U.S. the locus of high-quality, innovative software development. The size and sophistication of the U.S. market also contributed to the competitiveness of U.S. vendors, resulting in a variety of niche products, a great number of firms, and intense competition. The principal competitors to U.S. vendors are companies in Japan and Western Europe, which generally specialize in custom software and services in domestic markets and have little international presence.[21] (U)

NSA found that U.S. software companies dominate the world in this category such that there is virtually no foreign competition. Over 50 visits to computer and software stores in Canada, France, Germany, Japan, South Korea, Thailand, and the United Kingdom found products containing encryption from Microsoft, Lotus, Symantec, and other U.S. manufacturers dominating the shelves. No sources for this report could identify any general-purpose software products with encryption for confidentiality from a non-U. S. manufacturer. (U)

In contrast, NSA identified 40 U.S. general-purpose software products which include controlled confidentiality features. All of these products are under Commerce Department jurisdiction. In addition, three products have versions that are subject to State Department jurisdiction. (U)

Table 3.1 Selected Mass-Market General-Purpose Software Products with Encryption for Confidentiality under Commerce Jurisdiction (PROPIN)

* Higher-security versions of these products are licensed by the Department of State.

[21] Ibid. (U)

This study identified a significant number of foreign and U.S. general-purpose software products providing password protection but not data encryption. In the U.S., such products do not fall under State Department jurisdiction and are freely exportable. (U)

In the absence of significant foreign competition, the impact of U.S. export controls on the international market shares of U.S. general-purpose products is probably negligible. Customers are often unaware of the encryption features in these products, since such features are not emphasized in most cases. U.S. industry sources agree that foreign customers base their software purchases on the features implementing the primary function of the product (e.g., word processing or database), not seldom-used security features. In the future, security features in these products may be more important to end-users. (U)

SECURITY-SPECIFIC ENCRYPTION SOFTWARE

For the reasons given above, concrete estimates of market shares for security-specific encryption software are difficult to obtain. A firm estimate of the U.S. market share was obtained from only one country. Experts in the United Kingdom, a country with a well-developed indigenous encryption software capability, estimate the U.S. share of the market for security-specific encryption software products at only 15 percent, with 80 percent held by U.K. firms. (U)

Information from a variety of sources indicates that this market segment is quite competitive. U.S. software manufacturers face stiff competition in several foreign markets from such encryption exporting countries as France, the United Kingdom, Germany, and Israel. Also, in some countries export controls may have created additional market opportunities for local system integration firms and software houses, which already have a competitive advantage in that they are better situated to work closely with end-users and develop encryption solutions tailored to meet the conditions of the local environment. (U)

The NSA study confirmed the existence of a significant number of foreign and U.S. security-specific software products with controlled encryption features. According to NSA and TIS, the majority of such products are of U.S. origin; foreign products are predominantly from Western European suppliers. About half of the U.S. products in this category are under the licensing jurisdiction of the Department of Commerce. About half are under State Department jurisdiction. (U)

These products are usually not available on the shelf at retail stores either in the U.S. or abroad. In some 50 visits to computer and software stores in Canada, France, Japan, South Korea, Thailand, and the United Kingdom, neither U.S. nor foreign security-specific software products providing confidentiality were found. In addition, in telephone inquiries to 25 other retail outlets in these countries, none claimed to sell encryption software products. (Appendix B lists foreign stores surveyed.) Generally, such products can be purchased abroad only through direct contact with the manufacturer. Many U.S. companies have foreign distributors for their

products, and there are some distributors of foreign products in the U.S. Availability of U.S. products in the U.S. and Canada is slightly higher, and some U.S. products can be ordered through retail outlets. (U).

The TIS study identified 117 foreign software products with encryption for confidentiality. The next chapter gives more detailed information on these foreign retail products. As noted above, some of these products could not be confirmed or were no longer available by the time NSA attempted to confirm their existence. Some additional products were found by NSA and the Department of Commerce during this study. Obviously, this is a market in flux, and any firm number for products available is constantly changing. However, the TIS study appears to be a good approximation of the current size of the foreign market for retail confidentiality products. It does not, however, reveal the full extent of the availability of custom-made products, a number of which are developed overseas in academic institutions and defense enterprises exclusively for military, industrial, and government end-uses. (U)

The TIS study gives a good indication of the quantity of foreign software retail products available abroad. Unfortunately, it gives no indication of specific sales volumes or market shares attained by these products, information that is necessary to assess their importance in the market. The study also gives no information on the effects of foreign export controls on these products. Also, a comparative analysis of U.S. and foreign products is not available. NSA has undertaken an assessment of the quality of the security provided by the foreign products, but has not conducted similar analyses of U.S. products. Seventy-six foreign products are identified by TIS as using DES, but this identification appears to have been largely based on product advertising rather than an analysis of the products themselves. The results of NSA's analysis of these products are given in the next section. (U)

Each of these factors above must be taken into account to fully assess the foreign market for software products with encryption. NSA consultations with several foreign governments and with U.S. companies indicate that sales of most security-specific products are few and appear to be predominantly to customers within the country of origin of the product, with one exception: products targeted for financial applications, which seem to have wider market penetration. Several governments, like the United States, give more favorable treatment to exports of DES products for financial uses than for other end-uses. (U)

Any assessment of the current and future potential market for U.S. security-specific encryption software must also take into account direct competition which software products face from U.S. and foreign hardware devices and combination hardware/software products that are also designed to perform security-specific encryption functions. Several foreign firms are well positioned to expand from established market positions in security-specific hardware encryption to the rapidly expanding encryption software market. Leading foreign producers of hardware encryption with an international presence include Gretag and Crypto AG of Switzerland. It has been reported that a number of European firms which have traditionally sold DES hardware products have recently introduced their first DES software implementations. (U)

[

] (S NF NC)

[[22]

[23]] (S NF NC)

MARKET SHARE IN FOREIGN COUNTRIES

The Bureau of Export Administration asked U.S. embassies abroad to determine the U.S. share of the overseas encryption market. To date substantive information has been received from 30 countries. The information provided below represents the best estimates obtainable by U.S. embassy personnel, based on information provided by U.S. and foreign representatives of business, academia, and trade associations. Although the responses vary, most indicate that U.S. export controls adversely affect U.S. sales abroad. Unfortunately, these sources did not provide supporting data that would permit independent analysis of their estimates. Also, many market estimates do not distinguish between hardware and software, which makes it difficult to draw conclusions regarding controls on software markets. Nevertheless, these estimates represent the best available information on U.S. shares of foreign encryption software markets. (U)

With the exception of Canada (where U.S. export controls do not apply), sources in 14 countries indicated that U.S. export controls limit U.S. market share in their countries. Sources in seven countries indicated that export controls have either no impact or no major impact. Sources in one country (Israel) indicated that export controls also limit international cooperation in developing international data communications links and infrastructure. The other countries were unable to provide a definitive response. None of the sources provided hard evidence to confirm their assertions, other than estimates of the U.S. share of the software market. (U)

---

[22] *Foreign Reaction to the U.S. Key-Escrow Encryption Initiative. (U)*

[23] *Communications of the ACM, July, 1992. (U)*

Not all of the sources contacted agreed on the economic impact of U.S. export controls, perhaps due to varying degrees of competition from indigenous producers in individual countries. For example, unlike the majority of respondents, sources in Austria, Finland, and India indicated that export controls do not impede local marketability of U.S. products. In the case of Austria, this opinion was expressed by U.S. affiliates that export encryption software primarily to banking and government institutions (i.e. organizations that are generally exempt from controls on DES). Sources in Belgium indicated that U.S. export controls hamper the availability of U.S. products, but felt that the controls are no more restrictive than European controls. No other sources indicated an awareness of non-U.S. export controls on encryption. France, which has export, import, and domestic use controls at least as stringent as the U.S., was reported as a major foreign source of encryption software in Argentina, Australia, the Netherlands, and South Africa. However, neither TIS nor NSA identified any French encryption software products. (U)

In general, the majority of responses from overseas indicates a definite awareness among foreign industry sources of the existence of U.S. export controls on encryption software such as DES. They also reveal a perception that DES and other advanced algorithms are generally more exportable from other countries. These perceptions (whether accurate or not) are widespread and pervasive. They undoubtedly play a part in shaping the product-sourcing decision-making processes of prospective foreign purchasers and thereby adversely affect the U.S. presence in the highly competitive security-specific market. Unfortunately, the information from abroad is not precise enough to draw further conclusions about the economic impact on segments of the encryption market. In many cases, the responses from abroad did not distinguish between hardware and software markets. Some of the more substantive comments from abroad are summarized below. (U)

