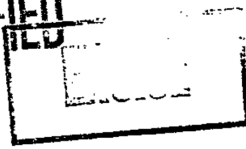


379

~~SECRET~~

UNCLASSIFIED



P
/ P

CIA/NHRTC - SMMORREL
07/02/93 - 703 482-6915
PM/DTP -

INR/IL -
EB/CIP -

EAP/RA -
NEA/RA -
EUR/P -

IMMEDIATE BEIJING, TEL AVIV IMMEDIATE, NEW DELHI
IMMEDIATE, DAMASCUS IMMEDIATE, ISLAMABAD IMMEDIATE+
ROUTINE CIA WASHDC//NHTC//NIC//OSWR, NSC WASH DC,
REUTIAA/DIRNSA WASHDC

E.O. 12356: DECL: OADR
TAGS: ETRD, ETTG, PINR, TSPL, KSTC
SUBJECT: (U) ENCRYPTION TECHNOLOGIES

DEPARTMENT OF STATE
9403964
IS/FPC/CID
Date: MAY 30 1997

() REVIEW
() EXEMPT
() DECLASSIFIED
FOIA Ex. 1(b)(7) - (D) 1551
PA Exempt 1003

TS authority to:
() S or () C OADR
include TS to () S or () C OADR

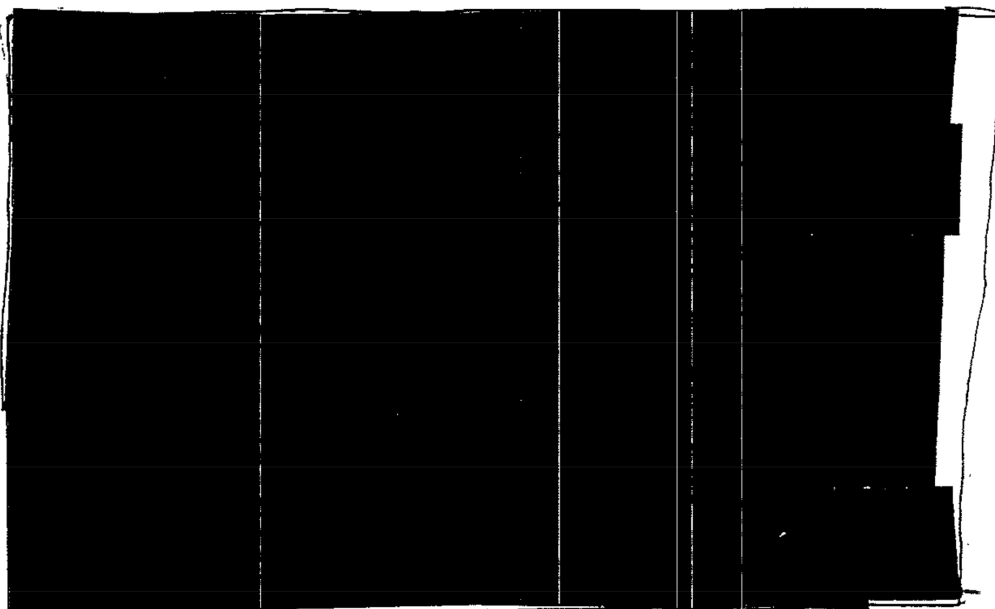
UNCLASSIFIED

~~SECRET~~

~~SECRET~~
2
UNCLASSIFIED

REF: STATE 141145

1. (U) SUMMARY & ACTION REQUESTED. THIS MESSAGE REQUESTS POSTS TO PROVIDE INFORMATION BY JULY 23 ON HOST GOVERNMENT LAWS AND POLICIES REGARDING ENCRYPTION AS A KEY INPUT TO THE ON-GOING NSC STUDY OF USG POLICY ON COMMERCIAL ENCRYPTION. QUESTIONS FOR RELEVANT HOST GOVERNMENT OFFICIALS ARE IN PARA 4 BELOW. BACKGROUND FOR POSTS' INFORMATION ON THE ISSUE IS IN PARAS 5-9. END SUMMARY.



