David Kahn
Windsor Gate
Great Neck, New York

December 28, 1954

The Director
National Security Agency
Arlington Hall, Vriginia

Sir:

The recent criticism of the nationalsecurity system by the American Association for the Advancement of Science prompted the New York Cipher Society to issue the enclosed "To Improve Our Cryptographic Defenses." As you can see, the statement first corrects an unwitting error in the Association's statement and then further explains the danger inherent in the present overly-restrictive cryptographic security system. We confine ourselves to our particular sphere of competence.

We are sending you a copy of this statement in the hope that the logic of its position will confince you to liberalize our current cryptographic security program.

"To Imppove Our Cryptographic Defenses" was adopted without objection by the New York Cipher Society at our regular monthly meeting held in New York on December 20, 1954. In addition to the Board of Directors of the American Association for the Advancement of Science, copies are being sent to President Eisenhower and to other parties.

We hope that this statement will prove of some assistance to you in your work of guarding the communication lines which are so vital to the nation. If you have any questions concerning the statement, please do not hesitate to write us.

Very truly yours,

David Kahn

President
New York Cipher Society

TO IMPROVE OUR CRYPTOGRAPHIC DEFENSES

The New York Cipher Society agrees with the principles calling for greater freedom of scientific information which were set forth in "Strengthening the Basis of National Security" by the Board of Directors of the American Association for the Advancement of Science. In that spirit of agreement, the Society wishes to point out that the Association has unwittingly implied opposition to its own suggested security policies in a field vital to the national defense. This it has done by its unqualified mention of "communication codes" in the following sentences:

> Communication codes, troop strength and disposition, strategic plans and other such information can be kept out of enemy hands, at least temporarily, by adequate security safeguards. Although such information eventually becomes obsolete or is compromised through operational use, until this happens secrecy is proper and effective.

No one can deny the truth of that statement, strictly read. The actual codes or ciphers used by our armed forces, the keys used in encipherment, the enemy codes or ciphers broken by our cryptanalysts, the messages resulting from such cryptanalysis -- all these properly lie within the bounds of security information. However, the Association seems to have overlooked here the fact -- elsewhere made explicit and essential to the argument -- that these specific, secret items ultimately derive from principles which are generic and

non-secret. In fact, these principles, systematically arranged, are well-known to us as the science of cryptography. This definition of cryptography as a science lets it add its voice to the Association's call for a freer dissemination of scientific information.

The Association's original statement would seem to exclude this participation, although it is clearly in line with Association policy that "the security of the nation requires the most favorable circumstances for the advancement of science, an environment that will foster a healthier, more imaginative, more energetic development than that which serves the enemies of freedom."

The situation regarding specific ciphers and general cryptography parallels that regarding weapons and basic scientific knowledge that the Association brings out. Just as basic scientific research furnishes the knowledge to create new weapons, so cryptographic progress furnishes the knowledge to invent new ciphers and methods of solution. And just as a request for more scientific information does not mean the compromise of any weapon, so a request for more cryptographic data does not imply revealing any official ciphers or cryptanalyses. This parallel exists, of course, because codes are, in a sense, a weapon, and because cryptography forms part of general scientific knowledge.

In sum, then, while specific governmental codes and ciphers should, like weapons, be kept secret, general cryptographic knowledge should, like basic scientific information, be broadcast as widely as possible. This is the fact which the Society fears may be blurred by the Association's blanket mention of "communication codes" and which the Society has tried to clarify in this note.

* * *

Since the security situation with respect to cryptography is exceptionally restrictive, the Society feels that it warrents a further statement:

Many reasons aggravate the cryptographic security situation in this country. One, undoubtedly, is the current confusion between basic research and subsequent results which the Society has tried to clear up in this statement. Another is the fact that through the ages cryptographic information has consistently been suppressed -- probably because of the very confusion exemplified in the Association's statement. Another is the natural exclusiveness of the professionals. Still another is the traumatic experience -- still all too fresh in the memory of many of our cryptographers -- of having an American expose all of his own country's most secret activities in this field, thereby ruining years of work on the solution of many foreign codes. All of these factors add up to the especially heavy restrictions on the free discussion of cryptography in this country.

Such a policy is, in the opinion of the Society, short-sighted at best and unconscionably dangerous at worst. Three reasons point to this conclusions.

The first is the set of arguments for less stringent security regulations advanced by the Association in its statement. All these arguments hold true for cryptography as well as for basic scientific knowledge because, as the Society explained, the latter includes the former. Further, the Society would make explicit the feeling behind the Association's statement that the security program ultimately threatens freedom of thought, that it is therefore repugnant to American ideals, and that it is tolerated only because

of the present world tension. Aside from this, the Society can add little to the Association's statement beyond remarking that outside criticism and suggestion would probably prove especially fruitful in a field which has so long been esoteric and withdrawn.

