

SECRET

CONFIDENTIAL

RESTRICTED

TO DATE 25 Jan 49 FROM TO FROM

___ Chief, ASA (10)___	___ Tech Staff (96)___
___ Executive O (11)___	___ Ch, Security Div (80)___
___ Co'r Joint Oper (12)___	___ Tech Staff (81)___
___ Deputy Chief, ASA (20)___	___ Ch, Materiel Br (82)___
___ Ch, Comm Res Sec (14) <input checked="" type="checkbox"/>	___ Ch, Methods Br (83)___
___ Ch, Hist Unit (13)___	___ Ch, Protective Br (84)___
___ Ch, Pers Sec (21)___	___ Ch, Maint Br (85)___
___ Ch, Org & Tng Sec (22)___	___ Ch, Res Lab Div (70)___
<input checked="" type="checkbox"/> Ch, Plans & Oper (23) <i>CHH</i>	___ Tech Staff (71)___
___ Ch, Materiel Sec (24)___	___ Ch, Ch Ciph & Cif Br (72)___
___ Ch, Fiscal Sec (25)___	___ Ch, Int Equip Br (73)___
___ Adjutant, ASA (26)___	___ Ch, Elec & Elec Br (74)___
___ Ch, Sec Cont Sec (27)___	___ Ch, Lab Serv Br (75)___
___ Ch, Operations Div (90)___	___ Ch, C'logic Br (76)___
___ Ch, Lab Br (91)___	___ Ch, Pers & Tng Br (61)___
___ Ch, Machine Br (92)___	___ Ch, Supply Br (62)___
___ Ch, Crypt Br (93)___	___ Co, Arlington Hall (40)___
___ Ch, Int Cont Br (94)___	
___ Ch, I & D Br (95)___	

- | | |
|--|--|
| <input type="checkbox"/> Approval & Return | <input type="checkbox"/> Information & File |
| <input type="checkbox"/> As Requested | <input type="checkbox"/> Recommendation |
| <input type="checkbox"/> Concurrence or Comments | <input type="checkbox"/> Signature if approved |
| <input type="checkbox"/> Information & Forwarding | <input type="checkbox"/> Your action by |
| <input checked="" type="checkbox"/> Information & Return | <input type="checkbox"/> Info upon which to base reply |

Have you seen this?

J

I had not seen the report # 1433
 Thanks, you very much
 CHH

File 032.1

Legislation - Esp. Act

F

Calendar No. 1480

80TH CONGRESS }
2d Session }

SENATE

} REPORT
No. 1433*Mr. Tarkenton*ENHANCING FURTHER THE SECURITY OF THE UNITED STATES
BY PREVENTING DISCLOSURES OF INFORMATION CONCERNING
THE CRYPTOGRAPHIC SYSTEMS AND THE COMMUNICATION
INTELLIGENCE ACTIVITIES OF THE UNITED STATES

MAY 28 (legislative day, MAY 20), 1948.—Ordered to be printed

Mr. BALDWIN, from the Committee on Armed Services, submitted the
following

REPORT

[To accompany S. 2680]

The Committee on Armed Services, to whom was referred the bill (S. 2680) to enhance further the security of the United States by preventing disclosures of information concerning the cryptographic systems and the communication intelligence activities of the United States, having considered the same, report favorably thereon with amendments and recommend that the bill, as amended, do pass.

AMENDMENTS TO THE BILL

Page 2, lines 24 and 25, strike out the sentence:

The term "cryptographic purposes" as used herein is correspondingly extended in the scope of its meaning.

Page 3, lines 13, 14, and 15, strike out the sentence:

The terms "communication intelligence activities" and "communication intelligence purposes" as used herein shall be construed accordingly.

PURPOSE OF THE BILL

The purpose of this bill is to prevent the revelation of important information about United States communication intelligence activities and United States codes and ciphers by persons who disclose such information without proper authority, and to prescribe penalties to those revealing such information. Stated briefly, this bill makes it a crime to reveal the methods, techniques, and matériel used in the transmission by this Nation of enciphered or coded messages. It does not control in any way the free dissemination of information which might be transmitted by code or cipher, unless that information

has been obtained by clandestine intercept and cryptanalysis. Further, it makes it a crime to reveal methods used by this Nation in breaking the secret codes of a foreign nation. It also prohibits under certain penalties the divulging of any information which may have come into this Government's hands as a result of such a code-breaking. The reason for the latter prohibition is to prevent the indication to a foreign nation that we had broken their code system.

