T E S T I M O N Y

RAND

Statement on Escrowed Key Proposals, Presented to the Subcommittee on Technology, Environment, and Aviation, U.S. House of Representatives

Willis H. Ware

CT-122

July 1994

The RAND testimony series contains the statements of RAND staff members as prepared for delivery.

Published 1994 by RAND
1700 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
To order RAND documents or to obtain additional information, contact Distribution Services: Telephone: (310) 451-7002; Fax: (310) 451-6915; Internet: order@rand.org.

VERBAL TESTIMONY

Statement on Escrowed Key Proposals

Presented by WILLIS H. WARE
Chairman, Computer System Security and Privacy Advisory Board

May 3, 1994

before the
Subcommittee on Technology, Environment, and Aviation
Congressman Tim Valentine, Chairman
Science and Technology Committee, U.S. House of Representatives

My name is Willis H. Ware. My career has been with the RAND Corporation for 42 years, and I now have an emeritus relationship with it. However, I am reporting today in behalf of the Computer System Security and Privacy Advisory Board (CSSPAB), and we thank you for the opportunity to be here. I have submitted a detailed written testimony and ask that it be included in the committee record. [Note: the chairman had already so ordered for all witnesses.]

The background of the Computer Security Act, the origin of the CSSPAB, and its mission and activities are in the written material.

I might just say parenthetically that all of the witnesses today have talked to the CSSPAB during its meetings, and we all know one another personally and collegially.

I think that the best way to summarize the CSSPAB view on the "encrypted key" initiative of the Administration is to paraphrase the relevant resolutions that the Board adopted since March 1992.

Since the Board includes, by statute, members from the computer industry, we first encountered the subject of cryptography in connection with export controls on such technology. It became clear that the exportability of such products is intimately related to the ability of

the United States computer and mass-market software industry to compete equitably in the international market. For each of them, the foreign market approximates 50% of the business base. We had also discussed the digital signature standard, which is part of the cryptographic picture as well.

We adopted a resolution in March 1992 acknowledging that cryptographic policy would be a difficult one for the country, that significant societal issues were raised by it, and that it was a matter directly involved with international competitiveness of U.S. industry. The resolution went on to call for

> ...a national level public review of the positive and negative implications of the widespread use of public and secret key cryptography....

and that this review

> ...must involve the national security, law enforcement, government unclassified/sensitive, and commercial communities...[including both vendors and users from the private sector].

This resolution was sent with a cover letter to the Secretary of Commerce, the Director of the Office of Management and Budget (OMB), the Director of the National Institute of Standards and Technology (NIST), the Assistant Secretary of Defense for Command, Control, Communications and Intelligence, the Director of the National Security Agency (NSA), and the Attorney General.

The cover letter stressed that cryptographic technology was unusual in that there is a large number of stakeholders, all of whom have legitimate but overlapping interests in cryptography and its use. Among the stakeholders are, of course, the government, the defense and law enforcement establishments, civil and non-classified government, private sector corporations, society at large as users of telephony and other

telecommunication services, the individual as a user of personal computers and data networks, and the academic community.

Later in 1992 we wrote to the Undersecretary of Commerce that the Board had "identified cryptography for general civilian use and its export control as a latent issue of high significance and [has] called for a national public review and dialogue."

At the end of 1992 and beginning of 1993, we also sent follow-up letters to members of the outgoing administration and the corresponding members of the new administration in an effort to assure that the issue did not get lost.

Following the April 16, 1993 announcement of Clipper, the Board was asked by Mr. Kammer to devote its June meeting to hearing public views on the Clipper program. At that meeting, we received 58 written submissions from a wide range of individuals and groups representing industry, academia, privacy rights advocates, and private citizens. The statements, along with an issues document, were forwarded to NIST. Parenthetically I might add that the Board had no prior knowledge of the Clipper initiative; it was as surprised as the rest of the country.

I ask that the issue document and its attached statements be made a matter of the committee record for this hearing. [Note: the chairman so ordered.]