Secondly, restriction of cryptographic information stunts the quality and quantity of amateur cryptographers -- a prime source for new men and ideas in this field. The shortsightedness of this policy will injure this nation, imperceptibly as the flow of new ideas and men slowly dries up, or frighteningly when a sudden mobilization calls in vain for cryptographers. Cryptographers cannot be trained overnight, but they will be needed overnight. Those who already know something about the subject will be available far more quickly than those who must be taught from the ground up. Further, these amateurs will have, because of their background, a far better understanding of the problems of practical cryptography than hastily war-trained men. Notably, nearly all important modern principles in the field stem from amateur inventions. Thomas Jefferson drew specifications for a cipher device 150 years ago which, slightly modified, is still used by the Army. Sir Charles Wheatstone, the famous British scientist, created an ingenious cryptograph and a cipher system so good that the British used it as a field cipher in World War I. An American electrical engineer, Gilbert S. Vernam, invented an automatic teletype-base enciphering-transmission mechanism unsurpassed today. To save a company from bankruptcy, a Swedish mechanical engineer named Boris C. W. Hagelin produced so excellent a cipher machine that both sides used it during World War II. And an American inventor, Edward H. Hebern, developed a cryptograph which, according to rumor, the government uses for top-secret communications. All of these

items embody important cryptographic principles; all have successfully met the tests of practical usage; and all have been created by amateur cryptographers -- all of which strikingly confirms the importance of amateur contributions to cryptography. The government grabs for these ideas, but unwisely rejects calls for help from possible contributors. The popularity of cryptograms in the puzzle pages of newspapers indicates a widespread interest in this subject, but the government, instead of developing this potential pool of cryptographers, actually beats down its interest by oppressive security regulations. Unless this policy is changed, what is now folly may become suicide.

Finally, the only modern authorities on cryptography who have discussed the subject of excessive secrecy both agree that greater dissemination of cryptographic information best serves the nation. The first, General Marcel Givierge, chief of the French cryptographic bureau whose work did so much to help win World War I, stated as far back as 1925 that

> "Too much secrecy is sometimes harmful; suppression of cryptographic information results in the lack of an informed personnel, while publication of general diffused knowledge of certain questions, such as that concerning transportation, does not prevent the general staff from concealing details of interest to the enemy."

The second, Yves Gyldén, author of the only scholarly history of the cryptographic bureaus in World War I, starts by condemning excessive secrecy and concludes by declaring that freedom of cryptographic information is essential to a good cryptographic service. After only four sentences of his book, he says:

> "That is, the secrecy which enshrouded almost all cryptographic activities before the war has proved itself to be a two-edged sword. The experiences of the World War proved conclusively that such secrecy most frequently does more harm than good. It prevents the spreading, among soldiers and civilians alike, of the general training in cryptography absolutely necessary for the conduct of modern warfare. It restricts the horizon of the cryptographer and lulls him into a fallacious self-conceit."

Further on: "In brief, all unnecessary secrecy is to a high degree obstructive to knowledge of and efficiency in cryptography!" And as the third of his concluding recommendations: "A maximum general knowledge of both cryptography and cryptanalysis, with the elimination of all unnecessary secrecy, should be given to the corps of officers."

Such, then, are the reasons why the New York Cipher Society believes that the present overly-restrictive cryptographic security program harms the nation. The Society feels that liberalization of the program should make available more basic cryptographic knowledge and should stimulate public interest in cryptography without disclosing any necessarily-secret results. This can be done along the lines laid down by the Association. Another way would be to release certain official publications on cryptography to the public. These books contain nothing about official ciphers and offer little if anything that is new to the science. However, they are well-written and complete, and they could fill a public demand which private industry does not fill (presumably because the demand is so small as to be unprofitable). In other sciences, the government construes such a furnishing of low-demand but important material to the public as one of its primary functions. But in cryptography -- a field vital to the national security -- it turns its back on this function. President Eisenhower's Executive Order 10450 (reorganizing the security

system) afforded the government an opportunity to downgrade these publications. Shamefully, instead of seizing that chance, the government used the order to upgrade them, thus not only making them unnecessarily hard to obtain for those interested reservists and military personnel who have a right to them, but also removing them entirely from the educational spheres of the many amateur cryptographers who could therefrom benefit themselves and their country.

The whole picture is not black, however. American cryptanalysts astonished the world with their famous prewar solution of the Japanese code. Undoubtedly the level of their accomplishment remains high: certain hints lend credence to this view. Nevertheless, the New York Cipher Society feels that even this brilliant work can be extended and improved, and that at least one way to do it would be to end the dangerous present policy of excessive secrecy. Thus can the best interests of America be served.