

~~TOP SECRET~~

24

USCIB: 13.5/55

~~APPENDED DOCUMENTS CONTAIN  
CODEWORD MATERIAL~~

20 April 1954

~~TOP SECRET~~MEMORANDUM FOR THE MEMBERS OF USCIB:

Subject: Compromises of SIGINT Information.

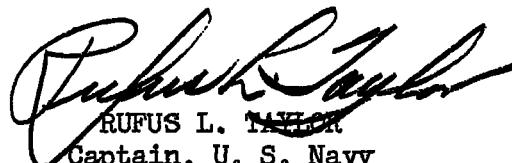
1. At the request of the Director, National Security Agency, the enclosed memorandum from GCHQ on the above subject is forwarded for information.

2. Comments by the Director, NSA, on the enclosed list of recommendations adopted by LSIB to improve the handling of certain UK crypto-systems are briefly summarized below:

"a. We are also concerned over the danger of transmitting plain-text when various on-line crypto-systems, including 5 UCO, are used and are investigating ways to prevent it.

"b. We already are printing Encipher and Decipher pads, OTP, in different colors.

"c. The recommendations regarding ROCKEX and ROLLICK are expected to result in improved security. These equipments are not being used by the U.S."

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

Enclosure

Copy of DGC/4217 dtd 26 Mar 1954.

~~APPENDED DOCUMENTS CONTAIN  
CODEWORD MATERIAL~~

USCIB: 13.5/55

Declassified and approved for release by NSA on 02-11-2014 pursuant to E.O. 13526

~~TOP SECRET~~

REF ID: A59621  
~~TOP SECRET FROTH~~

DGC/4217

26th March, 1954.

Director,  
National Security Agency.  
-----

COMPROMISES OF SIGINT INFORMATION

As a result of the proposal, referred to in DGC/3555 of 16th July 1953, that L.S.I.B. should review the whole problem of the compromise of Sigint information by misuse of Sigint communications a number of recommendations, designed to bring about a diminution in the number of such compromises, have been adopted.

2. I am glad to be able to tell you that during the period 27th July 1953 to 23rd December 1953 only three further compromises by U.K. authorities have been reported.

3. I am taking the opportunity, while sending you, at Appendix, a copy of the details of these three lapses, to ... enclose a copy of recommendations adopted by the U.K. concerning specific U.K. cryptosystems which are additional to the Regulations approved and adopted by L.S.I.B. which will be forwarded to U.S.C.I.B. shortly.

Deputy Director.

~~TOP SECRET CONTROL NUMBER~~ 54 3847  
COPY 24 OF 47 COPIES  
PAGE 1 OF 3 PAGES

~~TOP SECRET FROTH~~

Enclosure to

DGG/4217.

RECOMMENDATIONS ADOPTED BY L.S.I.B. TO IMPROVE  
THE HANDLING OF CERTAIN U.K. CYPHER SYSTEMS.

- 5 UCO (a) Highest priority should be given to the investigation of further improvement of the alarm system bearing in mind that the machine is normally handled by average personnel rather than by experts as in the field trials.
- (b) The arrangement of the jack field should be modified (and any other appropriate alterations made) to obviate errors arising from wrong connections resulting in the transmission of plain language tape.
- O.T.P. In future the "IN" copy of all one-time-pads used for Sigint communication should have the bottom right-hand corner dipped in red dye.
- ROCKEX Apart from strict attention being paid to training and supervision no further recommendations are made since the introduction of the mechanical modifications should effect the necessary improvement in security.
- ROLLICK A set of operating instructions with security sections suitably highlighted should be issued.

~~TOP SECRET CONTROL NUMBER~~ 54 884A-  
COPY 24 OF 47 COPIES  
PAGE 2 OF 3 PAGES

DGC/4217: 10

Appendix

COMPROMISES OF SIG-INT CODEWORD AND/OR MATERIAL

TOP SECRET FROTH NUMBER 54 884A  
COPY 2-4 OF 7 COPIES  
PAGE 3 OF 3 PAGES

TOP SECRET FROTH  
2  
3

TOP SECRET FROTH

No.	Date of Compromise	Circumstances	Classification	Subject Matter	Remarks	Action (other than disciplinary) taken to prevent recurrence
	27.7.53	Message transmitted by radio in clear over 5UCO by 2 Wireless Regiment, Famagusta. Operator's error leading to transmission of P/L tape being used to test circuit	SECRET codeword	[Redacted]	EO 3.3(h)(2) PL 86-36/50 USC 3605	O.C. 2 W.R. attempting to devise routine to prevent cross-patching.
	22.12.53	[Redacted]	TOP SECRET FROTH	Check and repeat of two words for corruptions (of no significance out of context) but including codeword	Possibility of interception cannot be discounted although the ROLLICK is a VIF point to point system, the codeword must therefore be considered compromised	Additional methods for preventing such error under consideration. This being a manual transmission the only satisfactory answer is strict circuit discipline.
	23.12.53	[Redacted]	CONFIDENTIAL	[Redacted]	[Redacted]	None, as the cause was due to the Assistant Circuit Controller failing to check on the mechanism after changing the key tape.