The Board had become concerned that the Clipper proposal had not been well understood or appreciated generally. On the other hand, it also understood that major government procurements were under way. The Board wanted to acknowledge these realities but also to restate its concerns about such a significant shift in the way communications within the country would be influenced, and also its concerns about the possible constitutional issues that had been raised but not resolved.

It adopted a resolution in June 1993 providing in part for an additional special meeting of the Board but also conveying a statement of issues as we had heard them. Among them were:

1. A convincing [rationale for] the problem that Clipper attempts to solve has not been provided.

2. Export and import controls over cryptographic products must be reviewed.

3. The Clipper/Capstone proposals do not address the needs of the software industry, especially the mass-market industry.

4. Complete information must be provided on the proposed key escrow scheme to assure it to be fully understood by the general public.

5. Further development and consideration of alternatives to the key escrow scheme need to be considered.

6. The economic implications for the Clipper/Capstone proposals have not been examined.

and

7. Congress, as well as the Administration, should play a role in the conduct and approval of the results of the interagency review, undertaken by the Administration.

In July 1993 we expressed concern that the path proposed by NIST on the Digital Signature Standard would not be in the best interests of the country.

In September 1993 we again said in a resolution

> ...the preliminary concerns stated [as above] in [the Board] Resolution...[of March 1993] have been confirmed as serious ...and...need to be resolved.

We reiterated the prior list of concerns, and restated for emphasis that both Congress and the Administration must be involved in the cryptographic issue. We also endorsed the Administration-conducted

interagency review but added that we thought industry should be involved in the process.

In a second resolution, at the same time, the Board restated its position that the issues surrounding cryptography be debated in a public forum; but it strengthened its view on Congressional involvement by asserting that

> ...the Board believes that the Congress of the U.S. must be involved in the establishment of cryptographic policy.

This is a much stronger statement about Congressional involvement than had been previously stated.

At the same time, we recast our acknowledgement of conflicting legitimate interests by saying that those of law enforcement and national security, those of U.S. computer and telecommunication companies in the international marketplace, and those of U.S. citizens both domestically and internationally must all three be protected and a balance among them be achieved.

In December 1993 we endorsed the proposed Congressionally mandated study by the National Research Council as best meeting our repeated calls for a national review of cryptography.

At our most recent meeting in March 1994, we noted that the lack of a digital signature standard risks the success and acceptance of the National Information Infrastructure (NII).

You will note that we did not take a position for or against Clipper. Our interpretation of the statutory mission of the Board is to identify and report latent issues stemming from widespread use of computer and telecommunications policy. Moreover, to have attempted to reach a Board position on Clipper would have placed our four government members in an

untenable conflict position, one that would have been very awkward for them.

On the other hand, it is clear from the record of meetings and resolutions that the Board has deep concerns about the Clipper initiative; concerns focussed not on its technical aspects but rather on the fact that it was not a decision debated openly, on the fact that Congress has not been involved, on the fact that it will impact the balance of power between the government and the people, and on the possibility that it may negatively impact the international competitiveness and interests of U.S. industry.

In summary, I would say that, in its several meetings from March 1992 to the present, the Board has diligently fulfilled the expectations of it as set forth in the Computer Security Act. We did identify national cryptographic policy as an enormously important national issue and called it to the attention of relevant officials; we did identify many dimensions of the issue that collectively make it a difficult matter for the country; we did focus attention of the government and the public and private sectors on the issue; we did provide a forum in which public views as well as government views could be heard; we assembled the only public record of ongoing activities and progress in the Clipper initiative; and we did create a public record pertinent to national cryptographic policy and its many dimensions.

I want to acknowledge that over the two years that the CSSPAB has so far addressed the national cryptography policy issue, we have received courteous and thoughtful receptivity from the many federal officials with whom we interacted, in both the present and prior Administrations. The Board appreciates the government agencies' responsiveness and their readiness to hear our views and cooperate with presentations and in supplying information.

