File 24

USCIB: 13.5/96

~~APPENDED DOCUMENT CONTAINS CODEWORD MATERIAL~~

24 January 1955

~~TOP SECRET - U.S. EYES ONLY~~

MEMORANDUM FOR THE MEMBERS OF USCIB:

Subject: Compromises of COMINT Information.

References: (a) CIBD #9 (Revised) dated 4 February 1954.
(b) USCIB 13.5/88 dated 8 November 1954.

1. Enclosed herewith are (a) final reports on compromises of COMINT information due to ineffective communications security initially reported in reference (b), (b) initial reports of twelve U.S. (and one British) compromises hitherto unreported, and (c) final reports on the last mentioned compromises. Inclusion of both initial and final reports were deemed necessary inasmuch as the final reports are not complete in themselves.

2. In order to prevent apparent duplicate reporting and lack of continuity, subsequent reports of compromise will be distributed only in complete final form except in cases when the nature of the compromise or other circumstances indicate that a USCIB member or the Executive Secretary needs the information immediately in order to take action thereon.

3. The twelve initial reports enclosed bring the total of this type compromise since May 1953 to 94.

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

Enclosures
1. Summaries of Compromises Reported in NSA Serial 000416S (USCIB 13.5/88).
2. Compromises of COMINT Information (NSA Serial 000519S).
3. Summaries of Compromises Reported in NSA Serial 000519S.

USCIB: 13.5/96

~~APPENDED DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~ NATIONAL SECURITY AGENCY

Summaries of Compromises Reported in NSA Serial 000416S

The following summaries complete action on the occurrences of compromises of COMINT information reported in NSA Serial 000416S, dated 15 September 1954:

a. Reference is made to the compromise of COMINT information which occurred at the 6910th Security Group, Landsberg, Germany, on 25 June 1954. In this instance the radio transmission of classified information in monoalphabetic substitution cipher resulted from use of a defective one-time key tape. Established procedures do not require an examination of tapes for defects by the user. The key tape used for this transmission was manufactured during the period 24 July 1951 through 12 May 1953. Prior to 10 June 1954, facilities were not available for effecting a 100% electronic counter check of one-time key tapes. However, on 10 June 1954, 100% electronic counter check of all three inch one-time key tapes was begun by this Agency. Statements have been received from the individuals concerned and support the facts as reported by the officer in charge. However, a description of the training program for communication security as applied to COMINT material was not included in the report received from the violating station.

b. Reference is made to the compromise of COMINT information which occurred at the 6961st Communications Squadron, San Antonio, Texas, on 23 July 1954. In this instance the teletype wire transmission of classified information in monoalphabetic substitution cipher resulted from mechanical malfunctioning of equipment. An inspection of the faulty equipment revealed that the operating cam on the main shaft had slipped, allowing the sensing pins to remain above the level of the tape guide. This prevented the tape from advancing properly to the next combination. Since the tape did not advance through the tape guide, the feed wheel stripped the feed holes in the tape. The following remedial measures have been effected by Commander, 6961st Communications Squadron to reduce the likelihood of a recurrence of a similar incident: maintenance personnel have been cautioned to ensure that the operating cam on the main shaft is properly adjusted and setscrews tightened to prevent the cam from shifting, and cryptographic operators have been cautioned to maintain an alert surveillance of key tape when operating PYTHON circuits. Statements have been received from the individuals concerned and support the facts as reported by the officer in charge. However, a description of the training program for communication security as applied to COMINT material was not included in the report received from the violating station.

~~TOP SECRET CONTROL NUMBER~~ 550019-H
COPY 24 OF 50 COPIES
PAGE 1 OF 1 PAGES

NATIONAL SECURITY AGENCY
Washington 25, D. C.

