Subject: Thoughts on Clipper
From: Stephen Walker <steve@tis.com>

What's Happened to Clipper?

Stephen T. Walker
Trusted Information Systems, Inc.

December 3, 1993

With all the activity on the President's Key Escrow proposal from April 16 until early September, one would expect that there would be a great deal to report over the past three months. However, things have been remarkably quiet on the Clipper front.

There has been essentially no news from the government since the mid-September announcement to interested members of Congress and their staffs that NIST and a group somewhere in the Department of the Treasury would be the key escrow agents. A Department of Justice meeting scheduled for October 14 was cancelled. Presumably the Interagency Review process continues. There are reports of meetings with various industry groups, but as of this writing I am unaware of any publicly announced conclusions.

During this period, however, there have been a number of related activities that are worthy of note. In the next few pages I will summarize these developments in chronological order. Following this, I will describe some of my observations and conclusions.

Summary of Events since September:

On September 28, comments were due on the Escrow Encryption Standard (EES). Unofficially we were told that some 265 comments were received. One was in favor of the proposed standard. Four abstained from voting. The remaining 260 were opposed. To my knowledge there has been no official word on the EES comments.

On September 30, the President relaxed export controls on many forms of computertechnology. The previous upper limit on license-free export of workstations without any controls had been at a level of 12.5 Million Theoretical Operations Per Second (MTOPS), a measure that takes into account the power of parallel computer systems. The new license-free export level will be 500 MTOPS. Whereas the limit for which a specific license was needed (and for which it was reasonable to expect approval) was 25 MTOPS, the new limit will be 2000 MTOPS. Some have speculated that there may be only a few computers in the world that exceed 2000 MTOPS. But except for very powerful parallel computers, it appears there are no longer significant controls on the export of general purpose computers from the US.

On October 12, hearings by the House Foreign Affairs Subcommittee on Economic Policy, Trade and Environment were held. The hearings consisted of two sessions: the first open to the public, the second a closed classified hearing.

Congressman Gejdenson, chairman of the Subcommittee, opened the session by stating that NSA "is attempting to put the genie back into the bottle. It won't happen, and a vibrant and productive sector of American industry may be sacrificed in the process."

All of the comments during the open session were strongly opposed to the government's continuing controls on the export of cryptography. Demonstrations were given of the ease with which cryptography can be imported from friendly countries and used to protect all forms of sensitive information including voice and data.

An update of the statistics of foreign availability of cryptography indicated that 366 companies in 31 foreign countries were actively manufacturing and/or distributing cryptographic products. Actual product literature on 200 foreign products was displayed, 123 of them using DES. Products from the UK, Germany, the Netherlands, Israel, and Russia were displayed.

Congressman Gejdenson asked to "borrow" several of the products, promising to return them. He then gave them to NSA representatives at the closed hearing later the same day. The products were returned following an NSA review on December 2, 1993.

On October 20, the 700 Club on the Christian Broadcasting Network presented a feature that was strongly opposed to key escrow.

In early November, Bruce Schneier's book entitled Applied Cryptography was published. The book contains source code listings for 14 encryption algorithms including DES and IDEA. The rumor that disks containing the source code would be available with the book (as has been done in the past) was false. One must order them separately, and they will not be shipped outside the US and Canada, at least knowingly.

On November 3, CNN highlighted the Clipper situation with a story featuring Congressman Brooks stating:

"We shouldn't allow the intelligence agencies to control the economic commercial future of this country."

"They have a legititmate concern, but they probably felt that way when they developed the automobile--made it harder to caught criminals--they could get away faster--drive longer than they could ride a horse."

On November 4, the GAO released a study prompted by hearings in May 1992 on foreign industrial espionage that was highly critical of the government's continuing controls on the export of cryptography. According to the news release that accompanied the report:

"The global competitiveness of American corporations is threatened by government policies restricting the use

> of commercial encryption technologies that could help protect US businesses from foreign governments' economic espionage operations, according to Congressman Jack Brooks (D-Texas), Chairman of the House Committee on the Judiciary."