WRITTEN TESTIMONY

Presented by WILLIS H. WARE
Chairman, Computer System Security and Privacy Advisory Board

May 3, 1994

before the
Subcommittee on Technology, Environment, and Aviation
Congressman Tim Valentine, Chairman
Science and Technology Committee, U.S. House of Representatives

I am reporting today in behalf of the Computer System Security and Privacy Advisory Board (CSSPAB), a statutory board that was created by the Computer Security Act of 1987 [the Act, Public Law 100-235]. It is a privilege for me to appear before you as spokesman for the Board. I will summarize first the background of the Board and, second, its deliberations and actions on the issue of national cryptographic policy and export control of cryptography. All of the documents referenced below and the chronology of the action is a matter of public record.

BACKGROUND

Under the terms of the Act, the Advisory Board is composed of 12 members and a separately appointed chairman. In the words of the Act:

> Sec. 21. (a) There is hereby established a Computer System Security and Privacy Advisory Board within the Department of Commerce. The Secretary of Commerce shall appoint the chairman of the Board. The Board shall be composed of twelve additional members appointed by the Secretary of Commerce as follows:
>
> > (1) four members from outside the Federal Government who are eminent in the computer or telecommunications industry, at least one of whom is representative of small or medium sized companies in such industries;
> >
> > (2) four members from outside the Federal Government who are eminent in the fields of computer or telecommunications technology, or related disciplines, but who are not employed by or representative of a producer of computer or telecommunications equipment;

and

(3) four members from the Federal Government who have computer systems management experience, including experience in computer systems security and privacy, at least one of whom shall be from the National Security Agency.

The mission of the Board is defined in the Act in the following way:

(b) The duties of the Board shall be--

(1) to identify emerging managerial, technical, administrative, and physical safeguard issues relative to computer systems security and privacy;

(2) to advise the Bureau of Standards [sic] and the Secretary of Commerce on security and privacy issues pertaining to Federal computer systems; and

(3) to report its findings to the Secretary of Commerce, the Director of the Office of Management and Budget, the Director of the National Security Agency, and the appropriate committees of the Congress.

Since the Board receives administrative support, in particular the Executive Secretary, through the National Institute of Standards and Technology (NIST) which is a component of the Department of Commerce, the Board is directed to function under the rules established by the Department of Commerce for advisory bodies. Accordingly, the charter for the Board is written by the Department of Commerce and is renewed every two years. Moreover, the Board functions under the Federal Advisory Committee Act (FACA) in its role of advising the Executive Branch of the United States Government and the committees of the Congress.

Unless we are discussing budget matters, our meetings are open to the public, our final documents are available to the public, and members of the public may have an opportunity to address the Board. In the near future, all of our resolutions and letters of transmittal, minutes of meetings, and other documents will be available electronically through the electronic bulletin board and other on-line information services

operated by NIST. In view of the FACA, it is important to appreciate that all decisions taken by the Board and all resolutions passed by it, including the prior supporting discussion, is conducted in a public forum.

Currently, the Board, because of term rotation, is not fully staffed; it currently lacks two members from outside of government. A quorum for the conduct of business is seven members. Since its inception in 1988, the Board has met quarterly in the greater Washington area.

AGENDA ITEMS

In responding to the general mandate in the Act, the Board initially concerned itself with a variety of issues, all concerned with computer security, but primarily directed to helping NIST respond to its directives under the Act. Among such topics in the first three years were: the agency security plans called for by the Act; the NIST annual budget; the NIST research program in support of computer security; NIST participation in other security-related matters such as the continuing effort to create [first] a national Federal Criteria for the evaluation of security products for information systems, but [now] an international effort with the same goal; and NIST support to agencies--for example, the preparation of a security handbook. The Board also attempts to stay informed of new developments and security-relevant initiatives within government, but it also occasionally hears presentations from the private sector.

