WDCAS-14 25 August 1947

SUBJECT: Proposed amended version of Bill S.1019

TO: Deputy Chief, Army Security Agency

1. a. The attached proposed amended version of S.1019, as adopted by the Intelligence and Security Sub-Committee of USCICC on 20 August 1947, has been carefully studied. By way of general comment, it is my opinion that because the bill is aimed directly at only one phase of matters pertaining to the security of the U.S., and especially because of the history of attempts to obtain legislation of this sort, it will excite undue attention and encounter most careful scrutiny for hidden motives, even though there are no hidden motives. Our experiences with the several attempts made in the past to have such very specific legislation enacted should be convincing in this regard. It appears to me that it would be more advisable and really easier to obtain passage of a modification to existing legislation rather than aim at brand new legislation bound to be examined with microscopic scrutiny for ulterior motives. On this possibility something further is stated below.

b. The new version is an improvement on previous attempts to correct the serious defects in the original bill, in that it eliminates the principal provision that would have been the center of much controversy, viz, Clause (3) of Sec. 1, the one that would make it a crime to publish or divulge any message which has been transmitted in a U. S. Government code or cipher.

c. Additional specific comments on the draft are contained in Par. 2 below.

2. a. The present draft still has one fatal defect, so far as its meeting the requirements of the situation which the bill is designed to meet. Under it, "whoever ... shall willfully communicate ..." shall be fined etc. It will probably be accepted by all concerned in considering this legislation that the term "willfully" means "intentionally or designedly, without lawful excuse, but not necessarily with an evil intent". "Willfully" here would imply only a person who, having asked

permission to divulge or publish classified information and having been denied such permission, then proceeds to divulge or publish the information could be indicted for his willful disregard of the prohibition. It is not that sort of violation of security that has caused us more difficulties. Recent cases of leakage of classified information have come largely from more loose talk or thoughtless action, without any willful attempt to circumvent an official prohibition. The word "willfully" should therefore be deleted.

b. On the other hand, this version, unlike S.1019, provides no procedure or means for authorizing the publication of any classified cryptologic information when this might be advisable. Thus under a strict interpretation it would be a violation for the armed services to publish documents containing classified information regarding the cryptographic or cryptanalytic activities of the services, for instructional or other purposes. The failure to provide some procedure or means of this sort should be corrected and a new Sec. 6 is proposed (see Inclosure 2).

c. The bill will very probably meet with strenuous objection from the representatives of the press. It reads: "Whoever having obtained ... knowledge of ... (3) any classified information concerning the communication intelligence activities of ... any foreign government; or (4) any classified information obtained from the communications of the United States or any foreign government by the processes of communication intelligence, shall willfully ... communicate ... or publish any such classified information shall be ... etc." This means that if an American newspaperman should obtain such information in some foreign country, he could not without expectation of serious punishment, send it to his home office in this country, nor could the editor at this home office publish it without similar expectation; the same goes for radio news, commentators, and net works. Considering how carefully the press examines any measure which even remotely might infringe upon its right to print what information it obtains, no matter how that information has been obtained, this part of the proposed bill will be a controversial issue. Unfortunately, I can recommend no change to eliminate this defect without a complete redrafting.

d. The definition, in Sec. 6, of the phrase "a person not authorized to receive such information" is probably too restrictive to be acceptable. It would means, for instance,

that the Secretary of the Treasury could not, without violating the law, disclose to the Secretary of State some classified information concerning a cryptographic system used by one of the agencies or bureaus in the Treasury Department, for example, the Bureau of Internal Revenue or the Bureau of Customs; vice versa, the Secretary of State could not disclose similar information to the Secretary of the Treasury. Nor could any foreign service officer in our diplomatic service, having obtained some information concerning the communication intelligence activities of some foreign government, disclose this information to his superiors, even to the Secretary of State himself, without violating the law. Also, Any American citizen abroad, who has in some manner or other obtained similar information and wants to communicate it to some U.S. agency where it might be useful or important, would have to make certain that the person to whom he discloses the information is authorized to receive it; he would violate the law if he disclosed it to the Ambassador or to any State Department employee in the Embassy--although presumably he would not violate the law if he disclosed it to the military or naval attaché. Furthermore, as the definition in Sec. 6 now stands, it would appear necessary, in a strict interpretation of the definition, that each and every civil service employee or officer assigned to duty in cryptologic work for the government be given written authority to receive such information, such authority to be signed by the Secretary of War, the Secretary of the Navy, or the Attorney General. This is carrying matters pretty far, it seems to me. It is suggested that Sec. 6 is not necessary and that the defects pointed out could be eliminated by changing the clause "a person not authorized to receive such information," appearing in Sec. 1, to make it read "a person not entitled to receive such information"--this being the wording in the long-standing Espionage Act. The present Sec. 6 can then be deleted.