Argentina[24]

The demand for encryption software in Argentina is negligible at this time, since information security awareness is at an embryonic stage. The market is difficult to quantify, but it is generally accepted that the U.S. is the leading supplier of encryption software with a market share of over 60 percent. Other leading suppliers are (in order of market share) Israel, France, and Switzerland. U.S. suppliers are expected to maintain or increase their share of the market as Argentina develops its data-processing infrastructure. Encryption software products are under development in Argentina, but no indigenous firms have begun commercial production. (U)

Local firms indicated that U.S. munitions controls impose long delays on the acquisition process. They stated that such delays have prompted the local development of encryption devices and software. (U)

---

[24] Sources: Local computer software trade association, leading suppliers and users of encryption software in Argentina, as reported by the U.S. Foreign and Commercial Service in Buenos Aires 2125, dated April 10, 1995. (U)

The Government of Argentina is currently evaluating encryption solutions, including digital signature, for its banking and financial sector. (U)

Australia[25]

The market for encryption software has not developed into a measurable segment, with much of the activity still at the academic level. The encryption market is poised to expand greatly within the next nine to twelve months. Demand surge will be driven by financial and banking institutions seeking to protect electronic transactions and the introduction of smart cards. Australian sources state that a rapid expansion of electronic commerce may be imminent. (U)

The Australian market is supplied primarily by local vendors and U.S. companies. The U.S. market share has remained stable in recent years. Japan, Taiwan, France (the firm Ingenico), the United Kingdom (Admiral Computing), and New Zealand are also sources of encryption software. No information is available on the size of the market or the market shares of individual countries. (U)

Austria[26]

Encryption accounts for approximately 1 percent of the total software market in Austria. The U.S. holds approximately 20 percent of the encryption market. The remaining 80 percent is held by the firm SNI (Siemens-Nixdorf). The U.S. market share has increased at an annual rate of about 5 percent in recent years. The banking sector and government account for most of the current and projected demand for encryption software in Austria. Future demand surges will be promoted by the needs of military, police, and industrial security, data networks, ISDN and asynchronous transfer mode networks. (U)

U.S. export controls pose no problems, according to three U.S. vendors identified by the U.S. Embassy. (U)

---

[25] Sources: Dr. William Caelli, Information Security Center, Queensland University of Technology, Jennifer Seberry, Center for Computer Security Research, University of Wollongong, and industry representatives, as reported by the U.S. Foreign and commercial Service in Sydney 719, dated April 7, 1995. (U)

[26] Source: U.S. vendors, as reported by the U.S. Foreign and Commercial Service in Vienna 2963, dated April 7, 1995. (U)

Canada[27]

The primary end-users of encryption software in Canada are government agencies, financial institutions, and other large business organizations. Future demand is expected to sustain or surpass a recent annual growth rate of about 10 to 15 percent, primarily by new users on the information highway. Long-range growth trends in Canada parallel those in the U.S., with the greatest market potential being in low-cost, mass-market encryption software for use by the public in network applications. (U)

Sixty percent of Canadian demand for encryption software is satisfied through imports. The majority (70 percent) of imported encryption software is of U.S. origin; the remainder is from Europe. A number of small, niche-oriented Canadian companies develop and market security-specific encryption software. One such company, a division of the telecommunications giant Northern Telecom, recently agreed to provide encryption software for Microsoft Exchange, a client-server messaging product. (U)

U.S. export controls do not directly affect U.S. exports to Canada, since the controls do not apply to Canada. They do, however, limit exports of Canadian software containing encryption developed in the U.S. (U)

Czech Republic[28]

Demand for encryption software in the Czech Republic is quite small. Near-term prospects for commercial encryption products are also small, but longer-term demand is expected to increase. (U)

The market share of U.S. producers is very small. Only two U.S. firms supply products to the Czech market. Since demand is negligible, export controls have not had a noticeable impact on imports to the Czech Republic. However, approximately a dozen Czech firms are reportedly developing their own encryption software in order to avoid U.S. export control regulations. No Czech firms are currently producing commercial encryption software. (U)

---

[27] Reported by the U.S. Foreign and Commercial Service in Ottawa 1706, dated April 10, 1995; and "Microsoft Picks Northern Telecom Encryption," *Newsbytes News Network*, October 20, 1994. (U)

[28] Reported by the U.S. Foreign and Commercial Service in Prague 1980, dated March 28, 1995. (U)

Denmark[29]

Sources in Denmark were unable to provide an estimate of current market demand, which is believed to be quite low compared to other developed nations. U.S. embassy reporting indicates that future demand growth will be explosive due to growing use of electronic commerce and rapid development of the Danish information infrastructure. Within the next 5 to 8 years total demand may reach $300 million, on an average per annum market consumption of roughly $50 million. (U)

U.S. suppliers are thought to satisfy 10 percent of demand in the banking sector, where U.S. export controls provide for an exemption, and zero or near zero percent of the remaining market segments. (U)

Denmark has only two significant indigenous commercial producers of encryption software. (U)

Finland[30]

Demand for encryption software is expected to increase due to increasing use of electronic commerce and open networks such as Compuserve and Internet. There are about 200,000 Finnish users of the Internet, and the number of users is expected to grow at an annual rate of 20 to 30 percent. (U)

About 60 to 80 percent of mass-market encryption software is of U.S. origin. The United Kingdom has a 20 to 30 percent market share. Germany holds about 20 percent of the import market. Imports of encryption software are expected to increase by about 10 percent over the next three years. (U)

Nokia Special Systems is the only local manufacturer of encryption software. (U)

U.S. export controls reportedly have no major impact on U.S. market share. (U)

---

[29] Reported by the U.S. Foreign and Commercial Service in Copenhagen 2000, dated April 21, 1995. (U)

[30] Reported by the U.S. Foreign and Commercial Service in Helsinki 5749, dated April 6, 1995. (U)

Germany[31]

Hard data are not available on the encryption software market, which is difficult to quantify. Demand in German businesses for encryption technology is reportedly high due in part to strict national data protection laws requiring the protection of all data of a personal nature and at least one state law requiring encryption of government files on portable computers. Sources generally agreed that demand for encryption software is on the rise. Estimates of annual growth rates range from 5 to 20 percent over the next several years. (U)

Sources in Germany were unable to provide precise figures on the U.S. market share for encryption software. Their estimates were, however, consistently low, the highest being 20 percent. They attribute the low U.S. market share to U.S. export controls. (U)

Most sources believe that the German market is covered primarily by German suppliers. One German firm (Uti-Maco) claimed a market share of over 50 percent. German companies reportedly win out over foreign suppliers, in part because of German customers' dissatisfaction with the lengthy licensing requirements of other countries. One German research institute reported concern among German customers that the U.S. was exporting only "soft" (i.e. easily breakable) encryption algorithms. (U)

India[32]

Current demand in India for encryption software is reportedly negligible. Approximately I percent of total software production in India is encryption, but the figure may grow to 15 percent within 5 years.[33] Future demand will be driven by Indian economic reforms-including reform of the banking sector and privatization of industries-and the development of a national information infrastructure. U.S. export controls do not currently have much impact on U.S. market share in India. However, Indian industry sources feel that U.S. export controls will have a greater impact as demand increases within the next two to three years. (U)

The U.S. is the leading foreign source of encryption software in India, with 35 percent of the market. The U.S. is followed by the United Kingdom (10 percent), Germany (8 percent), and Singapore (5 percent). The largest market share (42 percent) is accounted for by local vendors (approximately 18 in all, including affiliates of U.S. and other foreign firms). The defense sector is currently the largest consumer of encryption software in India. India is reportedly an exporter

---

[31] Sources: government and industry experts, local companies, as reported by the U.S. and Foreign Commercial Service in Bonn 7245, dated April 6, 1995. (U)

[32] Sources: Indian software producers, the National Association of Software and Services Companies, and the Manufacturers Association of Information Technology, as reported by the U.S. and Foreign Commercial Service in New Delhi 4082, April 13, 1995. (U)