The precise agenda of each meeting is determined by suggestions from the Board members plus additional ones from the Chairman and the Executive Secretary. The agenda is submitted to the membership prior to each meeting; and in accord with the FACA, our agenda, meeting place, and time are noticed in the Federal Register at least 30 days prior to the meeting.

In its six years of functioning, the Board has been requested once by the Deputy Director of NIST in support of the so-called "Clipper initiative" and is currently considering a request from the OMB in

connection with security aspects of the National Information Infrastructure [NII].

CRYPTOGRAPHY

The Board first encountered the subject of cryptography in connection with export controls on such technology. Vendors of computer systems and mass-market software made presentations to the Board and were also represented in the Board membership. Thus, it became clear that the exportability of cryptographic products were intimately related to the ability of the United States computer and mass-market software industry to compete equitably in the international market.

Because of the knowledge, experience, and background of all Board members, including the Chairman and the Executive Secretary, the subject of a suitable national standard for the so-called "Digital Signature Algorithm" (DSA) and the "Digital Signature Standard" (DSS) also came before the Board as early as 1991. Such a national standard is essential for the reliable, safe, orderly, and legal conduct of business via linked computer systems. This is commonly referred to as "electronic commerce" but digital signatures are also required for a wide variety of other transactions in which trust among the participants must be supported by legally accepted and binding digital signatures.

MARCH 1992 MEETING AND INITIAL RESOLUTION

The interest of the Board in cryptography peaked in 1992 and at its March meeting of that year, the Board passed its initial resolution on the subject. The Board understood, collectively and individually, that the subject was a very awkward one for the nation because there are so many stakeholders with a legitimate interest in the matter. Accordingly, we framed our resolution in the most general way, and suggested a mechanism for proceeding with the development of a suitable national policy. The transmittal letter restated the broad and intricate nature of the cryptographic issue and conveyed a sense of the Board's conviction of its importance.

In particular, the resolution [#1 of March 18, 1992] was as follows:

> The Board has examined the present status of the proposed Digital Signature Standard (DSS) being undertaken by the National Institute of Standards and Technology (NIST). In view of:
>
> (1) the significant public policy issues raised during the review of the proposed standard;
>
> (2) the increasingly pervasive use of digital technologies;
>
> (3) the potential impacts upon the security of the unclassified but sensitive government community;
>
> (4) the relationship of the DSS to the existing NIST cryptographic security program; and
>
> (5) the posture of the U.S. in international commerce.
>
> THE BOARD FINDS THAT:
>
> (1) a national level public review of the positive and negative implications of the widespread use of public and secret key cryptography is required. This national level review must involve the national security, law enforcement, government unclassified/sensitive, and commercial communities. Representatives from the private sector should include both vendors and users. In the next several months, NIST/NSA should sponsor a workshop on the widespread use of cryptography. This national review should be concluded by June 1993 and should result in a national policy concerning the use of cryptography in unclassified/sensitive government and the private sector.
>
> (2) NIST has made significant progress in resolving the technical issues related to the proposed DSS. The Board recommends that NIST continue to seek resolution of the patent, infrastructure, and other remaining issues raised during the public comment process. The Board recognizes that much of the work, and in particular the infrastructure, is algorithm independent and must be continued by NIST to assure timely implementation of digital signature technology within the government.

The resolution was adopted unanimously by the Board.

With the Board's authority and concurrence, the Chair drafted a cover letter which read as follows.