15 b,d

4. (U) THE FOLLOWING ARE KEY QUESTIONS:

A. REACTION TO THE CLIPPER PROPOSAL

TO WHAT EXTENT HAS THE CLIPPER PROPOSAL BEEN DISCUSSED AT VARIOUS LEVELS OF THE FOREIGN GOVERNMENT, OR WITHIN INDUSTRY?

ARE CLIPPER DEVICES LIKELY TO BE PERMITTED FOR IMPORTATION AND USE IN THE HOST COUNTRY? IF SO, WOULD THERE BE MUCH OF A DEMAND FOR CLIPPER DEVICES? WOULD THE

UNCLASSIFIED ~~SECRET~~

~~SECRET~~
UNCLASSIFIED

HOST COUNTRY DEMAND JOINT KEY HOLDING, OR EXCLUSIVE RIGHTS TO CLIPPER KEYS?

IS THE CLIPPER PROPOSAL LIKELY TO STIMULATE BROADER USE OF AN INDIGENOUSLY DEVELOPED ENCRYPTION TECHNOLOGY?

B. GENERAL POLICY ON PUBLIC ENCRYPTION

IS INDUSTRY, GOVERNMENT, OR THE PUBLIC CONCERNED ABOUT CURRENT LACK OF COMMUNICATIONS SECURITY?

WHAT LAWS OR REGULATIONS CONTROL ENCRYPTION (SOFTWARE OR HARDWARE) FOR CIVILIAN USE? HOW ARE THEY ENFORCED? WHAT STANDARDS OR SYSTEMS, IF ANY, ARE UNDER CURRENT DISCUSSION FOR COMMUNICATIONS SECURITY?

HOW MIGHT CURRENT POLICIES CHANGE, IF WIDESPREAD COMMUNICATIONS ENCRYPTION IS IMPLEMENTED IN THE US? IS THERE A POSSIBILITY OF A CRYPTOGRAPHY "RACE"? WHAT CONCERNS ARE THERE OVER THE NEED TO ESTABLISH INTERNATIONAL SECURE COMMUNICATIONS STANDARDS?

C. ECONOMIC/TRADE ISSUES

WHAT IS THE CURRENT AND FUTURE MARKET IN THE HOST COUNTRY FOR SECURE CIVILIAN COMMUNICATIONS SERVICES? WHAT IMPORT AND EXPORT REGULATIONS EXIST CONCERNING SECURE COMMUNICATIONS SYSTEMS?

WHAT ARE INDUSTRY'S PLANS FOR MARKETING SECURE COMMUNICATIONS DEVICES? WHAT DO THEY SEE AS THE LARGEST MARKETS FOR ENCRYPTION (BOTH GEOGRAPHIC AND APPLICATIONS AREAS)?

END QUESTIONS.

(U) PUBLIC ENCRYPTION MANAGEMENT: BACKGROUND

5. (U) NEW DEVELOPMENTS IN TELECOMMUNICATIONS HOLD GREAT PROMISE FOR THE AMERICAN ECONOMY--ITS PRODUCTIVITY AND GLOBAL COMPETITIVENESS. BUT THEY ALSO POSE RISKS TO THE U.S. GOVERNMENT'S ABILITY TO ENFORCE LAWS AND PROTECT NATIONAL SECURITY. SPECIFICALLY, A WAVE OF NEW, INEXPENSIVE, COMMERCIALY AVAILABLE ENCRYPTION PRODUCTS FOR MASS TELECOMMUNICATIONS HAS CAUSED THE ADMINISTRATION, WITH SOME URGENCY, TO SEEK NEW WAYS TO ACCOMMODATE THE GOVERNMENT'S INTERESTS IN PRIVACY.

~~SECRET~~
UNCLASSIFIED

UNCLASSIFIED

4

PRODUCTIVITY, COMPETITIVENESS, LAW ENFORCEMENT AND NATIONAL SECURITY. IN APRIL, THE PRESIDENT DIRECTED THAT A THOROUGH STUDY OF BROAD TELECOMMUNICATIONS AND ENCRYPTION ISSUES BE COMPLETED FOR THE PURPOSE OF DETERMINING THE LEAST BURDENSOME AND MOST EFFECTIVE METHODS OF MAINTAINING OUR CURRENT CAPABILITIES TO CONDUCT LEGALLY-AUTHORIZED AND EFFECTIVE COMMUNICATIONS INTERCEPTS AND TO CONTROL ENCRYPTION EXPORTS.

