COMBINED CIPHER MACHINE (CCM). 1951 - 1952 (S-042.162)

712

UNCLASSIFIED

A8-6(1) Security Violations (Compromises)

TOP SECRET

CODE-WORD





TOP SECRET

File if we have anything else on this — otherwise, destroy
JF

DEPARTMENT OF DEFENSE
ARMED FORCES SECURITY AGENCY
Washington 25, D. C.

AFSA-12/meb
Serial 00085

~~TOP SECRET~~
TOP SECRET

16 APR 1951

MEMORANDUM FOR THE DIRECTOR OF INTELLIGENCE, U. S. AIR FORCE
ATTN: CHIEF, AFOIN-C/SR

Subject: Alleged Security Violation

Reference: Chief, AFOIN-C/SR, Memo. of 4 Jan. 51 to Chief, AFSA-02

1. The questions raised by the reference, and the correspondence and despatches attached to it, are as follows:

a. Whether AFSAG 1219 was properly classified and designated.

b. Whether distribution of AFSAG 1219 as a registered cryptographic document, rather than as a codeword document, constituted a violation of security, and caused a possible compromise of the specific codeword involved.

c. Whether the transmission of a message change to AFSAG 1219 through normal administrative channels constituted an infraction of security.

2. A review of pertinent USCIB directives and agreements and Service regulations leads to the following conclusions:

a. With the specific codeword mentioned in it, AFSAG 1219 should have been designated with the codeword. However the specific codeword should not have been mentioned in it, since this mention was contrary to USCIB Directive No. 6.

b. In view of the circumstance that all holders and users of AFSAG 1219 were indoctrinated for codeword information and actually handled it as if it were a codeword document, the distribution of it as a registered cryptographic document, rather than as a codeword document, probably did not result in an actual violation of security, or a compromise of the codeword involved.

c. Changes to AFSAG 1219 were transmitted via normal administrative channels without violation of security. Changes

MEMORANDUM FOR THE DIRECTOR OF INTELLIGENCE, U. S. AIR FORCE
ATTN: CHIEF, AFOIN-C/SR

even to actual codeword documents may be disseminated through channels other than those prescribed for COMINT documents provided the changes do not themselves reveal COMINT codeword information.

3. AFSAG 1219 has been superseded by AFSAG 1219A, which avoids mention of specific codewords, as required by USCIB Directive No. 6.

J. N. WENGER
CAPTAIN, USN
DEPUTY DIRECTOR, AFSA

CC: AFSA-00B
AFSA-00C
AFSA-00T
AFSA-111 (3)
AFSA-02
AFSA-04
AFSA-12

Mr. Murphy/471/4-6-51
RE: ESLGoodwin/meb/13 Apr 51
AFSA-11/60235

~~TOP SECRET~~

DEPARTMENT OF DEFENSE
ARMED FORCES SECURITY AGENCY
WASHINGTON 25, D.C.

Serial: 0003

5 Jan 1952

~~TOP SECRET~~ ~~SECURITY INFORMATION~~

MEMORANDUM FOR THE DIRECTOR, COMMUNICATIONS-ELECTRONICS

SUBJECT: Possible Cryptanalytic Compromise of the Combined Cipher Machine

1. On 29 December 1951, the Director, Armed Forces Security Agency, forwarded to the Joint Chiefs of Staff a memorandum on the above subject substantially as follows:

a. In JCS 2074/10, the Joint Chiefs of Staff were advised of a serious danger to security of Combined (U.K.-U.S.) communications. It was stated that they would be further advised of progress and/or the ultimate solution when reached.

b. A new procedure for using the Combined Cipher Machine has been devised which overcomes this security weakness. It has been accepted by the Cypher Policy Board in London and will be put into effect on 7 January 1952.

2. An information copy of the message being sent to the Services will be forwarded to the Joint Communications-Electronics Committee.

FOR THE DIRECTOR:

Geo E Campbell

GEO. E. CAMPBELL
Colonel, AGC
Adjutant General

Copies to: OOA
OOC
OOT
11 (3)
12 (2)
04

JHDouglas/12/60472/wm/29Dec51

~~TOP SECRET~~

~~SECURITY INFORMATION~~

~~TOP SECRET~~

DEPARTMENT OF DEFENSE
ARMED FORCES SECURITY AGENCY
WASHINGTON 25, D.C.

Serial: 000263
20 December 1951

~~TOP SECRET - SECURITY INFORMATION~~

MEMORANDUM FOR THE DIRECTOR, COMMUNICATIONS-ELECTRONICS

SUBJECT: Possible Cryptanalytic Compromise of the Combined Cipher Machine

1. On 20 December 1951, the Director, Armed Forces Security Agency, forwarded to the Joint Chiefs of Staff a memorandum on the above subject substantially as follows:

a. On 4 December 1951, Armed Forces Security Agency (AFSA) discovered a method by which messages encrypted using the Combined Cipher Machine (CCM) can be broken in a very short time when the rotors are known. This is considered to constitute a serious danger to security of Combined (U.K.-U.S.) communications.

b. The U.S. Services, the Armed Forces Security Agency Council (AFSAC), and the Cypher Policy Board in London have all been informed of this danger and requested to reduce the use of this machine to an absolute minimum pending development of corrective measures.

c. The problem of overcoming this security weakness is being given urgent priority by the Armed Forces Security Agency and the Cypher Policy Board. The Joint Chiefs of Staff will be advised of progress and/or the ultimate solution when reached.