> The rapid progress of communications, computer, and electronic technology in the last 40 years has created a genuine civilian and non-defense demand for cryptographic techniques and devices to protect computer data, computer systems, and other communications against unauthorized access and eavesdropping.
>
> Cryptographic technology, which includes encryption, historically has been in the custody of the defense and military establishment of the United States. A similar situation has prevailed throughout the world for centuries, but there have become many stakeholders all of whom now have a legitimate interest in cryptography, its technology, its operational deployment, and its oversight. Among them are the following:
>
> - The Federal government for its own operational needs and in its role within the international community.
> - The defense establishment, notably the communications security and various intelligence functions.
> - Law enforcement for not only its own security needs but also for counter-intelligence actions against law-breaking organizations.
> - Civil and other non-classified government to protect its unclassified yet sensitive data.
> - Private sector corporations that function domestically and internationally and must protect sensitive data and communications.
> - Society at large as users of telephony and other services that must assure confidentiality and privacy for communications.
> - The individual as a user of personal computers and the data networks of the world with their extensive array of information services.
> - The academic community in pursuit of a legitimate discipline of study and research.
>
> The interests of all such parties overlap and are often in conflict which makes the matter an urgent concern of national policy. In view of this, the Computer System Security and Privacy Advisory Board (CSSPAB), created by the Computer Security Act of 1987 and charged under the Act to identify latent issues of national policy significance, resolved during its March 17-18 meeting to call for a national public review of the issue.

> The resolution and two related ones are [attached to] this letter. The Board commends them to your attention and solicits your support of this important action.

The other two resolutions [#2 and #3 of March 18, 1992] referenced in the transmittal letter (1) recommended that the DSS not be approved until the national review had been completed, and (2) stated the Board's intention not to take a position on the proposed DSS until the national review had been completed.

The package of three resolutions and the transmittal letter were sent to the Secretary of Commerce [Honorable Barbara Franklin], the Director of OMB [Honorable Richard Darman], the Director of NIST [Dr. John Lyons], Assistant Secretary of Defense for Command, Control, Communications and Intelligence [Mr. Duane Andrews], the Director of NSA [Vice Admiral W.O. Studeman] and the Attorney General [Honorable William Barr].

Other Steps by the Board in 1992

Letters of acknowledgement were received from most of the addressees and in particular, Dr. Robert White [Undersecretary of Commerce for Technology] informed us that the Director of NIST had commenced the activities pursuant to the conduct of such a review.

Accordingly, at its June 1992 meeting, the Board drafted a follow-up letter to the same addressees advising each of Dr. White's action, and again reiterating the Board conviction of the national importance of the issue. In particular, the Board wrote:

> ...pursuant to our responsibilities under the Computer Security Act of 1987, we [have] identified cryptography for general civilian use and its export control as a latent issue of high significance and [have] called for a national public review and dialogue.

The Board also advised in this letter that it would devote its next meeting entirely to the topic and solicited the cooperation of each entity to help set the agenda for the national review.

The Board also authorized the Chair and the Executive Secretary to "discuss the National Cryptographic Review with appropriate Federal officials" [Resolution #4 of March 18, 1992]. These visits and discussions were conducted in the fall of 1992.

Several common themes emerged during these discussions:

1. The review should not and could not take place solely within the government; private sector input should be solicited and encouraged.

2. All parties should have the opportunity to clearly state their positions.

3. There should be a recognition that the U.S. cannot control worldwide cryptographic policy.

4. While it is not clear how dynamic this issue may be, delays in addressing this issue must be avoided, since market forces and technology can change quickly.

5. The Board could serve a useful purpose by focusing attention on this issue during the transition period.

6. Finally, a June 1993 date for completion of the Review called for by the Board was unrealistic, particularly given the transition process.

DECEMBER 1992 MEETING

At its December 1992 meeting, the Board appreciated that the National Cryptographic Review was a subject that might get overlooked in the Presidential transition process. Accordingly, it drafted a letter to the same set of Federal officials plus a few others reiterating the importance of cryptography as a national issue and of the National Cryptographic Review, and urging that the matter be called specifically to the attention of the respective transition teams.

The Board authorized the Chair to send similar letters to the officials of the new Administration as they became known; this was done in the first two months of 1993.

Each of these bridging letters was very similar to the transmittal letter that accompanied the Board's initial resolution, but added comments about the importance of continuing attention to the issue.

JUNE 1993 MEETING AND RESOLUTIONS

The normally scheduled March meeting of 1993 was canceled because of budgetary uncertainties; and on April 16, 1993, the Administration announced its initiative to provide escrowed-key encryption technology to the government for secure telephony--the so-called Clipper initiative. This announcement was a complete surprise to the Board which had no prior indication that this event was even under consideration within the Executive Branch.

