February 9, 1993

Mr. George J. Tenet
Special Assistant to the President
Senior Director for Intelligence Programs
National Security Council
Old Executive Office Building
Suite 300
Washington, D.C.

Dear Mr. Tenet:

As a result of a briefing to you on January 26, 1993, by James Kallstrom and others you requested that several encryption related issues be more fully developed and described. These were: the "Clipper" methodology (and particularly the identification of key custodian candidates); approaches and methodologies to deal with other encryption applications; and identification of and greater detail regarding international aspects and issues of encryption.

Attached please find a briefing document concerning the first matter mentioned above, entitled "Clipper Encryption - AT&T Telephone Security Device Model 3600," XXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXX BLACKED OUT AS STILL SECRET XXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXX PER NSA XXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

We hope that that information provided in the attached briefing document is useful for you and your staff and other in reviewing and acting upon the issues identified therein. Further, we are preparing at your request to provide any additional information or details you deem necessary in order to address this matter.

Sincerely yours,

William S. Sessions
Director

Enclosure
1 - Mr. Clarke
1 - Mr. Kennedy
1 - Mr. Gow
1 - Mr. Collingwood
1 - Mr. Potts
1 - Mr. Gilbert
1 - Mr. Bayse
1 - Mr. McDonald
1 - Mr. Kallstrom
1 - Mr. Allen
1 - XXXXXXXXXXX
JKK:XXXXXXX (12)

CLIPPER ENCRYPTION
AT&T TELEPHONE SECURITY DEVICE
MODEL 3600

Executive Summary

I. Background - AT&T TSD-3600

II. Clipper Program

A. Program Methodology

1. Basis
2. Functional Overview
3. Encryption Algorithm

B. Program Procedures

1. Facilities & Security
2. Seed Key Creation
3. Composite Key Generation
4. Clipper Chip Programming
5. Split Key Procedures

C. Operational Procedures

1. Legal Process
2. Law Enforcement Access

D. Program Management

1. Clipper Program Management
2. Seed Key Creators
3. Split Key Custodians

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXX PARAGRAPH BLACKED OUT XXXXXXXX
XXXXXXXXX AS STILL SECRET NSA XXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

III. Policy Issues/Action

A. XXXXXXXXXXXX BLACKED OUT AS SECRET NSA XXXXXXXXXXXXXXX

B. ISSUES

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXX PARAGRAPH BLACKED OUT XXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXX AS STILL SECRET NSA XXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

C. ACTIONS

A. APPENDIX

SECRET

EXECUTIVE SUMMARY

By April 1, 1993, AT&T will have produced 10,000 "TSD 3600" voice encryption devices which, as manufactured, employ Data Encryption Standard (DES) encryption. These devices are portable, user-friendly and relatively inexpensive, and they can be used with any hardwired telephone.   XXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXX LINES BLACKED OUT AS STILL SECRET XXXXXXXXXXX
XXXXXXXXXXXXXX AS PER NSA XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Contemporaneous with AT&T's fielding of the TSD 3600 devices, the National Security Agency (NSA) has developed a new encryption methodolgy and computer chip which affords encryption strength vastly superior to DES, yet which allows for real time decryption by law enforcement, acting pursuant to legal process. It is referred to as "Clipper."

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXX PARAGRAPH BLACKED OUT AS XXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXX STILL SECRET PER NSA   XXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXX PARAGRAPH BLACKED OUT AS XXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXX STILL SECRET PER NSA   XXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
if the devices are modified to include the "Clipper" chip, they would be of great value to the Federal, state and local law enforcement community, especially in the area of counter

SECRET

narcotics, investigations, where there is a requirement to routinely communicate in a secure fashion. The modified TSD 3600s satisfy the existing need for user-friendly, interoperable, secure telecommunications devices.

The approximate cost of each TSD 3600 device to the Government is $1,000, which is about half the cost of Secure Telephone Unit (STU) devices commonly used by Government agencies for similar purposes. Th total cost to purchase 9,000 TSD devices would be approximately $9 million. The chief candidate for funding has been the Department of Justice Asset Forfeiture Super Surplus Fund. It should be noted that obligation or expenditure of these funds through a reprogramming requires that the Congressional appropriations committees be notified 15 days in advance of such reprogramming of funds.

The unique "Clipper" encryption methodology accomodates both public and governmental needs. Each "Clipper" chip bears a unique number or key, to facilitate decryption, that is generated by isinterested parties in a system amendable in idependent public verification. To ensure security, the key is "split" into two parts, with tow independent Government or private entities or custodians each holding only one part. Those two entities would then provide law enforcement with their part of the key only pursuant to court orders or authorizations specificied in Federal or state statutes pertaining to electronic surveillance.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXX MATERIAL BLACKED OUT AS XXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXX STILL SECRET PER NSA   XXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXX Once this information was obtained, the key information could be reconstructed and law enforcement could initiate decryption.