[33] This figure is understood to represent encryption software and software encompassing encryption. (U)

of encryption software, but neither TIS nor NSA identified any Indian encryption software products. The development of an indigenous encryption software industry is in keeping with past Indian industrial strategy of reducing reliance on foreign products and protecting indigenous high-technology industries. (U)

Israel[34]

The Israeli market for software with encryption is estimated at $5 million annually and is expected to grow to $10 million within five years. Israeli use of computer networks, including the Internet, grew 400 percent over the last year. Commercial and business use of computer networks is also increasing. Demand for software with encryption is expected to grow at a similar rate. (U)

Sixty Israeli companies produce software with encryption for the national security, government, and commercial segments of the Israeli market. Eighty percent of these producers are thought to sell custom-made programs for software applications. Sources claim that virtually no U.S.-origin software with encryption is sold in retail outlets in Israel. It is believed that encryption software imported from the U.S. is used to provide security for large main frame computers. A large share of the Israeli market for U.S. software imports is reportedly held by companies which have representatives or branches in Israel (e.g. IBM, Novell, Digital and CA). U.S. imports are not popular in the large-volume custom-made software market because they lack local Hebrew language support services. Very little software with encryption is imported from Europe, although Israel has many European-Israeli joint ventures producing software for the European market. (U)

Sources in Israel state that U.S. export controls severely limit U.S. exports of software with encryption to Israel. They also believe that U.S. export controls also limit U.S.-Israeli cooperation in developing international data communications links and infrastructure. (U)

Italy[35]

In 1990 an Italian market research firm estimated the Italian market for encryption software at $80 million. Demand was expected to reach $115 million by 1995. In fact, actual purchases are considered to be much lower, due in part to a lack of security awareness among Italian business organizations. Only 23 percent of Italian companies polled recently utilized the maximum level of security available to them. Only 20 percent of banks polled claimed to use

---

[34] Source: U.S. and Foreign Commercial Service reporting in Tel Aviv 8478, dated April 20, 1995. (U)

[35] Sources: officials of a research company, a major bank association, and information technology firms, as reported by the U.S. Foreign and Commercial Service in Rome 5284, dated April 10, 1995. (U)

encryption software. Purchases of encryption software are well below the consumption rate for the rest of the European Union. (U)

Demand among the public may increase after the introduction of home banking services. The market for such services is estimated at 1.5 million potential users. Other developments expected to promote demand for encryption software include the development of electronic commerce, plans for an information infrastructure, and increased use of Internet (expected to double last year's volume by 1996). (U)

Information sources in Italy identified no U.S. security-specific encryption software products marketed in Italy and only two Italian products—from Olivetti and possibly MAC Alenia Marconi Communications. (U)

Japan[36]

The Japanese market for encryption software is in the early stages of development and is several years behind the U.S. in terms of consumer demand and technical development by local firms. Demand is held down by a low sense of security awareness and a low rate of computerization relative to the U.S. The demand for encryption software should increase as the information technology market develops in Japan. At 7.8 personal computers per 100 people (versus 28.1 per 100 in the U.S.), PC usage is low but increasing rapidly, making Japan potentially the second largest market for computers and software. (U)

No figures are available on the U.S. share of the Japanese encryption market. A rough estimate of a portion of the U.S. market share may be derived from estimates of the Japanese packaged software market, which is estimated at $7 billion annually. U.S. producers hold about 6 percent of this market. If, as in Austria and India, roughly 1 percent of this market comprised encryption software, the U.S. share for prepackaged encryption software would be $4.2 million. (U)

[

] (PROPIN)

All industry and government sources contacted in Japan agreed that a relaxation of export controls would increase market opportunities for U.S. encryption software suppliers. Japanese companies lag behind the U.S. in encryption technology, but are expected to close the gap over time if existing U.S. export controls continue in effect. (U)

---

[36] As reported by the U.S. Foreign and Commercial Service in Tokyo 4216, dated April 11, 1995. (U)

The Netherlands[37]

Popular electronic communications applications that promote the use of encryption include electronic banking, E-mail, and online transactions. In December 1994, the Dutch Cabinet announced a high-priority action plan, "Electronic Highways, from Metaphor to Action." One of the action points is to develop a policy on cryptography. A 1994 draft proposal by the Minister of Justice to restrict the use of encryption was withdrawn due to major opposition. (U)

The total Dutch information technology market is expected to grow at an annual rate of 3 to 5 percent. The computer software segment is expected to increase by about 10 percent annually, with standard software packages currently valued at about $1.1 billion. Estimates of the value of the encryption software market vary widely, starting at $100 million. Industry sources estimate that U.S. firms supply at least 50 percent of the market. Local production is limited and estimated at 10 percent of the market. Imports from other European countries (Germany, the United Kingdom, and France) account for the remainder. (U)

The Netherlands is an international distribution center offering a gateway for U.S. and other firms wishing to distribute their products throughout Europe. At least two Dutch software distributors have stated that they were importing no U.S. products, preferring instead to deal with German and British products, because of restrictive U.S. export/re-export regulations. (U)

New Zealand[38]

The market for security-specific encryption software products is conservatively estimated by industry sources at $6.5 million per year. The market is growing at an annual rate of 20 to 30 percent. Figures are not available for general-purpose software products containing encryption. (U)

New Zealand is experiencing a growth in the use of public networks for electronic transactions and other business communications. Distributed computing and Internet connectivity will also drive demand for encryption software. The United Kingdom is the largest supplier of security-specific encryption software. The U.S. is second. Market shares are not known for general-purpose encryption products. (U)

Industry sources state that U.S. export controls have an adverse impact on the U.S. market share for security-specific encryption software. It is thought that U.S. export controls have little or no impact on the market share for general-purpose software incorporating encryption features. (U)

---

[37] As reported by the U.S. Foreign and Commercial Service in The Hague 7630, dated March 29, 1995. (U)

[38] From industry sources, as reported by the U.S. and Foreign Commercial Service in a memo to the U.S. Department of Commerce in April 1995. (U)

Norway[39]

The 1994 market for encryption software was estimated at $15 million, or approximately 3 percent of the total software market in Norway. Most of the demand is met by imports, primarily from the U.S. A smaller proportion is supplied by countries such as Sweden, Germany, and Israel. There are two major manufacturers of cryptographic equipment for military applications: Norwegian Defense Technology and Alcatel Telecom Norway. No information is available on market shares, but the U.S. is said to dominate the market. Nearly all encryption software used in Norway is reportedly based on the U.S. Data Encryption Standard (DES). (U)

Norway is expected to experience a steady increase in electronic commerce involving sensitive information, and future demand will most likely require stronger mass-market encryption software. Norway has a fairly strong tradition in developing encryption systems for the Norwegian military. Norwegian Privacy laws encourage the use of privacy on national networks. (U)

A relaxation of U.S. export controls is not expected to have a significant effect on the U.S. market share since U.S. products already dominate the market. However, a relaxation resulting in the export of more advanced encryption software would stimulate an expansion of the end-user base (and, therefore, sales). This suggests that currently exportable encryption software is receiving less than maximum market acceptance, particularly (as indicated above) for electronic commerce applications. (U)

South Africa[40]

Current demand for encryption software is small but growing steadily. Encryption software is widely used by banking and financial institutions, government and military entities, retail networks, and in the telecommunications sector. Future demand will be driven by advances in electronic banking and commerce, and prepayment networks for utilities. (U)

No statistics are available on the market for encryption software. The total value of all software imports during the year ending in June 1994 was approximately $49 million. The U.S. held a 71-percent share of the import market. Other major suppliers are: France, Israel, Germany, Switzerland, Italy, and the United Kingdom. South African companies that were contacted cited the U.S. as the single most important source of encryption software. Eleven South African companies also develop and market encryption software in South Africa. (U)

---

[39] As reported by the U.S. and Foreign Commercial Service in Oslo 1927, dated April 11, 1995; and "Norwegian Encryption Standard Moves Forward," *Computer Fraud & Security Bulletin*, 1994. (U)

[40] Sources: Local firms and the Rand Afrikaans University in Johannesburg, as reported by the U.S. and Foreign Commercial Service in Johannesburg 596, dated April 12, 1995. (U)

DES is the most widely used encryption algorithm in South Africa. The Pretty Good Privacy (PGP) program is used by a small sector of businesses. The Swiss International Data Encryption Algorithm (IDEA) is also in non-commercial use in South Africa. (U)