At present two other acts protect this information, but only in a limited way. Those are the Espionage Act of 1917 and the act of June 10, 1933 (48 Stat. 122). Under the first, unauthorized revelation of information of this kind can be penalized only if it can be proved that the person making the revelation did so with intent to injure the United States. Under the second, only diplomatic codes and messages transmitted in diplomatic codes are protected. The present bill is designed to protect against publication or any other revelation, regardless of intent, of all important information affecting United States communication intelligence operations and all direct information about all United States codes and ciphers.

As the matter now stands, prevention of the disclosure of information of our cryptographic systems, exclusive of State Department codes, and of communication intelligence activities rests solely on the discretion, loyalty, and good judgment of numerous individuals. These individuals are not now prohibited from making disclosures which can be most damaging to the security of the United States. They are subject to the temptations of personal gain and the advantages of publicity in making sensational disclosures of the information within the purview of this act.

The purpose of the bill is well summarized in the quotation from the Joint Congressional Committee for the Investigation of the Attack on Pearl Harbor, which recommended, on page 253 of the report, that—

* * * effective steps be taken to insure that statutory or other restrictions do not operate to the benefit of an enemy or other forces inimical to the Nation's security and to the handicap of our own intelligence agencies. With this in mind, the Congress should give serious study to, among other things, * * * legislation fully protecting the security of classified matter.

This bill is an attempt to provide just such legislation for only a small category of classified matter, a category which is both vital and vulnerable, to an almost unique degree.

EXPLANATION OF THE BILL

The bill would make it a crime, punishable by not more than \$10,000 fine, or 10 years' imprisonment, or both, to reveal two categories of information, namely; (1) Information which would nullify the efforts of United States communication intelligence agencies, and (2) information which would permit foreign governments to read the secret official communications of the United States. Information of the first category is covered by the following phrases (qualifying "information"):

* * * concerning the nature, preparation, or use of any code, cipher, or cryptographic system of * * * any foreign government.

* * * concerning the design, construction, use, maintenance, or repair of any device, apparatus, or appliance used or prepared or planned for use by * * * any foreign government.

* * * concerning the communication intelligence activities of the United States or any foreign government.

* * * obtained by the processes of communication intelligence from the communications of * * * any foreign government.

Information of the second category is covered by inclusion of the words, "the United States or" in the first, second, and fourth of the phrases quoted above. The bill does not prohibit the publication or disclosure of United States Government messages in general.

In addition, it should be noted that the restrictions on disclosure apply only to the types of classified information defined in the phrases quoted above.

DISCUSSION

Earlier versions of this same bill (S. 805, 79th Cong., and S. 1019, 80th Cong.) would have penalized the revelation or publication, not only of direct information about United States codes and ciphers themselves but of information transmitted in United States codes and ciphers. This provision is not included in the present version. Under the bill as now drafted there is no penalty for publishing the contents of United States Government communications (except, of course, those which reveal information in the categories directly protected by the bill itself). Even the texts of coded Government messages can be published without penalty as far as this bill is concerned, whether released for such publication by due authority of a Government department or passed out without authority or against orders by personnel of a department. In the latter case, of course, the Government personnel involved might be subject to punishment by administrative action but not, it is noted, under the provisions of this bill. It is noted, further, that in such a case the representative of the press who receives and publishes the information could not be penalized under this bill, since he should certainly be able to maintain unassailably the position that he had received the information in good faith from an employee or official whose authority to give it to him it was not his business to question.