On May 10, 1993, the Board was asked by the Deputy Director of NIST to devote its June meeting to hearing public views on the Clipper program. After preparation of a summary document, it advised NIST's Deputy Director by letter on August 8, 1993:

> At your request, the Computer System Security and Privacy Advisory Board devoted its June meeting to collecting public comments on the subject of the Administration's key escrow encryption technology as well as broader issues of cryptographic policy. In all, we heard two days of public statements and received 58 written submissions from a wide range of individuals and groups representing industry, academia, privacy rights advocates, and private citizens. The statements, along with a document summarizing the major issues, are enclosed in this package.

A full transcript of the meeting is also available. In view of the importance of the matter, the Board resolved [93-1] an additional special three-day meeting be held in July to hear yet more views from both public and government representatives.

The Board had grown concerned through all the discussions about Clipper that the full impact of the proposal was not well understood or appreciated. On the other hand, it also understood that major government procurements were under way or were imminent (e.g., the DoD Defense Messaging System) and that commitments had been made by the Executive Branch to take steps to acquire an initial group of 9,000 secure Clipper telephones. The Board wanted to acknowledge these realities but also to restate its concerns about such a significant shift in the way communications within the country would be influenced, and about the possible constitutional issues that had been raised but not resolved.

Accordingly, it passed two resolutions and in an attachment to the first, summarized a distillation of the many major concerns that had been expressed to the Board or had been distilled from them over five days of presentations that we had held.

In the first resolution [93-1], it noted:

> At Mr. Kammer's request we have conducted two days of hearings. The clear message of the majority of input was that there are serious concerns regarding the Key Escrow Initiative and the Board concurs with these concerns. Many of these issues are still to be fully understood and more time is needed to achieve that understanding.
>
> Accordingly, this Board resolves to have an additional meeting in July 1993 in order to more completely respond to Mr. Kammer's request and to fulfill its statutory obligations under P.L. 100-235. The Board recommends that the inter-agency review take note of our input collected, our preliminary finding, and adjust the timetable to allow for resolution of the significant issues and problems raised.
>
> Attached to this resolution is a preliminary distillation of the serious concerns and problems.

The "inter-agency review" mentioned in this resolution was a part of the Administration announcement of Clipper. To be conducted by the White House staff, it was to examine national cryptographic policy, including export control policy.

In the attachment to the resolution, the Board noted:

- A convincing statement of the problem that Clipper attempts to solve has not been provided.
- Export and import controls over cryptographic products must be reviewed. Based upon data compiled from U.S. and international vendors, current controls are negatively impacting U.S. competitiveness in the world market and are not inhibiting the foreign production and use of cryptography (DES and RSA).
- The Clipper/Capstone proposal does not address the needs of the software industry, which is a critical and significant component of the National Information Infrastructure and the U.S. economy.
- Additional DES encryption alternatives and key management alternatives should be considered since there is a significant installed base.
- The individuals reviewing the Skipjack algorithm and key management system must be given an appropriate time period and environment in which to perform a thorough review. This review must address the escrow protocol and chip implementation as well as the algorithm itself.
- Sufficient information must be provided on the proposed key escrow scheme to allow it to be fully understood by the general public.
- Further development and consideration of alternatives to the key escrow scheme need to be considered, e.g., three "escrow" entities, one of which is a non-government agency, and a software based solution.
- The economic implications for the Clipper/Capstone proposal have not been examined. These costs go beyond the vendor cost of the chip and include such factors as customer installation, maintenance, administration, chip replacement, integration and interfacing, government escrow system costs, etc.
- Legal issues raised by the proposal must be reviewed.
- Congress, as well as the Administration, should play a role in the conduct and approval of the results of the review.

The second resolution [93-2] reflected the Board's concern that the Clipper situation was moving more rapidly than people had been able to

understand and assimilate its impacts, but acknowledged that certain executive branch action could not be stalled while the cryptography policy issue was being resolved.