The "Clipper" methodology envisions the participation of three distinct types of parties. XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXX MATERIAL BLACKED OUT AS XXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXX STILL SECRET PER NSA   XXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
It is proposed that the second party, the two custodians of the "split" key infostructure, be comprised of two disinterested and trustworthy non-law enforcement Government agencies or entities. Although, such decision and selection are left for the Administration, a list of reccommended agencies and entities has been prepared (and included in the text), XXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXX This party would administer and oversee all facets of the "Clipper" program and methodology.

I. Background - AT&T Telephone Security Device

In mid 1992, AT&T concluded testing on a new encryption product, the Telephone Security Device (TSD) 3600 model. This device employs DES (Data Encryption Standard) based encryption technology in a portable device which can be connected to any hardwire telephone instrument. The technology of the AT&T device is such that it is superior to and more user friendly than similar telephone encryptino devices, and it is approximately half the price of such similar devices XXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

XXXXXXXXXXXXXX PARAGRAPH BLACKED OUT AS XXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXX STILL SECRET PER NSA   XXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

In November, 1992, then Attorney General William P. Barr recused himself regarding this matter and delegated the responsibility of dealing with AT&T and this issue to the Director, FBI XXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXX PARAGRAPH BLACKED OUT AS XXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXX STILL SECRET PER NSA   XXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXX PARAGRAPH BLACKED OUT AS XXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXX STILL SECRET PER NSA   XXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

SECRET

The Director, FBI, also concluded that this device, if modified with "Clipper", could provide outstanding voice encryption support for the FBI and other Federal, state and local agencies with whom there is a need to routinely communicate in a secure fashion, particularly in the area of counternarcotics.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXX PARAGRAPH BLACKED OUT AS XXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXX STILL SECRET PER NSA   XXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
Thus, AT&T will produce 9,000 TSD devices for Government purchase by April 1, 1993.

AT&T has advised that the unit cost to the Government of the TSD 3600 device, employing either DES or "Clipper" chip encryption. would be approximately $1,000. This cost is roughly half that which the FBI currently expends for STU type devices (approximately $2,000 per unit). Hence, the total cost for the purchase of 9,000 units at approximately $1,000 per unit will be $9 million. Although sevearl funding options are available the chief candidate has been the Department of Justice (DOJ) Asset Forfeiture Super Surplus Fund. It should be noted that obligation or expenditure of these funds through a reprogramming requires that the Congressional appropriations committees be notified 15 days in advance of such reprogramming of funds.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXX PARAGRAPH BLACKED OUT AS XXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXX STILL SECRET PER NSA   XXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

SECRET

II. Clipper Program

A. PROGRAM METHODOLOGY

1. Basis

The development of the CLIPPER encryption methodology by the National Security Agency (NSA), at the request of the Department of Justice, is based up a recognition that affordable, user-friendly, and highly secure encryption products are increasingly being developed and fielded by voice and data communication services and by vendors closely aligned with them.
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXX paragraph blacked out as TOP SECRET by NSA XXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

SECRET

2. Functional Overview

The Clipper chip provides law enforcement access by using a special chip key, unique to each device. In the AT&T TSD 3600, a unique session key is generated, external to the Clipper chip for each call. This session key is given to the chip to control the encryption algorithm. A device unique "chip key" is programmed into each Clipper at the time of manufacture. When two TSD 3600s go to secure operation, the device gives out its identification (ID) number and the session key encrypted in its chip key. Anyone with access to the chip key for that identified device will be able to recover the session key and listen to the transmission simultaneously with the intended receiver. This design means that the list of chip keys associated with the chip ID number provides access to all Clipper secured devices, and thus the list must be carefully generated and protected. Loss of the list would preclude legitmate access to the encrypted information and compromise of the list could allow unauthorized access.

The NSA developed chip based "Clipper" solution works with hardware encryption applications, such as those which might be used with regard to certain telecommunications and computers devices. The "Clipper" encryption methodolgy has unique components. In general, these components involve the creation of two initial (or "seed") keys XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXX the generation of combined programming key ("the identification number with the key; the programming of the computer chip; XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXX seperate key custody of the split keys (preferably carried out by two disinterested , non-law enforcement Government entities); and a "Clipper" progoram manager to oversee this process. This methodology ensure that user can be completely confident that their encrypted communications cannot be decrypted, even by the Government, absent traditional electronic surveillance legal process which would then permit law enforcement's reconstruction of the key information.

