

158



# AMERICAN EMBASSY THE HAGUE

# FAX

Date: 21-Sep-99

Number of pages including cover sheet: 5

To: [Redacted]

Export Control and Economic Sanctions

Ministry of Economic Affairs

Re: U.S. Encryption Policy

Phone: [Redacted]

Fax: [Redacted]

From: [Redacted]

Economic Officer

Economic Section

Phone: [Redacted]

Fax: [Redacted]

E-mail: [Redacted]

REMARKS:     Urgent     For your review     Reply ASAP     Please comment

Dear Mr. Bontenbal:

Following please find information regarding changes in U.S. encryption policy. If you have any questions, please call.

Sincerely,

[Redacted Signature]

## CHANGES TO U.S. ENCRYPTION POLICY

TECHNOLOGY IS ADVANCING AT SUCH A RAPID PACE THAT ATTEMPTS TO CONTROL ITS GLOBAL SPREAD UNDER THE EXISTING EXPORT CONTROL REGIME NEED TO BE REGULARLY REEVALUATED. ENCRYPTION PRODUCTS AND SERVICES ARE NEEDED AROUND THE WORLD TO PROVIDE CONFIDENCE AND SECURITY FOR ELECTRONIC COMMERCE AND BUSINESS. THE ADMINISTRATION BELIEVES THAT THIS ENCRYPTION UPDATE PROMOTES SECURE ELECTRONIC COMMERCE, INCLUDING E-BUSINESS, MAINTAINS U.S. LEADERSHIP IN INFORMATION TECHNOLOGY, PROTECTS PRIVACY, WHILE CONTINUING TO PROVIDE ESSENTIAL PROTECTIONS FOR NATIONAL SECURITY AND PUBLIC SAFETY.

OUR POLICY ACKNOWLEDGES THESE VITAL INTERESTS, BUT EVEN AS WE DO, IT IS IMPERATIVE THAT WE UPHOLD INTERNATIONAL UNDERSTANDINGS, AND STRIVE WITH OTHER NATIONS TO PREVENT THE ACQUISITION OF ENCRYPTION TECHNOLOGY TO SPONSORS OF TERRORISM, INTERNATIONAL CRIME SYNDICATES OR THOSE ATTEMPTING TO INCREASE THE AVAILABILITY OF WEAPONS OF MASS DESTRUCTION. END SUMMARY.

### BACKGROUND

OVER THE PAST YEAR, THE PUBLIC DEBATE OVER ENCRYPTION POLICY HAS BEEN SPIRITED AND THERE HAS BEEN A FLURRY OF ACTIVITY REGARDING ENCRYPTION EXPORT CONTROLS. AS YOU MAY KNOW, LAST FALL, VICE PRESIDENT GORE ANNOUNCED A SERIES OF UPDATES TO THE ADMINISTRATION'S EXPORT CONTROL POLICY ON ENCRYPTION AND PROMISED TO REVISIT ENCRYPTION CONTROLS WITHIN A YEAR. IN LINE WITH THIS PROMISE, THE U.S. ADMINISTRATION WILL BE ANNOUNCING SEPTEMBER 16 AN UPDATE WHICH REPRESENTS A NEW FRAMEWORK FOR EXPORT CONTROLS THAT MEETS THE NEEDS OF INDUSTRY TO BE COMPETITIVE IN A GLOBAL MARKET PLACE WHILE CONTINUING TO PROVIDE ESSENTIAL PROTECTIONS FOR NATIONAL SECURITY AND PUBLIC SAFETY. THE ADMINISTRATION'S UPDATE ACKNOWLEDGES THESE VITAL INTERESTS AND CONTINUES TO SUPPORT A BALANCED APPROACH WHICH CONSIDERS PRIVACY AND COMMERCE AS WELL AS PROTECTING IMPORTANT LAW ENFORCEMENT AND NATIONAL SECURITY EQUITIES.

### UPDATE

#### *GLOBAL EXPORTS TO INDIVIDUALS, COMMERCIAL FIRMS OR OTHER NONGOVERNMENTAL ENTITIES*

ANY ENCRYPTION COMMODITY OR SOFTWARE OF ANY KEY LENGTH CAN NOW BE EXPORTED UNDER A LICENSE EXCEPTION (I.E., WITHOUT A LICENSE) AFTER A TECHNICAL REVIEW, TO COMMERCIAL FIRMS AND OTHER NONGOVERNMENT END USERS IN ANY COUNTRY EXCEPT FOR THE SEVEN STATE SUPPORTERS OF

TERRORISM. EXPORTS PREVIOUSLY ALLOWED ONLY FOR A COMPANY'S INTERNAL USE CAN NOW BE USED FOR COMMUNICATION WITH OTHER FIRMS, SUPPLY CHAINS AND CUSTOMERS. ADDITIONALLY, TELECOMMUNICATION AND INTERNET SERVICE PROVIDERS MAY USE ANY ENCRYPTION COMMODITY OR SOFTWARE TO PROVIDE SERVICES TO COMMERCIAL FIRMS AND NONGOVERNMENT END USERS. PREVIOUS LIBERALIZATIONS FOR BANKS, FINANCIAL INSTITUTIONS AND OTHER APPROVED SECTORS ARE SUBSUMED UNDER THIS UPDATE. EXPORTS TO GOVERNMENTS CAN BE APPROVED UNDER A LICENSE.