2. The Joint Chiefs of Staff were informed that the Joint Communications-Electronics Committee would be advised of the subject matter by a separate memorandum.

FOR THE DIRECTOR:



Geo E. Campbell
GEO. E. CAMPBELL
Colonel, AGC
Adjutant General

Copies to: OOA
OOC
OOT
11 (3)
12 (2)
04

JHDouglas/12/60472/wn/20Dec51

~~TOP SECRET~~

7

DEPARTMENT OF DEFENSE
ARMED FORCES SECURITY AGENCY
WASHINGTON 25, D. C.

Serial: 000269

29 December 1951

TOP SECRET - SECURITY INFORMATION

MEMORANDUM FOR THE SECRETARY, JOINT CHIEFS OF STAFF

SUBJECT: Possible Cryptanalytic Compromise of the Combined Cipher Machine

1. The inclosure is forwarded for information of the Joint Chiefs of Staff.

2. Please furnish the Director, AFSA, with eighteen copies of the J.C.S. paper reproduced from this report.

RALPH J. CANINE
Major General, US Army
Director, Armed Forces Security Agency

Inclosure
Memo Rpt by DIRAFSA to J.C.S.,
dtd 29 Dec 51, subject as above

cc: AFSA-04 (1)
C/S (1)
OOC (1)
OOT (1)
11 (3)
12 (2)

Mr. J. H. Douglas/12/60472/dot
29 December 1951

AFSA/29 Dec 51

~~TOP SECRET~~ - SECURITY INFORMATION

MEMORANDUM BY THE DIRECTOR, ARMED FORCES SECURITY AGENCY

to the

JOINT CHIEFS OF STAFF

on

POSSIBLE CRYPTANALYTIC COMPROMISE OF THE COMBINED CIPHER MACHINE

1. In J.C.S. 2074/10, the Joint Chiefs of Staff were advised of a serious danger to security of Combined (U.K.-U.S.) communications. It was stated that they would be further advised of progress and/or the ultimate solution when reached.

2. A new procedure for using the Combined Cipher Machine has been devised which overcomes this security weakness. It has been accepted by the Cypher Policy Board in London and will be put into effect on 7 January 1952.

Inclosure with AFSA Serial 000269 dated 29 Dec 1951

~~TOP SECRET~~

OOT

7

DEPARTMENT OF DEFENSE
ARMED FORCES SECURITY AGENCY
WASHINGTON 25, D. C.

Serial: 000260

21 December 1951

~~TOP SECRET - SECURITY INFORMATION~~

MEMORANDUM FOR THE SECRETARY, JOINT CHIEFS OF STAFF

SUBJECT: Possible Cryptanalytic Compromise of the Combined Cipher Machine

1. The enclosure is forwarded for the information of the Joint Chiefs of Staff.

2. Please furnish the Director, Armed Forces Security Agency, with 18 copies of the J.C.S. paper reproduced from this report.

RALPH J. CANINE
Major General, US Army
Director, Armed Forces Security Agency

Enclosure
Memo Rpt by DIRAFSA for J.C.S.,
dated 20 Dec 51, subject as above

cc: AFSA-04 (1)
11 (3)
12 (2)
C/S (1)
OOC (1)
OOT (1)

Mr. J. H. Douglas/12/60472/dot
20 December 1951



~~TOP SECRET~~

TOP SECRET - SECURITY INFORMATION

MEMORANDUM BY THE DIRECTOR, ARMED FORCES SECURITY AGENCY

to the

JOINT CHIEFS OF STAFF

on

POSSIBLE CRYPTANALYTIC COMPROMISE OF THE COMBINED CIPHER MACHINE

1. On 4 December 1951, Armed Forces Security Agency (AFSA) discovered a method by which messages encrypted using the Combined Cipher Machine (CCM) can be broken in a very short time when the rotors are known. This is considered to constitute a serious danger to security of Combined (U.K.-U.S.) communications.

2. The U.S. Services, the Armed Forces Security Agency Council (AFSAC), and the Cypher Policy Board in London have all been informed of this danger and requested to reduce the use of this machine to an absolute minimum pending development of corrective measures. The U.S. Joint Communications-Electronics Committee (JCEC) is being informed by a separate paper.

3. The problem of overcoming this security weakness is being given urgent priority by the Armed Forces Security Agency and the Cypher Policy Board. The Joint Chiefs of Staff will be advised of progress and/or the ultimate solution when reached.

Enclosure with AFSA serial000260 of 21 Dec 51