6. (U) THE US GOVERNMENT RECENTLY DEVELOPED A MICROCIRCUIT (OFTEN REFERRED TO AS THE "CLIPPER CHIP") WHICH IS PROPOSED FOR WIDESPREAD USE IN CIVILIAN SECURE COMMUNICATIONS, INCLUDING CELLULAR TELEPHONES, FAX, AND COMPUTER DATA LINKS. THE CLIPPER CHIP NOT ONLY PROVIDES PRIVACY THROUGH ENCRYPTION THAT IS SUBSTANTIALLY MORE ROBUST THAN THE CURRENT GOVERNMENT STANDARD, BUT ALSO PERMITS ESCROWING OF THE KEYS NEEDED TO UNLOCK THE ENCRYPTION. [THE SYSTEM FOR THE ESCROWING OF KEYS WILL ALLOW THE GOVERNMENT TO GAIN ACCESS TO ENCRYPTED INFORMATION ONLY WITH APPROPRIATE LEGAL AUTHORIZATION.]

7. (U) THE CLIPPER PROPOSAL HAS GENERATED AN ACTIVE AND PUBLIC DIALOGUE AMONG US CIVIL LIBERTARIAN GROUPS, INDUSTRY REPRESENTATIVES, AND THE GOVERNMENT. THE COMMERCIAL SECTOR IS PRIMARILY CONCERNED ABOUT INDUSTRIAL ESPIONAGE AND THE VULNERABILITY OF US BUSINESS COMMUNICATIONS, PARTICULARLY OVERSEAS. TELECOMMUNICATIONS AND SOFTWARE COMPANIES ARE CONCERNED THAT THE PROPOSAL MIGHT JEOPARDIZE THE POTENTIAL MULTI-BILLION DOLLAR EXPORT MARKET FOR US-MANUFACTURED SECURE COMMUNICATIONS EQUIPMENT. WITHIN THE GOVERNMENT, LAW ENFORCEMENT AGENCIES ARE CONCERNED ABOUT THE POTENTIAL LOSS OF THEIR ABILITY TO EXECUTE LEGALLY-AUTHORIZED WIRETAPS, FOR EXAMPLE, TO COUNTER INTERNATIONAL NARCOTICS TRADE.



1.5 b.d

9. (U) ALTHOUGH WE KNOW THAT A NUMBER OF COUNTRIES TODAY HAVE VARYING REGULATIONS WITH REGARD TO THE IMPORT, EXPORT, AND USE OF ENCRYPTED COMMUNICATIONS (REFTEL), WE KNOW VERY LITTLE ABOUT FOREIGN GOVERNMENT AND INDUSTRY PLANS TO DEAL SPECIFICALLY WITH THE CLIPPER PROPOSAL, AND MORE GENERALLY, WITH ADVANCING ENCRYPTION TECHNOLOGIES.

UNCLASSIFIED

~~SECRET~~

5

UNCLASSIFIED

THE US GOVERNMENT HAS LARGE EQUITIES AT STAKE, AND ACCURATE ASSESSMENTS OF CURRENT AND FUTURE FOREIGN SECURE COMMUNICATIONS POLICIES ARE NEEDED AS A VITAL INPUT TO THE IMPORTANT POLICY REVIEW STILL UNDERWAY.

44

SINGAPORE IMMEDIATE
AIT TAIPEI IMMEDIATE
MOSCOW IMMEDIATE
COCOM IMMEDIATE
XMT REYKJAVIK
LUXEMBOURG
HELSINKI
DUBLIN
OTTAWA
LONDON
BERLIN
USNATO .

Sweden
Germany

UNCLASSIFIED
UNCLASSIFIED
UNCLASSIFIED

~~SECRET~~