On November 12, the Concerned Professionals for Social Responsibility (CPSR) issued a summary of their Freedom of Information Act (FOIA) request regarding an internal FBI digital telephony initiative called "Root Canal" that:

> "Raises serious doubts as to the accuracy of the FBI's claim that advances in telecommunications technology have hampered law enforcement efforts to execute court-authorized wiretaps."

In early November, I met with representatives of government and industry in the UK, France, the European Commission, and Germany. The reaction in Europe to NIST's proposal to license the Digital Signature Standard to Public Key Partners and to the Clipper key escrow initiative in general ranged from confusion to anger and frustration. Many people are upset and considering setting up their own cryptographic processes for digital signature and confidentiality.

On November 17, a meeting was held at IDA of the DoD - Industry Technology Review Group examining possible relaxation of the COCOM export rules for information security products and technology in light of the President's recent major relaxation of export controls on computer technology. This meeting resulted in little change in the DoD position on export control of cryptography.

However, the highlight of the meeting was an amazing performance by the NSA representative (which another government official proclaimed the best stonewall he had ever seen), claiming among other things that:

> "Cryptography is on the irreducible list" (meaning presumably that it could never come off the export control list).
>
> "Discussions of cryptography must not take place in meetings outside the DoD" (there were representatives from the Departments of State and Commerce and from industry as well).
>
> "Industry may put forth evidence that the government may take out of context."

During this meeting it was stated that as a result of the President's relaxation of export controls on computers, there was a new emphasis on "economic security" in addition to the traditional "national security" and "political security" elements. Presumably with the end of the cold war, our economic health counts more heavily than it used to in making export control decisions. (More later).

In their November 22 issue, Business Week had a two page article entitled "Duking It Out for the Decoder Ring" in which they review the fight over "federal limits on data-scrambling software." Among the more interesting quotes are:

"Clipper is the most rancid idea to come along in quite a long time." - Whit Diffie, Sun Microsystems.

" ~There is no one who believes that the status quo can be maintained, even in the NSA,~ says a former White House national security official."

In their summary table, Business Week gives the following prognosis:

On technology:

"Clipper chip will be used by government and by companies doing business with it. Beyond that, limited use."

On exports:

"Export controls will be relaxed early next year but not nearly as much as industry wants."

On verification (digital signature):

"For the most part, industry won't adopt the government standard."

On November 23, Congresswoman Maria Cantwell introduced HR3627 in the House of Representatives, which would:

transfer jurisdiction for civilian encryption products to the Department of Commerce,

decontrol mass-market and public domain software to all but embargoed and terrorist countries,

decontrol hardware incorporating decontrolled encryption software, and

expand categories of customers eligible for file encryption.

In late November, the Department of Defense (DoD) Authorization Bill passed Congress with specific language that directs the DoD to fund a "Comprehensive Independent Study of National Cryptography Policy" by the National Research Council (NRC), part of the National Academy of Sciences. This review, to be completed within two years (after participants receive appropriate clearances) may be the most important development for reaching a long term resolution of this national dilemma.

It is worthy of note that no fewer than four recent NRC studies have commented on the export topic, in general recommending some form of relaxation of export controls.

On November 24, Josef Pieprzyk and Leonid Tombak of the University of Wollongong, Australia, published an English translation of the Government Standard of the USSR (GOST) 28147-89 Cryptographic Protection for Data Processing Systems, the Soviet equivalent of DES.

On December 2, Aleksandr Malchik and Whitfield Diffie of Sun

Microsystems published a second English translation of the same standard. Whit's preface contains several interesting observations:

> "The Soviet system has 32 rounds rather than the 16 of DES."
>
> "In contrast to DES's meager 56 bits of key, GOST 28147-89 has 256 bits of primary key and 512 bits of secondary key."

The Soviet standard "does not place any limitation on the secrecy level of the protected information."

Software versions of GOST are available without apparent export control from Russia through English distributors.

There has been speculation that those industries throughout the world who need cryptographic protection but are hampered by government export restrictions should consider widespread adoption of GOST, which can be freely exported from Russia and imported to virtually any location on earth. This may be the only way to get good quality cryptography worldwide.

