DOCID: 3978871

NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
FORT GEORGE G. MEADE, MARYLAND 20755

P.L. 86-36

Serial: N1053
7 October 1980

MEMORANDUM FOR THE DEPUTY UNDER SECRETARY OF DEFENSE (POLICY REVIEW

SUBJECT: National Policy on Public Cryptography

1. Please refer to your DUSD (PR) memorandum I-08944/80, 22 September 1980, subject "National Policy on Public Cryptography."

2. While progress has been achieved in identifying the principle issues involved in a national policy on public cryptography, I have serious reservations concerning the proposed DoD response to Dr. Press and cannot support it in its present form. It would be most counter-productive to forward this response to Dr. Press without major modification as to both specific content and general philosophy.

3. I believe that the response does not describe the significant differences of opinion that have evolved between Defense and Commerce regarding many of the identified issues. We have not agreed with the proposed policy positions on Issues No. 1 and 2 and have earlier provided alternative statements for these issues. Despite our earlier submissions to you, as currently drafted the proposed positions do not protect the Government's legitimate national security concerns nor accommodate the results of NSA's recent work with the American Council on Education's (ACE) Study Group on Public Cryptography.

4. The issues analysis in the draft Appendix A does not represent, as implied in the introductory paragraph of the Summary, any sort of agreement between DoD and DOC participants and, as such, is misleading. Because of the lack of consensus concerning the "YES" and "NO" points included in each issue analysis, the points are confusing and misleading. I recommend that the "YES" and "NO" points be deleted and that only a list of the Issue statements and their respective DoD policy statement positions be forwarded to Dr. Press. In addition, I suggest that the penultimate sentence of the Summary be revised to read "Each policy statement represents only the Department of Defense position; it should be understood that the issues analysis undertaken jointly with the Department of Commerce surfaced broad disagreement regarding the factors impacting on each issue as well as the policy positions themselves." With this change, the final sentence of the Summary may be deleted.

5. I also recommend that the introductory paragraph to Section I be revised as follows:

"I. Academic and Industrial Research

Both national security concerns and the Constitutional rights of citizens, including freedom of expression under the First Amendment, must be considered and protected in this area. To this end the Government should adopt the following policy:"

This restatement sets the proper balance between the concerns that must be considered in establishing policy.

6. The following comments apply to the proposed DoD policy positions:

a. With regard to Issue No. 1, I do not believe that any amount of export business could compensate for the potential loss of SIGINT capability or compromise of communications security techniques and, therefore, do not accept the proposition that we foreclose the possibility of either voluntary or legislated controls over the domestic publication of privately funded cryptographic research results. Prior experience with the Atomic Energy Act provides adequate precedent in this regard. In addition, our experience with the American Council on Education's task force on public cryptography indicates an appreciation of the potential danger posed to national security interests by publication of research results and a receptiveness to some form of voluntary review. Consequently, I strongly recommend that the DoD position on Issue No. 1 should read:

"Privately funded cryptographic research leading to development and application of basic research should proceed under conditions in which individuals and institutions cooperate with the Government to identify activities having a potential impact on national security."

b. Issue No. 2 has been discussed with the DoD Office of the General Counsel. It is our considered judgment that foreclosure of the licensing approach is not sound policy. Even the "YES" and "NO" discussion points contained in the issue analysis do not support an absolute foreclosure. A policy position flatly stating that such a program will not be initiated is inconsistent with ongoing efforts to examine the possibility of establishing a voluntary or legislated review or licensing mechanism. The objection that prepublication review would "burden scarce Government resources" is inconsistent with our experience with reviewing NSF grant applications. I believe that expression of a firm DoD policy position on this particular issue is premature and strongly recommend the following alternative:

"The Federal Government has not yet reached a policy decision as to whether there should be voluntary review or licensing of cryptographic research by individuals or institutions. Until such a determination is made, private cryptographic researchers are encouraged to cooperate with the Government in the early identification of such cryptographic research to ensure that such research does not adversely impact on national security interests."

7. I am similarly concerned that the policy statements under Section III Export Controls, as presently worded, might cause foreign customers concern with regard to purchasing products offered by the U.S. and, in the long run, adversely impact on NSA operations. This concern can be diminished with relatively minor rewording as follows:

"The controls currently embodied in the International Traffic in Arms Regulations (ITAR) on the export of cryptographic equipment produced by the private sector are necessary to provide an effective means of governing the proliferation of advanced technological cryptographic equipment to foreign consumers. Moreover, the controls may be reviewed periodically to ensure they are clear and impose a minimal administrative burden to U.S. researchers." (Issues 8 and 9)

"The controls stipulated in ITAR and interpreted by Munitions Control Newsletter No. 80, limiting the export of cryptographic technical data, are necessary to ensure that national security technological expertise having direct or indirect application to the use of cryptographic equipment is not exported. Moreover, the controls may be reviewed periodically to ensure they are clear and impose a minimal administrative burden to U.S. researchers." (Issues 10 and 11)

8. Further, with regard to Issues No. 8-11, it must be recognized that the "NO" statements in the present Appendix are those of the DOC and reflect an attack on ITAR which, if permitted and disseminated, and which I am advised are not supported by existing case law, would be unnecessarily damaging to our efforts to assist in managing cryptographic export in the interest of national security. I consider this another excellent reason for deletion of the Appendix.

9. I would welcome the early opportunity to meet personally with you to discuss this matter further.

B. R. INMAN
Vice Admiral, U. S. Navy
Director, NSA/Chief, CSS

DOCID: 3978871

Serial: N1053

cc: DIR
D/DIR
DDPP
Q3
Q32 (2)
Q321
Q1
L221
F19
EX REG
GC
DDR
DDC
DDO
DDPR
A
B
W
G
V
P1
P4

P.L. 86-36

M/R: This memo based on inputs from DDO, DDR, DDC, and GC and its substance

[redacted]

constituted are enclosed.

[redacted]

P.L. 86-36

3 Oct 80/lie

Encls:
a/s (less encls)