e. The proposed bill does not make the "punishment fit the crime." It is clear that the disclosure of some piece of minor bureaucratic scandal not even remotely affecting the safety of the U.S., provided only that the information was classified (even as low as restricted) and obtained by the processes of communication intelligence, would be sufficient violation of the law to bring about the imprisonment of the offender for ten years, as well as his fining up to the sum of $10,000. It is doubtful if so stringent a proposal would meet with acceptance by the Congress, or avoid the blasts of the press. It is recommended that a graduated scale of sanctions and penalties be incorporated.

f. The proposed bill makes no allowance for the effects of the passage of time. It would, for example, be a violation of the law to publish anything about the codes and ciphers used by the Federal Army in the Civil War or about the solutions of Confederate ciphers by Federal cryptanalysts in the Civil War; on the other hand, it would not be a violation of the law to disclose information about a new cryptographic system in the research or development stage, provided it did not involve a device or apparatus. It is recommanded that the wprd "currently" be inserted in Sec. 1 before the word "classified", so as to insure that declassification would occur from time to time and that no person's safety could be impaired by a spiteful prosecution based upon disclosure of old and obsolete information.

g. There might still be some doubt as to whether or not the law would really prohibit the disclosure of information transmitted in a U.S. code or cipher. Reference is made here to clause (4): "Any classified information obtained from the communications of the United States or any foreign government by the processes of communication intelligence". It is true that the absence of a comma after "United States" probably implies that the qualifying phrase "by the processes of communication intelligence" also applies to "communications of the United States", but someday somebody might raise a question in the premises. If the clause is made to read: "Any classified information obtained from the communications of the United States ... by the processes of communication intelligence" it is obvious that such information would have to come from some foreign country, in which case, it would not be classified information within the scope of the definition given in Sec. 2, which requires that the matter be classified "by a United States government agency". I see no point in including in that clause "communications of the United States" at all, and recommend its deletion.

h. The definition of the term "communication intelligence (Sec. 5) as a field of endeavor" excludes the "intelligence" itself. This may be satisfactory for the purposes of the bill but is somewhat unusual as a definition.

i. The definition in Sec. 6, should be changed to read: "any person who, or agency which, is ...". The definition is pretty complex. Its deletion has been recommended above.

j. It is doubtful if the title of the bill should remain as it stands. How can the security of the United States be furthered by preventing disclosures of information concerning

the cryptographic systems and the communication intelligence activities of foreign governments?

3. It is still believed that a bill of much more general scope in relation to security and national defense would be preferable and moreover would receive the hearty support of all bureaus and branches of the armed forces. A suggested draft of an amendment to the so-called espionage Act of 1917 was submitted recently by this section. All references to cryptography, cryptanalysis, communication intelligence, etc., were eliminated from that draft, but the scope of the measure was broad enough to be applicable to anything of a cryptologic nature. Further, the punishments cited therein were graduated in severity, so as to make them fit the crime committed. This is believed sound in principle and it is believed that such a provision is likely to meet with more favor than would a bill wherein punishment for revealing top secret information is as severe as that for revealing restricted information. However, if there is now no possibility of presenting the AS-14 draft bill for consideration, then the present version will have to be used. A draft as amended in the light of the foregoing comments is submitted as Inclosure 2. However, as stated above, I am not able to suggest a simple change which will eliminate the objections cited in Par. 2c above.

2 Incls
2 drafts of S.1019 Bill

WILLIAM F. FRIEDMAN
Chief, Communications Research