~~TOP SECRET~~ ~~REF ID: A55077~~

File
You have one on this
Dear Sir 24

USCIB: 13/338

~~APPENDED DOCUMENTS CONTAIN CODE WORD MATERIAL~~

28 May 1953

~~TOP SECRET - SECURITY INFORMATION~~

MEMORANDUM FOR THE MEMBERS OF USCIB:

Subject: Security of COMINT Information.

The enclosure is forwarded for information at the request of the Director, NSA.

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

Enclosure
NSA Ser: 000303S dtd
26 May 53, w/1 incl.

USCIB: 13/338

~~APPENDED DOCUMENTS CONTAIN CODE WORD MATERIAL~~

~~TOP SECRET~~

Declassified and approved for release by NSA on 05-20-2014 pursuant to E.O. 13526

REF ID:A55077

~~TOP SECRET CANOE~~

This document is to be read only by those personnel officially indoctrinated in accordance with communication intelligence security regulations and authorized to receive the information reported herein.

NATIONAL SECURITY AGENCY
WASHINGTON 25, D. C.

Serial: 000303S

26 May 1953

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

MEMORANDUM FOR THE ACTING EXECUTIVE SECRETARY, USCIB

SUBJECT: Security of COMINT Information

1. During the period November 1952 - March 1953, the Director, NSA, received a considerable number of reports of incidents wherein COMINT information has been subjected to compromise. A summary of the incidents in which the Director, NSA, has determined that COMINT information must be considered potentially compromised is attached as Inclosure 1.

2. In one of the incidents summarized (paragraph 5 of the inclosure), the loss of a COMINT document can not be explained. The document is believed, however, to have been inadvertently destroyed. In all of the other incidents, COMINT information was subjected to compromise as the result of inadvertent failure to observe established rules and procedures for maintaining the security of COMINT communications.

3. The Director, NSA, has not observed thus far any positive evidence that foreign countries have exploited the compromises summarized in the inclosure. Although in some or all of these instances, the material in question actually may never have been obtained by unauthorized persons, the possibility that it has been compromised definitely exists, and the consequences must be faced.

4. As is indicated in the inclosure, certain COMINT codewords must be considered compromised. No positive security benefits would be expected to result from supersession of these codewords and no codeword changes therefore are recommended at this time.

5. It is requested that copies of this correspondence be forwarded to USCIB members for information. It is obvious that all possible effort must be exerted to prevent further compromises, and

Enclosure with USCIB 13/338 dated 28 May 1953.

REF ID:A55077

~~TOP SECRET CANOE~~

This document is to be read only by those personnel officially indoctrinated in accordance with communication intelligence security regulations and authorized to receive the information reported herein.

~~TOP SECRET CANOE~~ ~~SECURITY INFORMATION~~ Ser: 000303S

26 May 1953

USCIB members are enjoined to take all possible measures within activities under their jurisdiction to insure better security. The Director, NSA, will forward a copy to SUSLO with a request that appropriate British authorities be informed of its contents.

FOR THE DIRECTOR:

(Signed)
ALFRED R. MARCY
Colonel, US Army
Chief of Staff

Incl:
a/s

REF ID: A55077

This document is to be read only by those personnel officially indoctrinated in accordance with communication intelligence security regulations and authorized to receive the information reported herein.

EO 3.3(h)(2)
PL 86-36/50 USC 3605

~~TOP SECRET CANOE~~ - ~~SECURITY INFORMATION~~

SUMMARY OF RECENT COMPROMISES OF COMINT INFORMATION

1. A TOP SECRET CANOE message and six SECRET CHUTE messages originated at HQ NSA, and transmitted in an ORCUS system on various long-distance circuits were subjected to compromise (and must be considered compromised) because of an error which occurred on 10 November 1952 at CommSupAct, [redacted] The nature of the violation was the use of a "decrypt only" rotor arrangement at [redacted] for the encryption of two messages transmitted (ORCUS off-line) from that location. The TOP SECRET message mentioned above indicated that [redacted] communications are being exploited. The SECRET messages reveal successes in studies of [redacted] call signs, operating signals and frequency allocations.