U.S. export controls do not appear to be adversely affecting the sale of U.S. encryption software or technology to South Africa, primarily due to local industry's high regard for U.S. technology. (U)

Switzerland[41]

Switzerland is a major developer and consumer of encryption technology. It is a world leader in encryption hardware technology. The well developed, internationally-oriented Swiss economy promotes steady growth in the demand for encryption software. Sources claim its technologically advanced, export-oriented industry is a major developer and producer of encryption hardware and software. However, neither TIS nor NSA identified any Swiss encryption software products. The Swiss-developed IDEA encryption algorithm is superior to DES in terms of key length, making IDEA-encrypted text more difficult to break by trying all possible keys. IDEA has a 128-bit key length; DES has only a 56-bit key length. Developed by James Massay and Xuejia Lai at ETH, a technical institute in Zurich, IDEA is perceived by some as a potential replacement for DES as an industry standard.[42] Switzerland is reportedly an exporter of encryption software products and was cited as having an appreciable share of the encryption software market in at least two other countries under review. In response to a query from the U.S. Department of Commerce, Swiss export control officials stated that the Swiss government had by then received no export license applications for encryption software.[43] (U)

The latest available information indicates that U.S. encryption software products held only a 10 percent share of the Swiss market in 1994 and were down by 5 percentage points from the previous year (despite the presence of a large number of internationally-oriented financial institutions that are exempt from U.S. control). Meanwhile, Swiss products rose by 10 percentage points to a 55-percent share of the market. Other European products were up by 10 percent to a combined 35-percent share. (U)

Information on the size of the Swiss market is unavailable. (U)

---

[41] Sources: suppliers, distributors, and users in Switzerland, as reported by the U.S. and Foreign Commercial Service in Bern 1803, dated April 12, 1995. (U)

[42] General Accounting Office Report GAO-AIMD-95-23, January 23, 1995. (U)

[43] Bern 2664, June 7, 1995. (U)

Taiwan[44]

Taiwan's encryption software imports comprise less than 0.1 percent of software imports, which reached $134 million in 1994. Taiwan has no significant indigenous commercial production. Banks are thought to be the main end-users of encryption. They have a decided preference for hardware/software combinations and rarely purchase software alone. The demand for encryption software will undoubtedly increase with the development of Taiwan's national information infrastructure and will be met mainly by imports. (U)

U.S. suppliers lead the computer software market with approximately 56 percent of imports to Taiwan. U.S. suppliers of computer software will continue to maintain a large share of the market over the next five years. (U)

Distribution export licenses that are available for encryption software have reduced the adverse impact of export controls on the U.S. market share for encryption software. (U)

United Kingdom[45]

No reliable information is available on the size of the U.K. market for encryption software. One may assume that the market is fairly comparable to that of Italy (over $115 million), since the United Kingdom's economy, level of technology, and industrialization are roughly comparable to those of Italy. Consequently its information security requirements should also be comparable.[46] (U)

The number of indigenous producers of security-specific encryption software has been conservatively estimated at six. The greatest potential future market is thought to be in the implementation of security in public domain global information structures. (U)

The U.S. currently holds 15 percent of the U.K. market. Indigenous producers hold 80 percent. The U.S. share of the U.K. market has declined in recent years, reportedly due to U.S. export restrictions. Sources state that U.S. export controls have led the United Kingdom to

---

[44] Sources: Taiwan branch offices of U.S. encryption software producers, as reported by the U.S. and Foreign Commercial Service in Taipei 2080, dated April 12, 1995. (U)

[45] Sources: The Department of Trade and Industry, the Communications and Electronics Security Group, academic and government cryptography experts in the United Kingdom, as reported by the U.S. and Foreign Commercial Service in London 7288, dated April 10, 1995. (U)

[46] Sources in the U.K. estimated the market at only $500,000 to $600,000 in annual sales. This figure is extremely low for a nation the size of the U.K. Judging by the context in which it is given, the figure probably refers to dedicated encryption software only, without taking into consideration general-purpose software with encryption features. Even so, the figure may understate the extent of this subsegment as well. (U)

lessen its reliance on U.S. sources of technology and promote local development of encryption algorithms. (U)

PAST AND FUTURE MARKETS

From the 1950's to the late 1970's commercially produced encryption equipment, mostly hardware, was sold principally to government and military end-users. The major exception was the international financial market, which recognized the importance of cryptography, principally for data and user authentication purposes in funds transfers. This market was dominated by hardware devices. (U)

The 1980's began the "commercialization" of cryptography and the development of a software industry with an ever increasing percentage of sales to non-government organizations, no longer limited to the financial community. Major markets exist for encryption among non-banking industries with a history of industrial espionage, such as the petrochemical and pharmaceutical industries, due to recent media coverage and U.S. government briefings on the subject. Due to the widespread use of computer-aided design and manufacturing and the digitalization and transmission of engineering data, a much wider range of industries, from automobiles to semiconductors, now use encryption to maintain the confidentiality of data communications.[47] For these reasons, companies are more aware than ever before of the need to secure sensitive information during all stages of storage, processing, and transmission. (U)

The data acquired to date indicate the development of high-end and low-end commercial market sectors. End-users placing a high value on their data, such as governments and the financial community, still tend to prefer hardware-based cryptography and often obtain independent evaluations of the security provided by the equipment or software to be purchased. The majority of corporate purchases to date appear to fall in the low-end category, with purchase decisions often based on cost and ease of installation and without much knowledge of the real level of security. (U)

The foreign and domestic markets for encryption software in distributed computer environments, databases, and electronic mail will grow rapidly as the U.S. and other countries develop and popularize electronic commerce, public networks, and distributed processing. (A more long-term catalyst here and abroad is the development of national information infrastructures.) Current trends suggest that encryption in these environments will be implemented predominantly in software, as opposed to hardware. The E-mail encryption software of preference among informed users appears to be confidentiality software (such as PGP) that is strictly controlled under State Department jurisdiction. (U)

---

[47] Statement by Bob Rarog, Export Policy Manager, Digital Equipment Corporation. (U)

This control has the immediate effect of creating a niche for foreign producers of security add-on products for U.S. and other mass-market software products and certain other custom-made security-specific products. The future economic impact of U.S. export controls on foreign markets for general-purpose software has yet to be determined, but it appears to be less severe than the impact on security-specific encryption. (U)

The lack of strong built-in encryption features for confidentiality in today's commercial E-mail software combined with user demand for encryption by privacy-conscious consumers will promote the development and use of mass-market and custom-made security-specific encryption products, such as PGP, in the U.S. and abroad. The existence of U.S. and, to some extent, foreign export controls on encryption software will help promote the formation of markets shaped along national boundaries that resist penetration by foreign products. However, other factors, such as language preferences and familiarity with local business practices, undoubtedly will contribute to these market divisions. (U)

The international market for general-purpose software with and without encryption has consolidated around established producers in the U.S., Western Europe, and Japan. The U.S. is expected to maintain its dominant position in this market. Yet, many small and medium-sized U.S. firms are, for a variety of reasons, reluctant to develop products for export markets. Such firms will require up-to-date information on exporting, and fewer export restrictions (particularly on security features for data transmission) to capitalize on their technological strengths in the international market.[48] (U)

International competition is expected to increase in the security-specific encryption market. Demand for hardware encryption for government and military applications is likely to taper off near current levels and spur a shift to the software market by established hardware producers in the United Kingdom, France, Germany, and Switzerland. As competition increases, consumers will benefit from a wider selection and (eventually) lower unit prices. (U)

[

]

[48] Mary Smolenski, software industry analyst, *U.S. Global Trade Outlook, 1995-2000,* International Trade Administration, U.S. Department of Commerce, March 1995. (U)

[

[49]] (S/NF)

[49] *Foreign Reaction to the U.S. Key-Escrow Encryption Initiative* (U), CIA, August 31, 1993. (S)

IV. ANALYSIS OF FOREIGN SOFTWARE PRODUCTS WITH ENCRYPTION

The Presidential Review Directive mandating this study asked for a review of the types, quality and market penetration of foreign-produced encryption software products. In order to accomplish this, NSA attempted to procure products from a variety of countries and companies, as reflected in the Trusted Information Systems (TIS) database and other sources. Canadian products were not included, as there are no export controls between the U.S. and Canada. NSA sought to acquire products advertised as using DES as well as those advertised as using other encryption algorithms. Where there were multiple versions of a product, or related products from a single manufacturer, only one version was procured. Within these parameters, products were chosen randomly with no prior knowledge of the product's quality or availability. (U)

