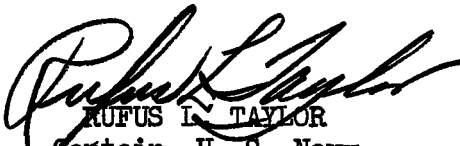プ24

USCIB: 13.5/68

24 May 1954

TOP SECRET

MEMORANDUM FOR THE MEMBERS OF USCIB:

Subject: Compromises of COMINT Codewords or Material.

1. Attached for your information is a memorandum from the Secretary, LSIB, outlining LSIB action in regard to security violations due to ineffective COMSEC practices.

2. The recommendations by GCHQ concerning specific British cryptosystems mentioned in paragraph 3 of the enclosure have been circulated as an enclosure with USCIB 13.5/55 dated 20 April 1954.

3. THIS DOCUMENT CONTAINS COMMUNICATIONS INTELLIGENCE INFORMATION AND SHALL BE HANDLED ONLY IN CHANNELS EXPRESSLY PROVIDED FOR COMINT.

RUFUS L. TAYLOR
Captain, U. S. Navy
Executive Secretary, USCIB

Enclosure
    Copy of LSIB Memo
    dated 6 May 1954

REPRODUCTION OF THIS DOCUMENT IN
WHOLE OR PART IS PROHIBITED EXCEPT
WITH PERMISSION OF THE ISSUING
OFFICE.

USCIB: 13.5/68

~~TOP SECRET~~

~~TOP SECRET~~

Oakley,
Priors Road,
Cheltenham,
Glos.

LSIB/119/54

6th May, 1954.

Executive Secretary,
United States Communications Intelligence Board.

COMPROMISES OF SIGINT CODEWORDS AND/OR MATERIAL

L.S.I.B. acknowledges receipt of five copies of U.S.C.I.B.
Directive No. 9, published in accordance with paragraph 46 of Appendix
'B' to the UKUSA Agreement. Similar instructions are being incorpora-
ted in the new version of IRSIG which will be issued shortly.

2.   In accordance with the provisions of Appendix 'B' the
Directors of G.C.H.Q. and N.S.A. have from time to time exchanged
details of the various instances of misuse of Sigint communications
from which it might be assumed that information had been compromised.
Through its concern at the large number of such misuses L.S.I.B. charged
its Security Committee, last July, with a review of the causes of the
errors occurring on U.K. communications.

3.   This review led to a list of recommendations designed to
bring about an improvement in the situation; these recommendations
have been formally adopted by L.S.I.B. and are being implemented by the
authorities concerned. A copy of the recommendations is attached at
Appendix for the information of your Board. Certain further recommenda-
tions concerning specific British cryptosystems have been communicated
by Director G.C.H.Q. to Director N.S.A.

4.   L.S.I.B. is pleased to note that the attention drawn to
this subject by the review appears to have had some effect on the U.K.
users at all levels.

5.   L.S.I.B. welcomes the revised instructions for the ASAM 2-1
cypher machine - the misuse of which had been responsible for a number
of compromises.

6.   L.S.I.B. intends to keep this subject under continuous
review and is confident that U.S.C.I.B. will take corresponding action
in view of the dangers to the common effort inherent in the misuse of
Sigint communications.

~~TOP SECRET~~   Secretary
London Signal Intelligence Board

TOP SECRET   LSIB/119/54
                                                             APPENDIX

RECOMMENDATIONS RELATING TO COMPROMISES OF
SIGINT CODEWORDS AND/OR MATERIAL.

1.   It is essential that personnel employed as Sigint cypher
operators should be specially selected to conform to high stan-
dard of quick-wittedness and that Departments and G.C.H.Q. should
select personnel with a view to ensuring that the right type of
man is employed. Particular attention should be paid to the
calibre of cypher operators posted overseas.

2.   Every effort should be made to maintain the highest possible
standard of training and particular attention should be paid to
supervision in all cypher offices where Sigint is handled. A high
standard of discipline must be maintained together with an equally
high standard of security education.

3.   Decisions concerning disciplinary action should not be taken
too hastily and should be made appropriate to the proportions of
the offence. All offences should be immediately followed by a
formal investigation.

4.   Security sections and highlights of "do's" and "don'ts" in
operating manuals and other cypher documents should be

        (i)   Printed in heavy type, or

        (ii) Printed in red, or

        (iii) Extracted and shown on inside covers.

5.   Constant attention should be paid to the efficient mechanical
and electrical working of cypher machines since the standard of
maintenance performed has a direct bearing on cypher security.

6.   Greater use of displayed slogans should be made on machines
and desks. It is appreciated that the effect of slogans is limited
by familiarity but their use should be investigated.