SECRET

U.S. Justice Department
Federal Bureau of Investigation

February 19, 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:

Reference my letter dated February 9 , 1993

Attached please find a briefing document entitled "Encryption: The Threat, Applications, and Potential Solutions," which responds to your request for additional information concerning the various encryption applications now being used and the potential approaches and methodologies to deal with them. As set out in referenced letter, this is the second of three subject areas you requested to have more fully developed and discussed. XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXX BLACKED OUT AS STILL SECRET XXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXX PER NSA XXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX This document is the product of a working group, comprimised of representatives of the Federal Bureau of Investigation, NSA and the Department of Justice.

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

Sincerely yours,

William S. Sessions
Director

1 - Director NSA

SECRET

~~~~~~

TOP SECRET
~~~~~~

INTRODUCTION

The successful conduct of electronic surveillance is crucial to effective law enforcement, to the preservation of the public safety, and to the maintenance of the national security. Recent advances in communications technology, particularly telecommunications technology, and the increased availability and use of encryption threaten to significantly curtail, and in many instances preclude, effective law enforcement XXXXXXXXXXXX XXXXX - LINE BLACKED OUT PER NSA AS STILL TOP SECRET XXXXXXXXXX Efforts have been made to develop, where available, technical solutions to the problems posed by advanced communications technologies and encryption in order to preserve the electronic surveillance technique.

XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXXXXXXX - BLACKED OUT PER NSA AS STILL TOP SECRET XXXXXXXXXXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX

Encryption is, or can be used in a number of applications to secure voice and data communications and stored information. The type of encryption used and the way it is implemented varies depending upon the nature of the application. Encryption applications are available to secure communications transmitted both in analog and digital formats. Digital communications, in particular, support and accommodate the use of encryption. Thus, encryption can be, and is, employed easily and inexpensively in computer based applications. To date, its use has been somewhat limited in certain areas such as in voice communications XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXXXXXXX - BLACKED OUT PER NSA AS STILL TOP SECRET XXXXXXXXXXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX However, as the transition proceeds from analog telephony to digital telephony, and as consumers migrate from wireline (e.g., basic telephone) to wireless (e.g., cordless or cellular telephone) communications devices, the use of encryption by telecommunications service providers and end-users can be expected to increase markedly in the near future. Hence, it is expected that encryption will soon be more widely available and more widely used with all communications applications.

This document responds to a National Security Council (NSC) request for additional information concerning the use of encryption in the various communications and information applications. Additionally, this document briefly describes potential technical and legislative solutions to the problems posed by the various encryption applications.

By letter dated February 9, 1993, from FBI Director William S. Sessions to Special Assistant to the President George Tenet, NSC, a detailed discussion of the "Clipper" encryption methodology was provided. The "Clipper" hardware (chip) based technical solution was discussed in the context of the AT&T TSD 3600 telephone encryption device. It was noted in the enclosed document to that communication that the "Clipper" chip methodology provided a solution to various hardware-based encryption applications (such as telecommunications, data or pure storage). Consequently, in this document, discussion of the

capability and methodology of "Clipper" and its efficacy in providing a hardware-based technological solution will be abbreviated.

Wireless telecommunications devices, such as cordless telephones and celluar telephones, however are vulnerable to unauthorized interception, as some recent cases of renown (e.g. the Governor Wilder case) demonstrate. Consequently, there is a fundamental need to apply some form of enhanced security to wireless telephone devices. As a result, there appears to be a widespread and growing recognition that additional security features, such as encryption, need to be incorporated into these devices. In this vein, the Privacy and Technology Task Force submitted a report in May 1991 to Senator Leahy, the Chairman of the Subcommittee on Privacy and Technology, Seantore Judiciary Committee, which recommended that cordless telephones be afforded privacy protection under Title III (cordless telephones currently are not statutorily protected because of the ease with which they can be intercepted). The Task Force noted that is is projected that cordless phones will be in 68% of American households by the end of the decade (the year 2000). The report also states that a number of task force members indicated that "technical privacy enhancing featuers for radio based systems should be more rapidly deployed by manufacturers and service providers." Currently, AT&T, Motorola, and other service providers and manufacturers are offering encryption for cellular devices or service.

Law enforcement's decryption requirements, particularly real time intelligibility of communications content, are the same for wireless and wireline voice communications. Also, as noted the area of wireless telecommunications. Hence, a solution to the threat posed by encryption in wireless, as well as wireline, devices is imperative.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXX PARAGRAPH BLACKED OUT AS XXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXX STILL SECRET PER NSA   XXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

APPLICATIONS

PC communications, including E-mail, increasingly are being used not only by businesses but also by indivduals. In 1992, approximately 19 million E-Mail users sent nearly 15 billion messages. With increased computer networking and with the recent acceptance of new E-mail standards, electronic messaging will increase dramatically. Existing E-mail standards generally support text transmissions, however, emerging E-mail systems can support voice, facsimile and video capabilities. These electronic communications are fast replacing real-time voice conversations and consequently will increasingly become the subject of electronic surveillance. As these types of communications are more frequenctly and widely used, the use of encryption to protect the communication content can be expected

to increase.