Various methods were used to procure products. NSA established a contractual relationship with TIS to purchase products and deliver them to NSA. NSA asked USG representatives abroad as well as foreign government officials to purchase specific products. Finally, selected NSA personnel traveling abroad purchased products. In addition, three software products obtained by TIS were given to NSA for analysis by Rep. Sam Gejdenson during a Congressional hearing in October, 1993. (U)

TIS in its study for the Software Publishers Association identified software products from 44 foreign producers, two of which are Canadian. Attempts were made to acquire products from 21 of the remaining 42 and were successful in 17 cases. In several instances sources were unable to obtain specific products requested, either because the supposed producer companies could not be located, because the products advertised were no longer available, or due to required export licensing paperwork that NSA elected not to provide. In one case, NSA did not purchase a product due to its high cost. In addition, NSA obtained several products from producers not on the TIS list. Altogether, 28 products from 22 foreign producers have been acquired to date. Table 4.1 lists the products that were sought and the results of those efforts. In some cases, information about export licensing requirements is noted in the table. For the other there was no specific information on what licensing requirements, if any, were applied to the individual export. In any event, both NSA and the private firm TIS were able to purchase software encryption products purportedly containing DES or other algorithms from a wide selection of countries. This confirms U.S. industry's claims that such products can be obtained. (U)

Table 4.1 Attempts to Acquire Selected Foreign Software Products with Encryption (S)

Product	Producer	Country	Algorithm	Attempt by	Result
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
16					
17					
18					
19					
20					
21					
22					
23					
24					
25					
26					

Product	Producer	Country	Algorithm	Attempt by	Result
27					
28					
29					
30					
31					
32					
33					
34					
35					
36					

* Contains identified algorithm plus one or more additional algorithm. Proprietary indicates a non-standardized, usually vendor proprietary algorithm.

Details of the analyses to determine the actual cryptographic quality of these products are available in a more highly-classified version of this paper. [

] (S)

Even if foreign products professing DES or other strong encryption algorithms are in fact not as secure as some U.S. products, their existence nonetheless can have an effect on U.S. industry's competitiveness. Most encryption users base their purchasing decisions on the stated encryption strength, other product features, company reputation, and price. They do not perform sophisticated analyses to determine the actual cryptographic capabilities of various products. Therefore, if foreign products appear to be superior to American products, U.S. firms may still lose potential sales. This would apply to potential customers in the United States as well as abroad. Some foreign encryption vendors reportedly use the existence of U.S. export controls on

strong encryption to differentiate their products and capture markets from U.S. firms. (U)

V. ECONOMIC IMPACT OF EXPORT CONTROLS

In order to determine the impact of existing export controls on U.S. encryption software vendors, BXA developed a comprehensive industry questionnaire addressing issues including lost sales, market potential, and product development. A copy of the survey instrument is attached as Appendix C. The questionnaire was developed working closely with the Software Publishers Association, the Business Software Alliance, and other industry groups, and was distributed in mid-March 1995 to over 200 encryption software vendors and other interested parties. Survey recipients included mass-market general-purpose software producers, as well as security-specific software vendors. The distribution list was compiled using association memberships, listings in trade periodicals and directories, references in encryption-related press articles, and the database of encryption vendors amassed by Trusted Information Systems. The survey was also posted on the Internet. Additional questionnaires were distributed to interested parties, such as lawyers and consultants representing encryption firms. Completion of the survey, which received OMB approval for distribution under the Paperwork Reduction Act, was voluntary. (U)

The final rate of return to the survey was less than originally expected. The net response was slightly less than one third (72 firms), including the companies responding that they were not involved in encryption software and those that had merged or have gone out of business. The economic impact analysis in this chapter was developed using the 36 completed surveys received, of which some were more "complete" than others. For those interested in reading actual company comments and data related to encryption sales, markets, and export controls, Appendix D contains pertinent individual company responses to questions on the survey. To help insure the confidentiality of this information, each company was given a number. The listing of company names and their numbers is given in Appendix E. (U)

As the data collection came to a close, several reasons emerged as to why the return rate was relatively low. (U)

- The survey was often "lost in the shuffle". Follow-up calls to a number of companies found that many firms in this business are very small, and that this voluntary study was not high on the priority list as they hustled to keep the daily business going. Calls made to non-responding firms often evoked a high level of interest and concern in the encryption export issue, but were very time-intensive. (U)

- One survey respondent commented that in a recent industry session, many participants indicated that they had not responded due to concerns that they might inadvertently give out information that would have adverse legal implications in the future, or that their proprietary data would be disclosed. (U)

- A number of firms apparently chose to disregard the survey because they were skeptical of efforts by the Government to accomplish anything of value related to encryption, which

has been an issue of controversy for at least a decade. (U)

- As a final point, Commerce expected a higher return from some of the software industry leaders, especially those dealing in mass-market software with encryption. While some were forthcoming with the survey data, others apparently decided instead to participate in private-sector initiatives on similar issues. (U)

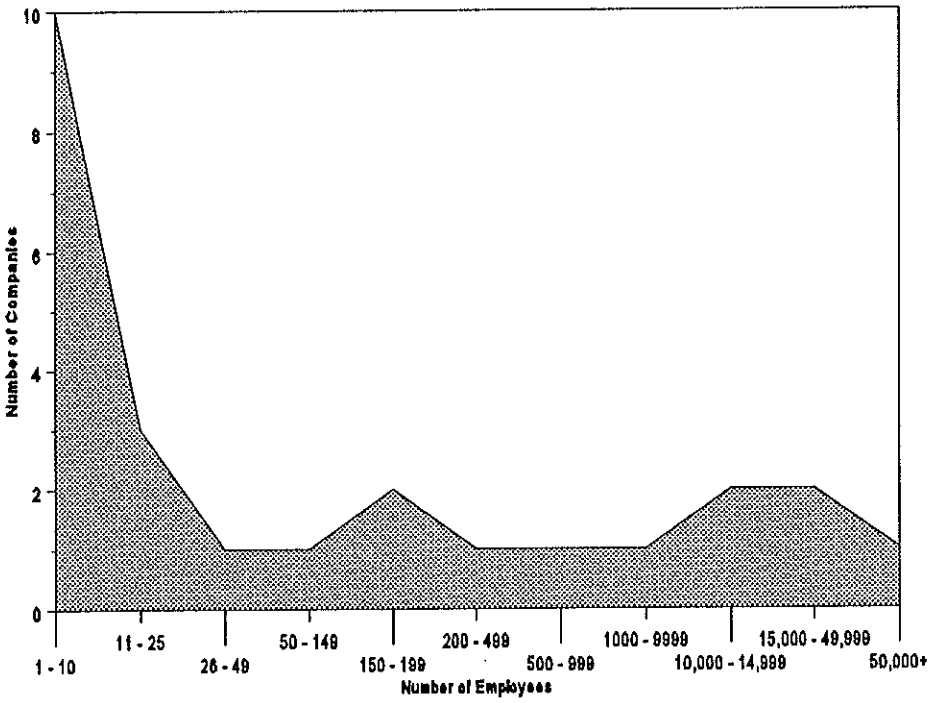
- Whatever the reason, those firms most vocal in expressing concern over the economic effects of export controls did not provide evidence to support their claims, though given ample opportunity to do so over a three-month period. (U)

DESCRIPTION OF SURVEY RESPONDENTS

Company Size

The available data clearly points to many encryption software developers as small, niche producers in the broader software field. Two-thirds of the survey responses (that provided employee information) were from very small companies -- less than fifteen people, and often less than five. An illustration of the survey respondents broken down by number of employees is shown in Figure 5.1. (U)

Figure 5.1 - Company Sizes (U)



Products And Markets

The majority of the survey respondents produce security-specific software products (rather than general-purpose) that perform a variety of encryption functions, including data encryption. By far the most common algorithm used is DES. Other algorithms mentioned were RSA, RC2/RC4 (often used for exportability), IDEA, and proprietary algorithms. At least one company utilizes a "flexible encryption" system capable of meeting a specific user's needs. These products have a multitude of "niche market" applications and do not necessarily compete with one another directly. Most firms sell to large corporations in financial and manufacturing sectors, as well as the U.S. government. Their products are marketed directly to customers -- through such mechanisms as telemarketing and mail order. A few distribute through "shareware" or on the Internet, while three mentioned retail outlets or resellers. Those few with retail/reseller distribution systems were more likely to have international distribution. (U)

