September 28, 1993

Director, Computer Systems Laboratory
National Institute of Standards and Technology
Technology Building, Room B-154
Gaithersburg, MD 20899
Attn: Proposed FIPS for Escrowed Encryption Standard

Dear Sir:

On behalf of TIS, I hereby submit our very serious objections to the referenced proposed Federal Information Processing Standard (FIPS) and our recommendation that this proposal be rejected by the Department of Commerce for consideration as a FIPS.

Our objections are in three all encompassing areas. First, this draft is a corruption of the basic FIPS process itself. Second, it is a technically content-free standard. Third, it lacks any evidence of an economic analysis of the cost-benefit relationship of the proposed key escrow process.

1. Corruption of the FIPS Process

This proposed FIPS deviates so significantly from the "normal" FIPS process that it violates almost thirty years of tradition of open standards that have been subjected to repeated public scrutiny and are as technically sound as any public process can make them. Independent of the contents of this proposed FIPS, this shift in the FIPS process itself must be resisted if we are ever to have technical standards that are acceptable to the public again.

The traditional FIPS process, as represented by the very recent FIPS 140-1 proposal, typically involves the generation of a set of technical ideas which are discussed in public workshops and seminars, followed by a draft proposed standard which is widely distributed for public comment, often followed by several iterations, each attempting to meet the technical concerns of particular segments of the public and, eventually, resulting in a FIPS document that represents an acceptable compromise of technical ideas. This process, amazingly similar to the way Congress passes legislation, however long and frustrating, is undoubtedly the best process we will ever devise for producing a publicly acceptable standard that will be implemented by industry and yield products that can be purchased by consumers as well as the Government.

The Escrowed Encryption Standard (EES) proposed FIPS completely ignores this process and puts forth in the briefest, technically content-free document possible, a proposal which forces the public to rely completely on secret information that they will never be able to examine or understand. Secret specifications may be a necessary part of developing equipment and

procedures for protecting classified national security related information. But, they have no place in a free society in protecting unclassified Government and commercial information.

One must assume that the technicians that have devised the classified background for this FIPS shell are good at what they are doing (though the rumored further delay in availability of Clipper chips to the first quarter of 1994 does not build one's confidence). But, one must question the need for such secrecy and the price the Government will pay for being unwilling to share the technology by which it intends to protect our unclassified information.

There are alternatives to key escrow encryption that are technically sound and could follow the traditional FIPS approach. There are multiple instances of telephone security devices that are presently commercially available using proprietary approaches that could serve as a useful model for a FIPS. There is a long tradition dating back at least to the Data Encryption Standard, by which NIST seeks proposals from industry and negotiates to have complete rights granted to the public to use the approved commercial approach.

For unspecified reasons, NIST has chosen to abdicate its FIPS procedures and, without seeking public suggestions, to proceed directly with this unorthodox classified FIPS approach.

The only apparent reason given for the haste with which this process is proceeding is that "the President said he wanted it." Apparently, the staff people who prepared the President's statement of April 16, 1993 on the Clipper Initiative included comments to the effect that NIST should proceed quickly to develop a FIPS covering key escrow procedures.

I do not believe that if President Clinton understood, when he signed the April 16 announcement, he was asking for such a corruption of the technical process by which FIPS are developed, he would have signed the announcement.

2. Technically Content-Free Standard

This proposed standard contains so little specific information that it is almost totally useless to anyone attempting to implement a key escrow telephone system. The single most important motive for a FIPS is to establish a means for interoperability among multiple vendors' products. If there is so little information available in the FIPS that no one knows how to implement it without a classified contract, then I believe this document should not be called a FIPS.

It relies upon specifications of the encryption/decryption algorithm (SKIPJACK) and the LEAF Creation Method 1 (LCM-1) that are classified.

There is precedent in a very brief FIPS (FIPS 107 on Local Area Networks), but, in this case, the FIPS references a publicly available, extensively reviewed and unclassified

American National/IEEE/ISO Standard (802.3) that gives complete specifications for implementing that standard.

Anything less than this should be unacceptable as a FIPS.

3. Lack of a Cost-Benefit

The entire key escrow process, as it has been reported in public over the past six months, seems to be devoid of any analysis of what it will cost verses what it will accomplish. Perhaps the Government has performed such an analysis, but I am unaware of any indications to that effect.

In the same spirit that I offered my comments on the fundamental flaws in the NIST proposal to license the Digital Signature Algorithm to the Public Key Partners Corporation, I now offer the following relatively superficial analysis of the law enforcement benefits of key escrow. I hope this simple look will be augmented by better information from the Administration that will show that I am wrong in my approach and/or conclusions.

> If one estimates the number of telephone security devices that may be in use in the U.S. in the next ten years, one must acknowledge that, for the most part, the general public will not spend the extra money to protect its routine phone calls from an unforeseen threat. Businesses will probably purchase these devices for their executives but not bother for the bulk of their routine transactions. As a result, I estimate that, optimistically, as many as ten percent (10%) of the public phones in the U.S. may be protected with security devices in the next ten years. Given that the Administration has assured us that the public will not be prohibited from using alternative encryption systems, when one considers how many of these devices will be key escrow devices, one must take into account already available competing devices such as the AT&T proprietary 3600s and the Cylink DES devices which do not use key escrow procedures. I estimate that of the installed devices, no more than fifty percent (50%) will be key escrowed devices in the next ten years.
>
> The number of Title III wiretaps that take place in a given year is approximately 4,000 (the number of court ordered wiretaps is approximately 800 times an average of 5 physical taps per court order). If my estimate of the number of key escrow phone devices is accurate and those estimates represent the population of phones that the law enforcement authorities expect to encounter when placing a wiretap, then we should see approximately 200 actual key escrowed phone taps in any given year or approximately 16 per month; 1 every 2 days or so. This is hardly enough to justify all the key escrow administrative expenses.

Unfortunately, the estimates of five percent (5%) of the U.S. phones having and using key escrow devices is not likely to be representative of the population of phones that law enforcement authorities will encounter. Business executives will use key escrow phones, but

those that do not want their calls monitored by anyone will choose devices that are not subject to key escrow. So even the optimistic numbers cited above are probably overly optimistic. One cannot avoid commenting that it appears the key escrow agents will no doubt make the Maytag repair man look like a beehive of activity.

I recognize that there may be an EES II on the way that will extend key escrow to computer communications and perhaps increase the activity of the key escrow agents. On the other hand, presumably any Title III wiretaps of computer communications are already included in the estimated 4,000 wiretaps per year, so perhaps not.

And for this, how much will it cost to operate the key escrow process? Does anyone know?

I offer the above admittedly superficial analysis in the hope that the Administration will be forth coming with better documented estimates to justify why it is so intent on proceeding so quickly down the key escrow path. I fear that the proposed EES is just a symptom of a process that seems out of control.

One can only hope that the President's Interagency review of cryptography, that is expected to reach its conclusions soon, will recognize that there really is no need to proceed at such great speed and that the Administration and the public will be much better served by using a somewhat accelerated FIPS process, that makes use of public technical input, in establishing the U.S. public telephone security policy for the next twenty or thirty years.

Slow down and look at the alternatives! We cannot afford not to!

Sincerely,

Stephen T. Walker

cc: John Podesta