The bill, while carefully avoiding the infringement of civil liberties, extends the protected field covered by the extremely narrow act of June 10, 1933 (48 Stat. 122), the latter being of far too limited application to afford to certain highly secret Government activities the protection which they need. The need for protection of this sort is best illustrated by an account of the very circumstances which surrounded the enactment of the act of June 10, 1933. In 1931 there had been published in the United States a book which gave a detailed account of United States successes in breaking Japanese diplomatic codes during the decade prior to publication. In 1933 it was learned that the same author had already placed in the hands of his publishers the manuscript of another book which made further detailed revelations of United States success in the breaking of foreign diplomatic codes. Immediate action secured the passage by the Congress of the measure of June 10, which effectively stopped publication of the second book. Unfortunately, the first book had done, and continued to do, irreparable harm. It had caused a furor in Japanese Government circles, and Japanese diplomatic codes had been changed shortly after its appearance. The new codes were more complex and difficult to solve than the old ones, and throughout the years from then until World War II not only the Japanese diplomatic

cryptographers but the military and naval cryptographers as well were obviously devoting more study to cryptography than they ever had before. In 1934 they introduced their first diplomatic machine cipher. Year by year, their codes and ciphers improved progressively by radical steps, and United States cryptanalysts had more and more difficulty and required more and more time to break them. It can be said that United States inability to decode the important Japanese military communications in the days immediately leading up to Pearl Harbor was directly ascribable to the state of code-security consciousness which the revelations of a decade earlier had forced on Japanese officialdom.

RECOMMENDATION OF THE NAVY DEPARTMENT

There is appended a letter from the Secretary of the Navy which recites the views of the Navy Department in recommending enactment of this bill.

DEPARTMENT OF THE NAVY,
Washington, May 7, 1948.

HON. CHAN GURNEY,
Chairman of the Committee on Armed Services,
United States Senate.

MY DEAR MR. CHAIRMAN: There is transmitted herewith a draft of a proposed bill to enhance further the security of the United States by preventing disclosures of information concerning the cryptographic systems and the communication intelligence activities of the United States.

The purpose of the proposed bill is to further insure the military security of the United States by providing that the unauthorized disclosure by any person of classified information concerning the cryptographic systems and the communication-intelligence activities of the United States shall be a statutory offense.

During the war it was necessary to make a great many matters of a confidential nature accessible to a considerable number of service personnel and employees who have since been severed from their wartime duties and who may fail to safeguard official information which is within their knowledge. Existing laws do not adequately protect the security of information of this character, and it is considered of utmost urgency and importance from the standpoint of national security that legislation be enacted which will fully protect the security of classified matter. The joint committee of Congress which investigated the Pearl Harbor attack recognized this fact and in its report recommended that Congress give serious study, among other things, to "legislation fully protecting the security of classified matter."

The proposed bill represents the combined views of the Army, Navy, Air Force, Central Intelligence Agency, and the Department of State, as to the legislation which is necessary to prevent the unauthorized disclosure of such classified information. The Navy Department is sponsoring this legislation on behalf of all of the foregoing organizations. The proposed bill is submitted as a substitute for H. R. 2965, covering the same subject, which was introduced in the first session of the Eightieth Congress at the request of the Navy Department. The principal points of difference between H. R. 2965 and the bill now proposed are as follows:

The clause in H. R. 2965 providing penalties for revealing information transmitted in United States cryptographic systems has been omitted in the proposed bill. While there is still a need for a statute to protect United States cryptographic systems by prohibiting, or in some way limiting, the publication or other revelation to foreign governments, or individuals, of the texts of messages which have been transmitted in those systems, because of its controversial nature this clause has been omitted in the proposed bill in the interest of the bill's primary purpose. H. R. 2965 would apply only to persons who had acquired information by virtue of certain employment by the United States or foreign governments. Under this limitation a person who had stolen this information from the Government could reveal it with impunity. Also an individual or group of individuals

who had privately engaged in cryptanalysis of foreign systems could publish their technical results with impunity, although such publication would be just as damaging to the United States communication intelligence effectiveness as if it had been by a Government employee. The proposed bill omits the qualification as to employment. With the elimination in the proposed bill of the employment feature, there is no longer any need for the separate section 1 and section 2, which appear in H. R. 2965, one of which applies to persons employed by the United States and the other to persons employed by foreign governments. H. R. 2965, as introduced, covered "information" of certain categories, while the proposed bill covers "classified information" of these categories, and the term "classified information" is defined. This change has been made to overcome certain objections of the United States Archivist. Where the terms "cryptanalysis" and "cryptanalytic" were used in H. R. 2965, the term "communication intelligence" has been substituted in the proposed bill as being more suitable for the conveyance of the intended meaning.