Many survey respondents were reluctant to provide their sales data for encryption products. In addition, several companies were introducing new products into the market, and did not yet have sales data. Based on those companies that did provide information, sales of encryption software have increased markedly over the past five years, in response to increasing demands for computer security products. [ ] of the companies surveyed provided sufficient financial data on their encryption sales to provide a figure for combined foreign and domestic revenue for 1994: $3.3 billion. The vast majority of this sum is accounted for by sales of general-purpose software with encryption as a minor feature, as the security specific market sales figures available totaled only $ 55 million. The combined figure, while not representing the total industry, demonstrates that the size of the market is certainly significant. (PROPIN)

Survey respondents appear to face only limited competition from foreign firms in the U.S. market. Most companies knew of no foreign competitors. Respondents providing for specific examples of foreign competition listed Uti-Maco and FAST of Germany, ASCOM of Switzerland, Highware of Belgium, Dynasoft BoKS of Sweden, Checkpoint Firewall and Ellemtrix of Israel, Instant Access and Monotype of the U.K., and Aladdin (U.S.-based company with French operations). (U)

EXPORT LICENSING

Only seven companies responding to the survey currently apply for and receive export licenses from the Department of State. The majority of their controlled encryption exports involve products using the DES algorithm for financial applications. Those survey respondents that export encryption products that are under Department of Commerce jurisdiction often developed software packages with specific encryption features (e.g., reduced key length) in order to fall within Department of Commerce's more flexible licensing system. (U)

The time involved in processing the State export licenses and commodity jurisdiction decisions was cited by most companies as a factor of concern. The majority of companies were

able to secure export licenses for their DES-based products within two to six weeks from the Department of State. Occasionally these companies experienced delays of up to six or eight months, citing policy decisions as a frequent reason for prolonged license application reviews. Nevertheless, many companies reported a noticeable improvement in the State Department's licensing system due to a recent streamlining of their license processing procedures. As a result, many companies saw their export license processing times cut in half. (U)

Although the ability to secure export licenses in a timely manner was cited as important to encryption exporters, they did not consider the process to obtain these licenses to be a hindrance to their competitiveness. Only two of the seven companies involved in the export licensing process had an application denied by the Department of State. [

] Many companies complained more about the prohibition of exporting DES algorithms abroad and the necessity to develop special exportable versions of their software packages, as opposed to the licensing process in general. (PROPIN)

Companies that dealt exclusively with the Commerce Department's licensing system did not express any concerns over the processing times involved for receiving export authorization. Many noted, however, that the costs incurred to develop exportable versions of their products and then administer their exports were burdensome. One company indicated that the additional administrative expenses adversely impacted its business practices, customer relations, competitiveness, and gross margin. Another one said that a two year lead time in their development of new mass-market products is required to ensure that the products will be judged to fall within Commerce jurisdiction. (U)

EXPORT ISSUES

Of all the companies surveyed, only one company volunteered that it felt its encryption products should not be exported. Since its product contained DES, foreign markets were not considered nor would they be. While this company's lack of interest in penetrating foreign markets was unusual, the opinion on DES was not. At least seven of the companies surveyed emphatically maintained that since their products incorporate DES, they don't even bother to try to get an export license, and have given up on foreign markets. For the small companies, many deem the difficulty and time expended in pursuing export licenses even for applications that may be approved (e.g., financial) not worth the effort, even considering the potential growth in market size. (U)

[

]

[

] (PROPIN)

FOREIGN MARKETS

Only three survey respondents had a sizable (>15%) share of foreign markets. Many respondents said they had no market share overseas due to U.S. export control restrictions. Four companies had overseas market shares ranging from 10%-55%. U.S. market shares overseas were apparently not limited significantly by foreign import or domestic use restrictions on encryption. A few mentioned that they had to obtain approval of the French Government (and one was prohibited from selling there). Other countries mentioned by at least one respondent as having some type of domestic use/import documentation requirements for encryption software were Russia, South Korea, Switzerland and Singapore. (U)

Many of the companies that do not currently export their product due to export controls believe that there is a significant potential foreign market for their products. However, these companies are unable to quantify the size of this market, or to evaluate their losses as a result of not having access to it. These companies do not market overseas, but most receive inquiries from foreign parties on a regular basis (describing these inquiries as coming "constantly," "daily," or "five times a month"). Some companies have considered developing an exportable version of their products (and some already have them), but hesitate to do so because they believe the foreign demand is for encryption at least as secure as DES, if not stronger. Even among buyers not highly knowledgeable about encryption, word of mouth has led to a general sense that "exportable" U.S. encryption software is not satisfactory. Customers are also interested in software that allows them to choose which algorithm to use ("crypto with a hole"), which is also subject to U.S. export controls. (U)

One survey respondent believes that export control policy has negatively affected domestic sales of its product. A significant number of this company's potential domestic customers are seeking encryption software to communicate with international associates, and since it believes its product cannot be exported, it is unable to fulfill this need. (U)

Some firms acknowledge that the current foreign market for products like theirs is probably small, but is expected to grow substantially. They believe that not being able to participate at the early stage of market development will be a tremendous obstacle to their future international competitiveness. Most believe the potential foreign market is substantial, and predict that their export sales could increase significantly if allowed to export stronger algorithms -- some by orders of magnitude. (U)

EMPLOYMENT

The Presidential review directive for this study requested an evaluation of the impact of encryption export controls on jobs in the computer software industry. While our industry survey attempted to address this issue, by and large companies were not able to provide this type of information. Many companies that do not export at all due to export restrictions logically responded that none of their employment relied on export sales. They are unable, however, to predict how many jobs may be created should export controls be lifted because they have no real way to gauge the actual size of foreign markets or the share of these markets that they might capture. (U)

Those companies now exporting their products under Commerce or State licensing jurisdiction tended to respond that all of their employment (all employment in their security/ encryption division) was dependent on these sales. Since few of the companies had been denied a license by State or Commerce, employment was not significantly affected. Again, some companies whose products are now under Commerce jurisdiction believe that their export sales would increase dramatically if they were able to incorporate stronger algorithms, which would in turn require additional employees to meet the demand. (U)

Appendix A - Glossary of Terms

The following is a listing of common terms related to encryption that are used in this paper:

Authentication: This is process by which the receiver of a coded digital message can verify the identify of the sender and/or the integrity of the message. It is often done through the use of a digital signature in public key systems, and through the use of a shared secret in secret key systems. Since digital signatures cannot be repudiated, that is, the signer of the document cannot later disown it as a forgery, the recipient can be confident of the authenticity of the sender and of the integrity of the message. (U)

Cryptographic Application Interface (a.k.a. Crypto With a Hole): A method for allowing hardware or software products to take advantage of cryptographic features without embedding such cryptographic features in the products themselves. A hardware device such as a secure phone that uses a security chip might have an empty chip socket; the buyer would have to acquire the necessary security chip separately and insert it himself. In software, the applications program would contain no encryption algorithms but would have a software interface written to easily allow the use of encryption algorithm code acquired separately. This might be done either to allow purchasers a choice of cryptographic applications for a product or perhaps in hopes of avoiding export controls on confidentiality products. However, such specially-designed cryptographic applications interfaces are subject to control under the ITAR. (U)

Digital Signature: A method in public key encryption techniques to verify authenticity of the sender of a message. A one-way hash function is used to compute a value that is a function of the message that is being sent. This hash function creates essentially a "fingerprint" of the data as by its nature it is computationally infeasible to obtain the same hash value from two different messages. The recipient of the message validates the signature in a three-step process. The hash value of the data is computed by the validator, then the validator transforms the hash value that arrived with the (purportedly) signed message using the signer's public key component and compares the results. If the two match, the signature is valid. (U)

Encryption algorithm: This is the mathematical function used for encryption and decryption. There are two basic types: symmetric or "secret-key" algorithms and asymmetric or "public-key" algorithms. Symmetric-key algorithms use the same secret key for encryption and decryption. The best known secret-key algorithm is the Data Encryption Standard (DES), developed in the 1970s at the request of the U.S. National Bureau of Standards (now NIST). It has become the *de facto* national standard for many applications, and it has a 56-bit key length that allows for 72 quadrillion possible key combinations. (U)