JULY 1993 MEETING AND RESOLUTION

Concurrently with introduction of the Clipper initiative, the NIST proposal for a Digital Signature Standard (DSS) had encountered troublesome patent difficulties and some of the presentations to the Board at its specially called meeting in July did in fact relate to the DSS. Accordingly, a resolution [93-4] was passed noting that the original goal of a royalty-free DSS standard had not been achieved, that the economic impact on the country of a proposed NIST plan to establish certain exclusive patent licensing arrangements had not been examined, and expressing our concern that this path would not be in the best interests of the country.

SEPTEMBER 1993 MEETING AND RESOLUTIONS

Even though a number of other things were important for Board consideration, half of our regularly scheduled September meeting was again devoted to Clipper matters. Accordingly, an additional resolution [93-5] was framed and adopted as follows:

> Subsequent to the June 2-4, 1993 meeting of the CSSPAB, the Board has held an additional 4 days of public hearings and has collected additional public input.
>
> The clear message is that the preliminary concerns stated in Resolution #1 of that date [September 1-2, 1993] have been confirmed as serious concerns which need to be resolved.
>
> Public input has heightened the concerns of the Board to the following issues:
>
> - A convincing statement of the problem that Clipper attempts to solve has not been provided.
>
> - Export and import controls over cryptographic products must be reviewed. Based upon data compiled from U.S. and international vendors, current controls are negatively impacting U.S. competitiveness in the world market and are not inhibiting the foreign production and use of cryptography (DES and RSA).

- The Clipper/Capstone proposal does not address the needs of the software industry, which is a critical and significant component of the National Information Infrastructure and the U.S. economy.

- Additional DES encryption alternatives and key management alternatives should be considered since there is a significant installed base.

- The individuals reviewing the Skipjack algorithm and key management system must be given an appropriate time period and environment in which to perform a thorough review. This review must address the escrow protocol and chip implementation as well as the algorithm itself.

- Sufficient information must be provided on the proposed key escrow scheme to allow it to be fully understood by the general public.

- Further development and consideration of alternatives to the key escrow scheme need to be considered, e.g., three "escrow" entities, one of which is a non-government agency, and a software based solution.

- The economic implications for the Clipper/Capstone proposal have not been examined. These costs go beyond the vendor cost of the chip and include such factors as customer installation, maintenance, administration, chip replacement, integration and interfacing, government escrow system costs, etc.

- Legal issues raised by the proposal must be reviewed.

- Congress, as well as the Administration, should play a role in the conduct and approval of the results of the review.

Moreover, the following are additional concerns of the Board:

- Implementation of the Clipper initiative may negatively impact the availability of cost-effective security products to the U.S. Government and the private sector;

and

- Clipper products may not be marketable or usable worldwide.

While this resolution is similar to prior ones, it recasts some of the issues of concern and restates for emphasis that "Congress as well as the Administration should play a role in the conduct and approval of the results of the [national cryptographic] review."

By way of explaining why we framed the Congressional role as noted, it has been the Board's understanding that an Administration-sponsored review of cryptography would be conducted, including the export control aspects, and that it would be available in the fall of 1993 and could be briefed to the Board. The Board believed that this review would provide suggestions, if not options, for a national cryptographic policy.

The Board strengthened its views in a second resolution [93-6] as follows:

> The Board believes that in deciding cryptographic policies and standards in the U.S., there is a compelling need to consider and evaluate the concerns listed below. We, therefore, endorse the process being pursued by the Administration in the form of an interagency review but believe the scope of that review needs to include adequate industry input. We reaffirm our recommendation (of March 1992) that the issues surrounding this policy be debated in a public forum. In view of the worldwide significance of these issues the Board believes that the Congress of the U.S. must be involved in the establishment of cryptographic policy.
>
> The Board, furthermore, believes that there are a number of issues that must be resolved before any new or additional cryptographic solution is approved as a U.S. government standard:
>
> 1. The protection of law enforcement and national security interests;
>
> 2. The protection of U.S. computer and telecommunication interests in the international marketplace; and
>
> 3. The protection of U.S. persons' interests both domestically and internationally.