On December 3, the Data Encryption Standard five year reaffirmation and the FIPS 140-1 Security Requirements for Cryptographic Modules were signed by the Secretary of Commerce.

Meanwhile:

Observations on the worldwide availability of cryptographic products:

The ongoing SPA-sponsored study of the worldwide availability of cryptographic products has confirmed, as of December 3, 203 foreign manufactured products, 127 of which utilize DES. There are active manufacturers and/or distributors in at least 32 countries around the world; indeed, the sun never sets on sale of cryptographic products.

But a much more ominous finding (for the US, at least) concerns the apparent ease with which vendors in foreign countries, including the United Kingdom, Germany, Denmark, and Israel, can ship DES-based cryptographic products to the US and presumably the rest of the world. In most cases, a phone call with a credit card number results in immediate shipment without any apparent government red tape. In many cases products as good as or better than those developed in the US arrived overnight.

These companies either have no government export controls to contend with or they fill out the paperwork after the fact with the certain knowledge that export will be approved retroactively.

It appears that companies in countries other than the US are allowed to operate on the premise that if the country to which the product is being shipped is not a COCOM proscribed country or a locally designated terrorist country, they are free to ship products containing DES-quality cryptography. Would that it were so in the US.

While in Europe, I was told that "the government does not mind a few small companies exporting small quantities of DES products. Indeed, there are concerns that if this government did prosecute, they might open up a legal can of worms since there appears to be no formal basis for the government to stop such exports. If, however, a company gets too big or sells too many products, they will be ~visited~ by the government and encouraged to stop."

In France, I learned that the rumor that the government requires registration of everyone's individual encryption keys is false. What they do require is registration of the general use of cryptography. If a company wants to encrypt its communications, it must tell the government of its intention and get the government's approval. It is not clear if there is any actual export control of cryptographic products from France.

In a written comment from a firm in Australia, we heard that in order to export cryptographic products from there, one must obtain a certificate that the country to which one is exporting does not "repress its citizens! Such a certificate is not hard to get for friendly countries."

It is becoming clear that if this situation stays as it is, the National Information Infrastructure will get its security from outside the US!

...On the Economics of Key Escrow:

In our comments on the Escrow Encryption Standard last September, we pointed out that based on:

> the wiretap statistics the law enforcement community has been using in the Clipper Initiative debate (approximately 800 wiretap court orders per year times approximately 5 physical wiretaps per court order), and
>
> an optimistic assessment of the number of key escrow phone security devices that are likely to be in place in the US in ten years (5%),

one can expect the key escrow agents to receive roughly 200 key escrowed calls per year or one every 44 hours {800 x 5 x 5% divided into 365 days}. This assumes that those whom law enforcement community are likely to wiretap (i.e., presumed criminals) will use key escrow devices in the same ratio as the general public, an unrealistic but conservative assumption.

Now that the key escrow agents have been tentatively named and are beginning to get organized, one can actually begin to assign costs to their operation and examine whether there is any economic sense to all this.

Each key escrow center will have to operate 24 hours a day, 7 days a week, 365 days a year because one can never know when a call from law enforcement will come in. NIST estimates that it will take ten people to fully operate a key escrow center. Assigning an approximate fully loaded cost for an employee of $150K per year, this means that the recurring personnel costs alone for one center will be $1.5M per year; two centers will be $3M per year. Conservatively, the costs of running two centers will be approximately double the personnel costs or $6M per year. If we can expect the above estimated 200 calls per year for key escrow requests, this equates to $30,000 per call.

The law enforcement community, in their arguments that wiretaps are used sparingly because they cost so much, has estimated that a typical conventional wiretap today costs between $50,000 and $60,000. If, in addition to those existing costs, the law enforcement community were to have to reimburse the costs of the key escrow process, the cost of a typical wiretap will increase by 50% or more. Does this make any sense?

...On the Legal Basis for Key Escrow:

While I was in France, a question about the US concerns for key escrow arose in discussions with government officials. After all, they asked, if there is as strong a separation of powers between the Executive and Judicial Branches of government in the US as there is in France, what are the objections to key escrow? I pointed out that this question hits directly at the concern of many in the US.