#### *GLOBAL EXPORTS OF RETAIL PRODUCTS*

RETAIL ENCRYPTION COMMODITIES AND SOFTWARE OF ANY KEY LENGTH MAY BE EXPORTED UNDER A LICENSE EXCEPTION (I.E., WITHOUT A LICENSE) AFTER A TECHNICAL REVIEW, TO ANY RECIPIENT IN ANY COUNTRY EXCEPT TO THE SEVEN STATE SUPPORTERS OF TERRORISM. RETAIL ENCRYPTION COMMODITIES AND SOFTWARE ARE THOSE PRODUCTS WHICH DO NOT REQUIRE SUBSTANTIAL SUPPORT FOR INSTALLATION AND USE AND WHICH ARE SOLD IN TANGIBLE FORM THROUGH INDEPENDENT RETAIL OUTLETS, OR PRODUCTS WHICH HAVE BEEN SPECIALLY DESIGNED FOR INDIVIDUAL CONSUMER USE AND ARE TRANSFERRED BY TANGIBLE OR INTANGIBLE MEANS. THERE IS NO RESTRICTION ON THE USE OF THESE PRODUCTS. ADDITIONALLY, TELECOMMUNICATION AND INTERNET SERVICE PROVIDERS MAY USE RETAIL ENCRYPTION COMMODITIES AND SOFTWARE TO PROVIDE SERVICES TO ANY RECIPIENT.

#### *IMPLEMENTATION OF THE DECEMBER 1998 WASSENAAR ARRANGEMENT REVISIONS*

LAST YEAR, THE WASSENAAR ARRANGEMENT (THIRTY THREE COUNTRIES WHICH HAVE COMMON CONTROLS ON EXPORTS, INCLUDING ENCRYPTION) MADE A NUMBER OF CHANGES TO MODERNIZE MULTILATERAL ENCRYPTION CONTROLS. AS PART OF THIS UPDATE, THE U.S. WILL ALLOW EXPORTS WITHOUT A LICENSE OF 56 BITS DES AND EQUIVALENT PRODUCTS, INCLUDING TOOLKITS AND CHIPS, TO ALL USERS AND DESTINATIONS (EXCEPT THE SEVEN STATE SUPPORTERS OF TERRORISM) AFTER A TECHNICAL REVIEW. ENCRYPTION COMMODITIES AND SOFTWARE WITH KEY LENGTHS OF 64-BITS OR LESS WHICH MEET THE MASS MARKET REQUIREMENTS OF WASSENAAR'S NEW CRYPTOGRAPHIC NOTE WILL ALSO BE ELIGIBLE FOR EXPORT WITHOUT A LICENSE AFTER A TECHNICAL REVIEW.

#### *U. S. SUBSIDIARIES*

FOREIGN NATIONALS WORKING IN THE UNITED STATES NO LONGER NEED AN EXPORT LICENSE TO WORK FOR U.S. FIRMS ON ENCRYPTION. THIS EXTENDS THE POLICY ADOPTED IN LAST YEAR'S UPDATE, WHICH ALLOWED FOREIGN NATIONALS TO WORK FOR

FOREIGN SUBSIDIARIES OF U.S. FIRMS UNDER A LICENSE EXCEPTION (I.E., WITHOUT A LICENSE).

#### **EXPORT REPORTING**

POST-EXPORT REPORTING WILL NOW BE REQUIRED FOR ANY EXPORT TO A NON-U.S. ENTITY OF ANY PRODUCT ABOVE 64 BITS. REPORTING HELPS ENSURE COMPLIANCE WITH OUR REGULATIONS AND ALLOWS US TO REDUCE LICENSING REQUIREMENTS. THE REPORTING REQUIREMENTS WILL BE STREAMLINED TO REFLECT BUSINESS MODELS AND PRACTICES, AND WILL BE BASED ON WHAT COMPANIES NORMALLY COLLECT. WE INTEND TO CONSULT WITH INDUSTRY ON HOW BEST TO IMPLEMENT THIS PART OF THE UPDATE.