Asymmetric-key algorithms require pairs of keys: one key of each pair is used for encryption and the other for decryption. The decryption key must be kept secret, but the encryption key can be made public, e.g. published in a directory, hence the term "public-key

encryption". RSA and Diffie-Hellman algorithms are the best-known public-key encryption methods. Note that the public-key algorithms, while more convenient to use, are much slower than the secret-key algorithms, so users wishing to encrypt significant amounts of information typically use secret-key algorithms to encrypt the information and use public-key methods to securely exchange the necessary secret keys. (U)

Key: A numerical parameter or set of symbols that is required to utilize an algorithm to encrypt and decrypt a message. Symmetric-key encryption algorithms such as DES use a single secret key for encryption and decryption, which both the sender and receiver must know beforehand to pass messages back and forth. Asymmetric-key algorithms use public key/private key pairs. A particular person's public key, which can be made available to everyone, allows anyone to encrypt a message for that person. The message can only be decrypted using that person's corresponding private key, which is kept secret. In either case, the difficulty of guessing the key varies exponentially with the key length. If the key is 8 bits long, then there are $2^8 = 256$ possible keys; a 56-bit key yields $2^{56} = 72$ quadrillion possible keys. (U)

Key Management: The generation, distribution, entry and destruction of the key settings. The effectiveness of an encryption software package hinges on its handling of key management. (U)

In evaluating the computer encryption software industry,

General-Purpose Software: Software products containing encryption as an added feature but not the primary purpose of the product. Examples of this type of software are word processing, spreadsheet and database packages that have a file encryption function as part of their features. (U)

Mass-market Software: Computer software that is available to the public via sales from stock at retail selling points, by means of over-the-counter transactions, mail order transactions or telephone call transactions. Furthermore, the software must be designed for installation by the user without further substantial support by the supplier. Substantial support does not include telephone (voice only) help line services for installation or basic operation training provided by the supplier. (U)

Security-specific Software: Computer software, the principal purpose of which is to provide specific security-related functions - access control, authentication, file encryption, etc. It is usually purchased separately from other applications to fill a user's specific security needs. (U)

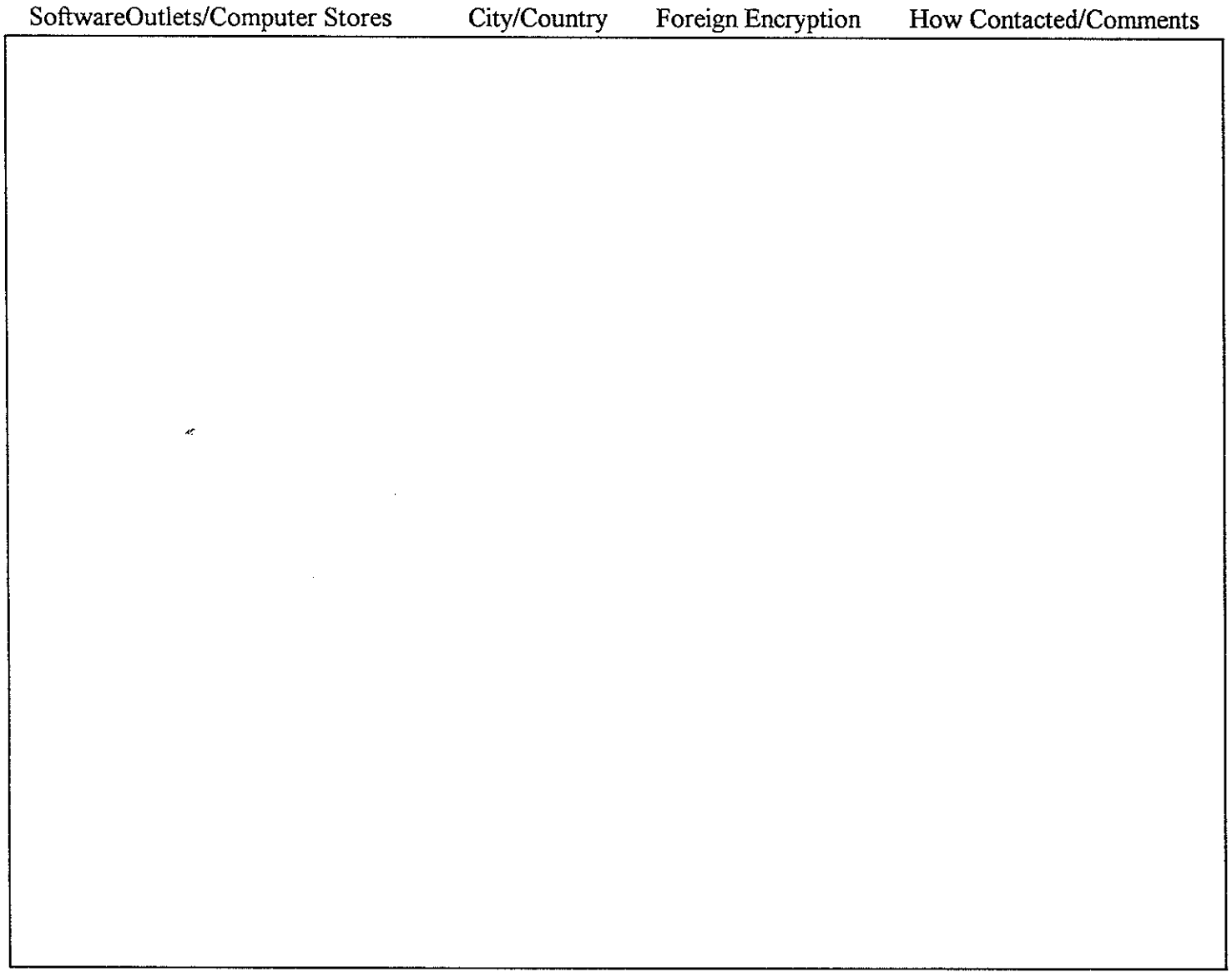
Appendix B- Foreign Software Outlets Contacted by NSA (FOUO)

Software Outlets/Computer Stores	City/Country	Foreign Encryption	How Contacted/Comments

SoftwareOutlets/Computer Stores	City/Country	Foreign Encryption	How Contacted/Comments

SoftwareOutlets/Computer Stores	City/Country	Foreign Encryption	How Contacted/Comments

SoftwareOutlets/Computer Stores	City/Country	Foreign Encryption	How Contacted/Comments


SoftwareOutlets/Computer Stores
City/Country
Foreign Encryption
How Contacted/Comments

Appendix C - BXA Encryption Marketing Survey

OMB Control # 0694-0087
Expires 12/95

BXA Office of Strategic Industries and Economic Security,
Economic Analysis Division,
Encryption Software Marketing Survey

President Clinton has directed that the Administration undertake a study of the competitiveness of U.S. companies in the international market for computer software with encryption. In support of this effort, BXA has initiated a study to evaluate the impact of current export controls on worldwide encryption software sales and the international competitiveness of the U.S. software industry. The results of this study, which will be finalized July 1, 1995, will be used by the Interagency Working Group on Encryption and Telecommunications Policy in evaluating the overall U.S. encryption policy, including export control regulations.

NOTE: All answers will be treated and protected by the Government as company proprietary information. Confidential business information will not be disclosed without permission of the source, but may be aggregated in such a way that the source of the information cannot be identified.

Directions:

This survey applies to all software that contains cryptography (password protection, data encoding, digital signatures, etc.), including mass market software for which encryption is not the primary function. The survey is divided into two sections to better delineate between current market data and industry potential. The answers to the questions in Section I will establish the information base necessary for a quantitative analysis of individual products, how they are exported, and their established markets. The responses to the Section II questions will outline the less definitive but equally important encryption software industry evaluation on market growth and potential. **Any information you can provide is welcome. If your company produces no encryption software products, please indicate below and return this survey to us.**

_____ **No software products containing encryption are made.**

Please send responses to: U.S. Department of Commerce
Bureau of Export Administration, Office of Strategic Industries and Economic Security, Economic Analysis Division
Attn: Karen Swasey, Division Director
Room 1608, 14th & Pennsylvania Ave., N.W.
Washington, D.C. 20230
Tel: 202-482-5953, Fax: 202-482-3195

The due date for responses is April 15, 1995.