The Navy Department, in conjunction with the Army, Air Force, Central Intelligence Agency, and Department of State, strongly recommends the enactment of the proposed legislation.

An identical report has been transmitted to the Speaker of the House of Representatives this date.

The Navy Department has been advised by the Bureau of the Budget that there is no objection to the submission of this report to the Congress.

Sincerely yours,

W. JOHN KENNEY,
Acting Secretary of the Navy.

80TH CONGRESS
2D SESSION

S. 2680

(H.R. 5,1019)

IN THE SENATE OF THE UNITED STATES

MAY 17 (legislative day, MAY 10), 1948

Mr. GURNEY introduced the following bill; which was read twice and referred to the Committee on Armed Services

A BILL

To enhance further the security of the United States by preventing disclosures of information concerning the cryptographic systems and the communication intelligence activities of the United States.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*
3 That whoever shall communicate, furnish, transmit, or other-
4 wise make available to an unauthorized person, or publish,
5 or use in any manner prejudicial to the safety or interest
6 of the United States or for the benefit of any foreign gov-
7 ernment to the detriment of the United States any classified
8 information (1) concerning the nature, preparation, or use
9 of any code, cipher, or cryptographic system of the United

1 States or any foreign government; or (2) concerning the
2 design, construction, use, maintenance, or repair of any
3 device, apparatus, or appliance used or prepared or planned
4 for use by the United States or any foreign government for
5 cryptographic or communication intelligence purposes; or
6 (3) concerning the communication intelligence activities of
7 the United States or any foreign government; or (4)
8 obtained by the processes of communication intelligence from
9 the communications of the United States or any foreign
10 government, shall be fined not more than \$10,000 or
11 imprisoned not more than ten years or both.

12 SEC. 2. (a) The term "classified information" as used
13 herein shall be construed to mean information which, at the
14 time of a violation under this Act, is, for reasons of national
15 security, specifically designated by a United States Govern-
16 ment agency for limited or restricted dissemination or dis-
17 tribution.

18 (b) The terms "code", "cipher", and "cryptographic
19 system" as used herein shall be construed to include in their
20 meanings, in addition to their usual meanings, any method
21 of secret writing and any mechanical or electrical device
22 or method used for the purpose of disguising or concealing
23 the contents, significance, or meanings of communications.
24 The term "cryptographic purposes" as used herein is corre-
25 spondingly extended in the scope of its meaning.

1 (c) The term "foreign government" as used herein
2 shall be construed to include in its meaning any person or
3 persons acting or purporting to act for or on behalf of
4 any faction, party, department, agency, bureau, or military
5 force of or within a foreign country, or for or on behalf
6 of any government or any person or persons purporting to
7 act as a government within a foreign country, whether or
8 not such government is recognized by the United States.

9 (d) The term "communication intelligence" as used
10 herein shall be construed to mean all procedures and methods
11 used in the interception of communications and the obtain-
12 ing of information from such communications by other than
13 the intended recipients. The terms "communication intelli-
14 gence activities" and "communication intelligence purposes"
15 as used herein shall be construed accordingly.

16 (e) The term "unauthorized person" as used herein
17 shall be construed to mean any person who, or agency which,
18 is not authorized to receive information of the categories
19 set forth in section 1 of this Act, by the President, or by
20 the head of a department or agency of the United States
21 Government which is expressly designated by the President
22 to engage in communication intelligence activities for the
23 United States.

24 SEC. 3. Nothing in this Act shall prohibit the furnish-
25 ing, upon lawful demand, of information to any regularly

- 1 constituted committee of the Senate or House of Representa-
- 2 tives of the United States of America, or joint committee
- 3 thereof.

80TH CONGRESS
2D SESSION

S. 2680

A BILL

To enhance further the security of the United States by preventing disclosures of information concerning the cryptographic systems and the communication intelligence activities of the United States.

By Mr. GURNEY

MAY 17 (legislative day, MAY 10), 1948
Read twice and referred to the Committee on
Armed Services