Low speed data transmissions typically run at speeds less than 64 thousand bits of information per second (64Kb/s). The use of encryption of these low speed applications can be either software or hardware based. With respect to certain data communcations such as facsimile and E-mail, law enforcement typically requires real-time access to these communications, the the same way as it does for voice communications.

For the above mentioned data applications and others XXXXXXX - sentence blacked out as per NSA XXXX - Classified XXXXXX. However, software based encryption is more widely used in these low speed data transmission-related applications for the reasons previously discussed: cost and ease of use. Encryption for functions such as E-mail and individual (non-bulk) file transfers across a local area network (LAN) can be provided and typicallly is provided, as part of a communications software package. Thus, this encryption is essentially free to mass market software publishers as previously discussed. XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXXXXX - remaining paragraph blacked out as per NSA - XXXX XXXX Classified XXXXXXX.

Voice/Data Applications
XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXXXXX - Paragraph blacked out as per NSA - XXXX XXXX Classified XXXXXX. XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX

- Real time access to and decryption of voice/data communications secured by software-based encryption XXXX XXXX XXXX XXXXXXX - Paragraph blacked out as per NSA - XXXX XXXX Classified XXXXXX. XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX in the near future. XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXXXXX - Paragraph blacked out as per NSA - XXXX XXXX Classified XXXXXX. XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX

Stored Information Applications

- Real time access to and decryption of stored electronic information secured by hardware based encryption could be performed utilizing the Clipper technique.

XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXXXXX - Paragraph blacked out as per NSA - XXXX XXXX Classified XXXXXX. XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX

XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXXXXX - Paragraph blacked out as per NSA - XXXX XXXX Classified XXXXXX. XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX

- Technical solutions, such as they are, will only work if they are incorporated into all encryption products. To ensure that this occures, legislation mandating the use of Government approved encryption products or adherence to Government encryption criteria is required.

HIGH SPEED DATA TRANSMISSIONS:

As data networks expand and as the requirements to support geographically widespread networks increase, there will be an increased demand for the development of faster speed transmissions to benefit from these high speed networks. As a result, users will be able to take advantage of these high speed data highways to transmit increased amounts of data associated with video, high volume data retrieval, and other high speed data services. These types of data services are typically used by large commercial, banking and Government institutions. Because of the sensitive banking data and personel information, there is a need to utilize encryption. By way of example, major inter-bank data transmissions typically utilize DES-based or comparable encryption.

High speed transmissions today typically run in the range of 10-50 Mbit/sec (10-50 million bits per second). At these data rates, hardware based encryption is the only feasible approach to data security. In this regard, the "Clipper" technique offers a suitable solution. In its current configuration, "Clipper" is designed to run at speeds of 10 Mbits/sec and if necessary, it can easily be engineered to run at speeds up to 100 Mbits/sec.

High speed transmissions can be viewed from a law enforcement intereception standpoint in two ways. If, as with interceptions of voice communications, the transmissions are comprised of individual data communications that have be multiplexed or bundled, law enforcement has a need for real time access to and decryption of the specific communications that are the subject of the interception. If, on the other hand, the high speed transmissions were of a bulk file or other volumious information transfer, it would not be physically possible or even desirable to process or view the product of the interception in real time. In these instances, access to the communications would be practically obtained "after the fact," under circumstances where the communications is no longer in transit but rather in storage.

LEGISLATION
XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX
XXXXXXXXX - BLACKED OUT PER NSA AS STILL TOP SECRET XXXXXXXXXXXX
XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX
XXXX XXXX XXXX XXXX PARAGRAPH BLACKED OUT XXXX XXXX XXXX XXXX
XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX
XXXXXXXXX - BLACKED OUT PER NSA AS STILL TOP SECRET XXXXXXXXXXXX
XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX

SOLUTIONS
In brief, the technical solutions and approaches developed to satisfy law enforcement's decryption requirements with regard to the main encryption applications are as follows:

Voice/Data Applications
XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX
XXXX XXXXXXX - Paragraph blacked out as per NSA - XXXX XXXX

Classified XXXXXX. XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX

- Real time access to and decryption of voice/data communications secured by software-based encryption XXXX XXXX XXXX XXXXXXX - Paragraph blacked out as per NSA - XXXX XXXX Classified XXXXXX. XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX in the near future. XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXXXXX - Paragraph blacked out as per NSA - XXXX XXXX Classified XXXXXX. XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX

Stored Information Applications

- Real time access to and decryption of stored electronic information secured by hardware based encryption could be performed utilizing the Clipper technique.

XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXXXXX - Paragraph blacked out as per NSA - XXXX XXXX Classified XXXXXX. XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX

XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXXXXX - Paragraph blacked out as per NSA - XXXX XXXX Classified XXXXXX. XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX

- Technical solutions, such as they are, will only work if they are incorporated into all encryption products. To ensure that this occures, legislation mandating the use of Government approved encryption products or adherence to Government encryption criteria is required.

Return to the Clipper Papers Page