Key escrow, as being proposed by the US government Clipper Initiative, does not take advantage of the very significant separation of powers employed elsewhere in government (e.g., in the wire tap laws). On the contrary, the Executive Branch contends that it can implement key escrow entirely within the Executive Branch without further legislation. Unfortunately for the average citizen, this convenient expedient also allows the Executive Branch to change the rules that govern key escrow at any time without any oversight from elsewhere within the government.

A key escrow system that involved the Judiciary Branch as the escrow agent (there would be no need to have more than one agent to create an illusion of independence) might be much more acceptable to the average American citizen. In such a proposal there would be a true escrow relationship with the Judiciary Branch responsible to both the Executive Branch and the citizen. Of course this would require legislation to create such a process. It is not clear why such an arrangement is not being sought by the government. Perhaps it is just that it would take too long. Perhaps it would be better to take the time and do it right.

...On "Where is the Harm?"

Following the closed hearing on October 12, we were told that industry must show significant economic harm before a change can take place in the export controls on cryptography. At that hearing industry representatives testified that a $6-7B industry was at stake and that at least one major US vendor was losing $70M per quarter because of its inability to supply good quality cryptography to its multinational customers. It would seem that no matter how much information on losses one presents, it will never be enough to satisfy the government.

The government would very much like to limit this debate to an argument about looses of sales by the US computer industry. In so doing they can claim that the "security of the nation" is being jeopardized by an industry "that only worries about increasing sales."

But lost sales of computer products are not the aspect of economic security that should be concerning us.

There are two ways that government export controls affect our economic security:

> directly, through the loss of sales of computer products that employ cryptography, and
>
> indirectly and much more substantially, through the loss of government and commercial sensitive information if it remains unprotected on US and international computer networks.

The real concern here is the tradeoff between:

> the cost to all of us if our important government and corporate secrets are lost,
>
> versus
>
> the cost to national security and law enforcement interests if cryptography becomes more widespread, domestically and overseas.

Our government would have us believe that a major disaster will occur if good quality cryptography were to become widely available. But our survey indicates that good quality cryptography is already widely available from foreign sources. The governments of our friends overseas apparently are not concerned. They are not only not stopping the export of cryptographic products but in some cases, actively promoting them. And so far, at least, the national security disaster has not happened.

Why is it acceptable for friendly foreign countries to export to us but not for us to export to them? If US industry were allowed to export good quality cryptography, would the national security disaster happen any more quickly? We will not have to wait long to answer these questions. Soon foreign sources will dominate sales of cryptographic products in the US as well as overseas.

If the US government is so concerned about the availability of good quality cryptographic products throughout the world, their case would be much more believable if they exerted even a fraction of the energy they spend trying to stop US exports on pressuring the governments of friendly countries to control their own exports.

And what about the economic security disaster that will happen as increasing levels of US and multinational information on computer networks remains exposed because effective products to protect it are not available? At some point, it is inevitable that the cost of losing US government and industry sensitive information will exceed the cost to foreign intelligence from increased use of cryptography overseas. Do we have to wait for this disaster to seek a change in US export policy?

...On A National Policy on Cryptography:

In March 1992 the Computer System Security and Privacy Advisory Board recommended a national review of the use of cryptography in the US. Such a review is needed to find an appropriate balance between:

> the legitimate interests of citizens, private organizations, and the government to protect their own sensitive information, and
>
> the legitimate interests of the law enforcement and national security communities to listen to the communications of our adversaries.

One outcome of such a review might be a national policy on cryptography that would clarify where the boundary between the citizen's right to privacy and the government's need to listen exists. One version of such a policy might be:

> Good quality cryptography shall be available to all private citizens and organizations without government restriction.
>
> Good quality cryptography shall be defined as that which is routinely available throughout the world for the protection of sensitive information (e.g., the Data Encryption Standard (DES) or RSA encryption algorithms).
> Without government restriction shall mean without the interference of government through export control, imposition of key escrow, or other restrictive measures.

It is my personal opinion that until a national policy such as this becomes enacted into law, the debate on this topic will never end.