Under the "Clipper" encryption methodology, it is reccommended that three disctince types of parties be involved; (1) XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXX (2) two Government agencies or entities who each serve as custodians of one part of the split key information; and (3) a Government program manger who oversees (a) the creation of seed keys, (b) the generation of a combined key (and programming of computer chips with the key information and appropriate identifiers) XXXXXXXXXXXXXXXXXXX and (c) the secure distribution and custodial storage of the split key information.

3. Encryption Algorithm

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX The cryptographic strength of the "Clipper" algorithm is very substantial and should be highlighted. With regard to the AT&T TSD 3600 device and other similar devices, these vendors almost exclusively employ DES encryption. Des encryption is based upon the use of 56-bit key information. "Clipper" employs an algorithm which is based upon an 80 bit key. Although only 24 bits longer, "Clipper" encryption provides for 16 million times as many permuntations which makes it geometrically more difficult to decrypt. This fact is a critical counterpart to the encryption methodology and makes "Clipper" encryption attractive.

SECRET

B. PROGRAM PROCEDURES

In order to receive public acceptance and install confidence in the vendors and users of computer chips produced pursuant to this methodology, the procedures employed by the 'Clipper" encryption methodology must be rigorous and flawless. The methodology must not only be flawless, it must also create a strong perception that it is faultless.

1. Facility and Security

The current plans are to physically carry out the "Clipper" programming procedures, at least initially, on the premises of Mykotronx, Inc. (the company which produces the "Clipper" Chip) within a specially created Sensitive Compartmentalized Information Facility (SCIF). It is proposed that the entire procedure be administered and overseen by the program mananger (below). Access to the SCIF will be strictly monitored by employing top level security procedures and limited to necessary parties (below). XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

2. "Seed" Key Creation

The first activitiy component of the "Clipper" encryption methodology is the creation of the "seed" keys. XXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX Each entity, uitilizing a seperate lap top computer will create an 80 bity random number of "seed" key on a floppy disk. The two seed keys created by these entities on their respective floppy disks will immediately be taken to a single computer work station for the purpose of generating a final composite key.

3. Composite Key Generation.

The foregoing kes are taken to a single computer workstation to be processed and to produce a final key ("the key"). In this process, the two independently created 80 bit "seed" keys are integrated into a new composite 80 bit programming key. After the programming key is created, the original seed key information and floppy disks are destroyed.

4. "Clipper" Chip Programming

After the new 80 bit programming key has been generated, the key information is ready to be programmed into a computer chip (the "Clipper" chip). In this process, a prelimnary test will be performed to make sure that each chip functions properly and is not defective. The programming key is used to generate a unique chip key for each chip. After a properly functions chip is cleared for use, the chip key information is embedded into the chip, along with unique information which identifies the device and serial number of the chip. At the conclusion of this process, the producer or purchaser of the chip takes possession of the "Clipper" computer chip.

5. Split Key Procedures.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXX PARAGRAPH BLACKED OUT AS XXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXX STILL SECRET PER NSA   XXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX residual memory including the key information, located in the workstation will be destroyed at the conclusion of each programming session.

C. OPERATIONAL PROCEDURES

1. Legal Process

Although, self evident to most, eveyone should understand that the "split" key information retain in part by each of the two custodians will never be disclosed to anyone absent legal authority. Such authority is exclusively found in the Federal and state electronic surveillance statutes (e.g. Title III and FISA), which only permit electronic survillance to be conducted pursuant to court order or a recognized statutorily based authorization, ie., emergency Title III (18 USC 2518 (7)). The two government custodians would, like providers of electronic communications services, landlords, custodians and others, be subject to the "assistance" provisions found in Title III and FISA. The assistance provisions state, in part, that when directed by the court (pursuant to a secondary court order) a person shall "furnish the applicant forthwith all information, facilities and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that such service provider, landlord, custodian or person in according the person whose communications are to be intercepted."

2. Law Enforcement Access

As stated above, the two Governmental custodians will only disclose their portion of the split key information pursuant to being served with legal process (court order or statutory authorization).

In a typical scenario, a Title III or FISA court order would have been obtained by a law enforcement entity. XXXX XXXX XXXX
XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX
XXXX sentence and paragraph remains classified by NSA XXXX
XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX
XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX

XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX
XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX
XXXX XXXX paragraph blacked out as classified XXXX XXXX XXXX
XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX
XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX

At this point and thereafter, for the duration of the period authorized in the court order, real time decryption could occur. (see appendix).

Appendix remains classifed by NSA.

Return to the Clipper Papers Page