2. On 20 December 1952, a message classified SECRET CHUTE was inadvertently transmitted in plain-language on land-line from HQ ASA, Europe, Frankfurt, to 8608 AAU, Scheyern. As a result of this transmission security violation, the message must be considered compromised. The message contains a reference to [redacted] and reveals thereby that the [redacted] has been solved and is being exploited. The report of investigation by ASA Europe stated that the two men responsible were severely reprimanded.

3. Four messages, two sent 30 December 1952, and two sent 31 December 1952, are considered compromised as the result of operator error on those dates at 8611 AAU, Baumholder. The nature of the error was re-use of ORCUS (off-line) message rotor alignments, and failure to check-decrypt prior to transmission of the messages. Each of the messages was classified SECRET CHUTE, and consisted of intercept operators' log extracts. The texts indicated some exploitation of [redacted] but no elements of cryptanalysis were indicated. A full investigation of the incidents has been conducted by ASA, Europe, whereupon it was decided that the form of logging at encrypting positions must be changed, and a formal training program must be conducted at 8611 AAU.

4. On 24 January 1953, the 6920th Security Group reported the inadvertent transmission in the clear of the COMINT codeword TWEED over an on-line APOLLO circuit between the 6920th Security Group, Johnson Air Base, Irumagawa, and the 2143rd Air Weather Wing, Tokyo. There was no clear-text transmission of codeword information. As a result of this error, the codeword must be considered compromised. The 6920th Security Group now requires that on-line operators send a preliminary stereotyped unclassified plain-language transmission prior to encipherment in such cases. This procedure should prevent recurrence of the error.

EO 3.3(h)(2)
PL 86-36/50 USC 3605

5. On 26 January 1953 the loss of [redacted] was discovered. One portion of the document was classified SECRET WITCH and the remainder was classified SECRET CHUTE. The document had been retained in a secure area at Arlington Hall Station in the custody of NSA personnel who are fully cleared and indoctrinated for COMINT. The loss has not been explained despite a thorough investigation of the incident, and the document therefore must be considered compromised. Investigating authorities are of the opinion, however, that the loss did not result from penetration or defection. This opinion is based not only upon an examination of physical security and personnel security conditions, but also upon consideration that subversive intent would be equally served and better covered if an agent merely noted that the U.S. has reconstructed These call signs. The document is believed to have been inadvertently destroyed.

6. Four SECRET CHUTE messages must be considered compromised as the result of rotor failure and failure of operating personnel to perform effective check decryption prior to transmission. The incident occurred on 11 February 1953 in an ORCUS off-line radio transmission from DET.E, 333rd Communications Reconnaissance Company, Nome, to the U.S. The messages reveal methods and successes in traffic analysis, including D/F reporting and the exploitation of [redacted] The codeword was not included in the compromised texts.

7. On 12 February 1953, a portion of a TOP SECRET CANOE message was inadvertently transmitted in the clear during an intended plain-language test transmission on land line from HQ USAFSS, Brooks AFB, San Antonio, to HQ, NSA. As a result of this violation, the clear text portion transmitted must be considered compromised. It reveals [redacted]

8. On 13 February, 1953, as the result of an operator error at 6961 Communication Security Squadron, Brooks AFB, San Antonio, a small portion of COMINT raw intercept was transmitted in the clear on a radio circuit. On-line APOLLO was intended. The transmitted portion must be considered compromised. The compromised material is CONFIDENTIAL.

9. During a two day period (2 and 3 March 1953) there were three operator errors at 6920th Security Group, Johnson Air Base, Irumagawa, in APOLLO on-line radio circuits from Japan to the U.S. In each of the three incidents, a small portion of the text of a SECRET CHUTE message was transmitted in plain language. In two of these incidents the plain language transmissions were limited to raw intercept and as a result, CONFIDENTIAL COMINT material is considered compromised. In the third incident, SECRET CHUTE evidences of successful analysis of [redacted] were sent in the clear and this information (although not the codeword in this case) must be considered compromised.