I. INDUSTRY PRODUCTS & MARKET

1. Please identify the software products (indicating those which are mass-market) you produce which contain (or versions of which contain) cryptography. Cryptographic or encryption software is that which uses cryptography in any way including methods to protect passwords, encode data to provide confidentiality, or provide digital signatures for transmission identification. For each product, please provide the following information:

Product Information

a. What is the product's primary function (e.g., word processing, database, security, etc.)?

b. What security functions using cryptography are included (e.g., data encryption, data integrity, user authentication, digital signature, etc.)?

c. For each security function, what cryptographic algorithm is used, and with what key length? Exactly how is the key generated or specified by the user? For example, is it derived through a password or entered in some other manner?

d. Are key management features included? Please describe.

Market Information

e. What were the total sales (in units and revenue) for the product for each year between 1990-1994 in the U.S.? Outside the U.S. (if possible provide a breakdown by region, e.g., Europe, Asia, etc.)?

f. Please categorize the principal customers of the product (e.g., financial, services, manufacturing, government, etc.).

g. How is the product marketed in the U.S. (e.g. retail outlets, mail order, etc.).?

h. What is the product's estimated share of the U.S. market? Also, give an estimate of the future market share expected for this product. Please explain how you arrived at these estimates.

i. How is the product marketed abroad (e.g. retail outlets, mail order, etc.)? If it varies by country, please specify.

j. What is the product's estimated share of the non-U.S. market? Please explain how you arrived at this estimate. Please give an estimate of the future foreign market growth for this product and explain how you arrived at this estimate.

k. Does the product face competition in the U.S. market from foreign products? If so, please specify the competing foreign product(s) and encryption features. Please also indicate the estimated share such products have of the U.S. market and how you arrived at this estimate.

l. Have you had trouble exporting this product to any countries due to foreign import restrictions? If so, please indicate which nation(s) and the restrictions you encountered.

m. Have you experienced or are you aware of any restrictions that may apply to the use of this product in other nations? If so, please describe.

Export Licensing

n. Do you export the product? Which Department (Commerce or State) has export licensing jurisdiction? Have you attempted to get a validated export license or munitions license for the product? *If not, please go to question q.*

o. Have export licenses for this product been granted (provide license numbers if possible)? Please give the total number of products licensed for export and the resulting revenue, for each year between 1990-1994. Also, for each year, indicate the average time needed to obtain a license.

p. Have export licenses for this product been denied (provide license numbers if possible)? Please indicate the total number of denials for each year between 1990-1994.

Where a product was denied export, please document if possible:

- The potential customer, destination country, and intended end-use.
- Whether a competing product from another vendor subsequently got the sale. If available, what product, from what vendor, in what country?
- Whether encryption features of the competing product are comparable to your product. If so, please provide details.
- The value of the proposed export.

q. Are you aware of potential customers not considering your product because they know it could not be exported? How do you know they did not consider your product and why? Why did they assume your product could not be exported?

r. Have you not applied for an export license for the product, assuming that the application would be denied? If so, please document to the extent possible:

- Why you assumed it would be denied.
- The value of the foregone export.
- The potential customer, the destination country, and the intended end-use.
- Whether a competing product from another vendor subsequently got the sale. If so, what product, from what vendor, in what country?
- Whether the encryption features of the competing product are comparable to your product. Please provide details.

2. For <u>all</u> the encryption software products sold by your company, what is the administrative cost of verifying that upgrades of the software are in compliance with State and Commerce export control levels?

3. How many jobs (full-time equivalent) in your company depend on sales of software products with encryption features which make them subject to individual munitions licensing requirements by the Department of State? Please indicate the number of jobs and the percentage of total employees. Sales of such products accounted for what percentage of your company's total revenues for each of the years 1990-1994?

4. How many jobs (full-time equivalent) in your company depend on sales of software products containing encryption which are eligible for bulk or distribution licensing by the Department of State? Please indicate the number of jobs and the percentage of total employees. Sales of such products accounted for what percentage of your company's total revenues for each of the years 1990-1994?

5. How many jobs (full-time equivalent) in your company depend on sales of software products containing encryption which are eligible for general license under the Department of Commerce? Please indicate the number of jobs and the percentage of total employees. Sales of such products accounted for what percentage of your company's total revenues for each of the years 1990-1994?

II. MARKET GROWTH & POTENTIAL

1. <u>Product Features</u>

a. Have current export controls prevented you from implementing security functions, specific

algorithms, key strengths, or key management in mass market products? Please explain.

b. Which of the above encryption features have you omitted or reduced the key length for products destined for foreign markets? Please identify the products and provide market information if not included above.

c. What impact would the inclusion of these omitted encryption features have on the products -- would it change the intended end-use or attract new end-users? Please provide market assessment leading to this conclusion.

d. Did your company consider including additional encryption features in the products it is currently selling but rejected such inclusion because it knew the resulting product would not be approved for export? How did the company know it would not be approved for export? Why did your company initially consider including such features? If customer demand, how did your company assess that demand?

e. What products have you considered producing that would be viable in foreign markets but you did not produce owing to current export controls on encryption technology? Describe the proposed product, projected foreign sales, and how you arrived at that projection.

2. <u>Market Potential</u>

a. Please estimate the total value (in $U.S.) of foreign sales you would expect, over and above potential sales of products you currently can export, from exports of products with stronger security features. Please explain how you arrived at this estimate. Who are the principal customers or types of customers for these products you feel you cannot bring to market under current export controls, and why do you believe export controls restrict access to these markets? Break the foreign markets down by region if possible, and identify the destination countries and intended end use(s). Please be as specific as possible (e.g. cite examples).

b. Please estimate the total value (in $U.S.) of sales of encryption products in the U.S. that you believe you forego as a result of U.S. export controls. Please explain how you arrived at this estimate.

c. How many (alternately, what percentage) and what type of your existing customers have inquired about security features? What type of features are they interested in (password, authentications, confidentiality)? What strength? Do they consider security to be an important feature? How important? Please quantify your answers and explain how you arrived at them.

d. What type of potential customers do you believe have never inquired about purchasing one or more of your company's products because they know you could not meet their security demands? What is the basis for this belief? Please estimate the loss of sales to your firm attributable to this foreign customer perception, and explain how you arrived at this

estimate.

e. Do you know of competing foreign products being sold which have security features that you can't provide due to export controls? If possible, please identify the products, their vendors, and in what countries they are available. Please explain in each case how export controls prevent you from providing competitive security features. If possible, please provide sales and market share information for the foreign products you cite, and indicate the source of that information.

- **Any additional comments on or relevant examples of lost sales, revenue, and market by U.S. companies would be most welcome.**

BURDEN ESTIMATE AND REQUEST FOR COMMENTS. *Public reported burden is estimated to average 3 hours per response for those companies who choose to participate in this voluntary project. Should you have any comments on this burden estimate or any other aspect of this survey, please contact the BXA Reports Clearance Office, Bureau of Export Administration, Room 6883, U.S. Department of Commerce, Washington, D.C., 20230, and the U.S. Office of Management and Budget, Paperwork Reduction Project (Control # 0694-0087), Washington, D.C. 20503.*

Appendix D - Industry Encryption Survey Data

In order to evaluate the impact that U.S., export controls are having on industry, Commerce initiated a voluntary encryption software survey that was directed to 228 companies identified as being involved in the encryption software industry. To help insure the confidentiality of the company comments and data, each company was given a number which were used in the following analysis. A listing of the company names for each number is given in Appendix E. (U)

EXPORT LICENSING

[

] (PROPIN)

[

] (PROPIN)

POTENTIAL GROWTH

[

(PROPIN)

FOREIGN INTEREST

[

] (PROPIN)

[

] (PROPIN)

FOREIGN MARKET SHARE

[

] (PROPIN)

EXPORT SALES

[

] (PROPIN)

[

] (PROPIN)

Appendix E - Company Name/Number Listing

Company Names/Numbers Used In Section 5 Of This Study: (PROPIN)

1
2.
3.
4.
5.
6.
7.
8.
9.
10.
11.
12.
13.
14.
15.
16.
17.
18.
19.
20.
21.
22.
23.
24.
25.
26.
27.
28.
29.
30.
31.
32.
33.
34.