It very carefully noted the three conflicting interests (which are restated derivatives of those included in the April 1992 transmittal letter), and the Board stated unequivocally that "In view of the worldwide significance of these issues...the Congress of the United States must be involved in the establishment of cryptographic policy."

This is a much stronger statement about Congressional involvement. Previously, the Board had only said that "Congress as well as the Administration should play a role in the conduct and approval of the results of the [national cryptographic] review."

DECEMBER 1993 MEETING AND RESOLUTIONS

The Board again heard updates on various Clipper-related matters and thereby, helped inform the public what events were transpiring and how decisions and choices were being made. The Board also was briefed on the Congressionally mandated study of cryptography to be performed by the National Research Council (NRC), and in a resolution [93-7], stated that such a study "best accomplishes our repeated calls for a national review of cryptography dating back to March 1992," that the Board would like ongoing updates, and that the NRC be encouraged to conclude the study as quickly as possible.

During the several meetings of 1992-1993, it gradually became clear that NIST could not conduct a national review all by itself, and its management stated this fact to the Board at one time. At various times the Board had encouraged NIST to undertake certain background analyses that could contribute to an overall study. [For example, Resolution #2 of September 17, 1992].

MARCH 1994 MEETING AND RESOLUTION

More updates on security and Clipper-related matters were presented during a two-day agenda, and the Board adopted a resolution [94-1] endorsing the National Performance Review but also noting that "progress on essential parts of the security architecture for the NII appear to be very slow" and also that "the lack of a digital signature standard risks the success and acceptance of the NII."

CONDUCT OF THE NATIONAL CRYPTOGRAPHIC REVIEW

The Board has realized all along that such a broad examination of a subject that had never been widely discussed publicly would be difficult to conduct, primarily because of the conflicting interests of so many stakeholders inherent in cryptography. We found no one within

government willing to accept the challenge and, eventually, we realized that NIST could not do it either. Various ideas such as an outside group, a Blue Ribbon Commission led by an eminent respected public personage, or a high-level specially constituted government committee were discussed but without a specific conclusion and position. At the moment, the Board considers the intended NRC study to be the best chance for an objective consideration of all the complexities of cryptography.

PRIVACY

The word "privacy" does appear in the Board's title and charter, and it is defined by the Act in terms of the Privacy Act of 1974.

> (4) the term 'sensitive information' means any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

As meant by the Computer Security Act, privacy is thus an information-use matter as it was originally intended to be in the Privacy Act. The Board planned to address privacy in this context during 1993, but cryptography and, in particular, Clipper dominated Board affairs throughout the year. While cryptography is directly related to the assurance of confidentiality of information, it is only indirectly related to privacy, as the term is defined by the two acts. Moreover, the Administration effort known as the Information Infrastructure Task Force (IITF) is also examing privacy in the information-use context of the NII, and the Board has opted to wait until its work has been completed and can be presented to us.

SUMMARY

From March 1992 through the present, the Computer System Security and Privacy Advisory Board has diligently and persistently concerned itself with national cryptographic policy and various events related to it. In

these two years and based on its publicly available record, the Board has:

- Focused attention of government agencies on the cryptographic issue;
- Focused attention of the public and various private-sector organizations on the cryptographic issues;
- Provided a forum in which public views as well as government views could be heard;
- Assembled the only public record of ongoing activities and progress in the Clipper initiative; and
- Created a public record for national cryptographic policy, and its many dimensions -- Clipper, Capstone, DSS, public concerns, industry concerns, constitutional concerns.

In the Board's dealings with many Federal officials, we have received courteous and thoughtful receptivity and attention from both the present and prior Administration. The Board appreciates the government agencies' responsiveness and their readiness to hear our views and cooperate with presentations and in supplying information.