#### **CYBERSPACE ELECTRONIC SECURITY ACT (CESA)**

THIS ANNOUNCEMENT WILL ALSO BE ACCOMPANIED BY A DRAFT BILL, THE CYBERSPACE ELECTRONIC SECURITY ACT (CESA), WHICH WILL BE SUBMITTED TO CONGRESS. CESA PROVIDES IMPORTANT NEW PRIVACY PROTECTIONS FOR OUR CITIZENS WHO USE STRONG ENCRYPTION TOOLS TO PROTECT THEIR INFORMATION AND NARROWLY TAILORED PROVISIONS TO ASSIST THE GOVERNMENT IN PROTECTING THE PUBLIC SAFETY. CESA DOES NOT RESTRICT OR REGULATE THE DOMESTIC USE OF STRONG ENCRYPTION. THE ADMINISTRATION UNDERSTANDS THAT ENCRYPTION IS ESSENTIAL FOR LAW-ABIDING CITIZENS TO COMMUNICATE SECURELY. AS ENCRYPTION BECOMES MORE WIDESPREAD, HOWEVER, CRIMINALS WILL ALSO TAKE ADVANTAGE OF THE NEW TECHNOLOGY. WITH STRONG ENCRYPTION, DRUG DEALERS OR OTHER CRIMINALS CAN KEEP EXTENSIVE RECORDS ON THEIR COMPUTER HARD DRIVES, SAFE IN THE KNOWLEDGE THAT THESE INCRIMINATING RECORDS WILL BE UNREADABLE IF THE COMPUTER IS EVER SEIZED. EVEN MORE DISTURBINGLY, CRIMINAL AND TERRORIST NETWORKS CAN USE STRONG ENCRYPTION FOR THEIR E-MAILS, PHONE CALLS, AND OTHER COMMUNICATIONS WITHIN THE UNITED STATES AND ABROAD.

WHILE CESA DOES NOT REQUIRE ANYONE TO STORE THEIR KEYS WITH THIRD PARTIES, ITS KEY RECOVERY AGENT AND GOVERNMENTAL ACCESS PROVISIONS DO PROVIDE SPECIAL PROTECTIONS WHEN THEY DO. THIS WILL HELP TO ENSURE TRUSTED RELATIONSHIPS IN A NUMBER OF WAYS. FIRST, THROUGH THE USE OF CIVIL AND CRIMINAL PENALTIES, CESA GREATLY RESTRICTS WHAT OUTSIDE COMPANIES -- KEY RECOVERY AGENTS -- MAY DO WITH A CUSTOMER'S KEY AND PROHIBITS THESE AGENTS FROM SELLING INFORMATION ABOUT THEIR CUSTOMERS TO THIRD PARTIES. SECOND, CESA STRICTLY LIMITS THE GOVERNMENT'S ACCESS TO KEYS STORED WITH KEY RECOVERY AGENTS IN FAMILIAR, CONSTITUTIONALLY GROUNDED WAYS SUCH AS THROUGH THE USE OF NARROWLY APPLIED COURT ORDERS AND SEARCH WARRANTS.

THE EARLIER CESA DRAFT THAT RECEIVED MUCH MEDIA

ATTENTION, CONTAINED A PROVISION FOR SEARCH WARRANTS THAT COULD BE USED BY THE GOVERNMENT TO ACQUIRE KEYS FROM A SUBJECT AND WAIT TO NOTIFY THEM FOR A REASONABLY SHORT PERIOD OF TIME. THAT PROVISION HAS BEEN REMOVED. THE ADMINISTRATION BELIEVES THAT SUCH AUTHORITIES MAY BE IMPORTANT, BUT IS TAKING THIS FIRST STEP WITHOUT THEM AND WILL WAIT TO SEE WHAT IMPACT THE WIDESPREAD USE OF STRONG ENCRYPTION BY CRIMINALS HAS ON THE ABILITY OF LAW ENFORCEMENT TO ENSURE PUBLIC SAFETY AND HOW SUCH AN IMPACT SHOULD BE ADDRESSED.

ALONG WITH THE EXPORT CONTROL UPDATES, WE ARE CONFIDENT THAT CESA WILL PROVIDE A SOLID FRAMEWORK WITHIN WHICH OUR CITIZENS AND INDUSTRY CAN CONTINUE TO ENJOY STRONG PRIVACY PROTECTIONS AND WORLDWIDE INFORMATION TECHNOLOGY LEADERSHIP AS WE MOVE INTO THE 21ST CENTURY. AT THE SAME TIME THEY MAY BE COMFORTED IN KNOWING THAT THEIR SAFETY CAN BE MAINTAINED WITHOUT ENDANGERING OUR CHERISHED VALUES OF CIVIL LIBERTIES AND PRIVACY FROM OVER BROAD GOVERNMENT POWERS.

AMERICA'S NATIONAL SECURITY WILL INCREASINGLY DEPEND ON STRONG AND CAPABLE LAW ENFORCEMENT ORGANIZATIONS. THE NEW FRAMEWORK FOR EXPORT CONTROLS MUST BE COMPLEMENTED BY PROVIDING UPDATED TOOLS FOR LAW ENFORCEMENT.