~~TOP SECRET FROTH~~

COMPROMISES OF COMINT INFORMATION

1. On 1 June 1954, a communications security violation occurred at the 1st Radio Squadron Mobile, Misawa Air Base, Japan. On that date portions of fourteen SECRET CODEWORD messages were enciphered in depth and transmitted over communications circuits composed of radio and wire links. Successful interception must be presumed and the information, including the SECRET CODEWORD, must be considered compromised. The probability of locating the depth is 95 per cent. Once the depth is located, plain text recovery is not difficult. The compromise represents a serious breach of COMINT. The following information has been revealed:

2. On 7 June 1954, a communications security violation occurred at the First Weather Wing, Tokyo, Japan. On that date portions of two TOP SECRET CODEWORD messages were inadvertently transmitted in the clear to the Fleet Weather Central, Yokosuka, Japan. Since the transmissions utilized a wire circuit vulnerable to interception, the information must be considered compromised. The subject violation, if intercepted, reveals our ability

3. On 8 June 1954, a communications security violation occurred at the 15th RSM, Osan, Korea. On that date portions of two TOP SECRET CODEWORD messages were enciphered in depth and transmitted over communications circuits composed of radio and wire links vulnerable to interception. Although this transmission is considered compromised, it is highly improbable that the depths can be located since they are very short in relation to the number of comparisons for the crypto period. The compromise involves a portion of a

~~TOP SECRET CONTROL NUMBER~~ 54-3242
COPY ____ OF 61 COPIES
PAGE 1 OF 4 PAGES

~~TOP SECRET FROTH~~

4. On 9 June 1954, a communications security violation occurred at the 1st Radio Squadron Mobile, Misawa Air Base Japan. On that date portions of nineteen SECRET CODEWORD messages were enciphered in depth and transmitted over communications circuits composed of radio and wire links vulnerable to interception. The information in depth must be considered compromised. The possibility of locating the depth is approximately 95 per cent. The compromise, very serious in nature, reveals the following COMINT:

[redacted]

5. On 21 July 1954, a communications security violation occurred at the Army Security Agency, Europe. On that date a SECRET CODEWORD and a CONFIDENTIAL message were inadvertently transmitted in mono-alphabetic substitution cipher to the 8606th Administrative Area Unit, Herzo Base, Germany. Since the circuit, composed of a wire circuit with relay points at Frankfurt, Ginnheim and Nurnberg, is vulnerable to interception, and since mono-alphabetic substitution cipher is vulnerable to cryptanalytic attack, the transmissions must be considered compromised. Although the CONFIDENTIAL message did not reveal COMINT, the SECRET CODEWORD message reveals our ability to [redacted] Further, the message disclosed, in technical terms, our difficulty in recording this type signal.

6. On 23 July 1954, a communications security violation occurred at the 1st Wireless Regiment. On that date a portion of a SECRET CODEWORD message was transmitted in the clear over a landline circuit to the 502nd Communications Reconnaissance Company, Heilbronn, Germany. Since the relevant transmission was vulnerable to interception, it must be considered compromised. [redacted]

~~TOP SECRET CONTROL NUMBER~~ 54-3242
COPY ___ OF 61 COPIES
PAGE 2 OF 4 PAGES

~~TOP SECRET FROTH~~

7. On 29 July 1954, a communications security violation occurred at the 29th Radio Squadron Mobile, Yontan, Okinawa. On that date portions of a TOP SECRET CODEWORD message were enciphered in depth and transmitted over communications circuits composed of radio and wire links vulnerable to interception to the 6920th Security Group. Successful interception must be assumed and the subject portions considered compromised. However, it is improbable that the depth in this message can be located and read since the length of the depth is small in comparison to the number of characters enciphered during this crypto period. The information compromised contains COMINT information,

8. On 7 August 1954, a communications security violation occurred at the Army Security Agency, Pacific. On that date a portion of a CONFIDENTIAL message was inadvertently transmitted in the clear over a communications circuit composed of radio and wire links to the National Security Agency, Washington 25, D. C. Since the relevant transmission was vulnerable to interception, the information must be considered compromised. The subject violation discloses our ability to

9. On 7 August 1954, a communications security violation occurred at the 6961st Communications Squadron, San Antonio, Texas. On that date a portion of a SECRET CODEWORD message was transmitted in mono-alphabetic substitution cipher over a landline circuit to the National Security Agency, Washington 25, D.C. Since the circuit was vulnerable to intercept, the mono-alphabetic portion of the subject transmission must be considered compromised. The information compromised is

10. On 8 August 1954, a communications security violation occurred at the 6961st Communications Squadron, San Antonio, Texas. On that date a portion of a SECRET CODEWORD message was inadvertently transmitted in the clear to the 10th Radio Squadron Mobile, Chicksands Priory, England. As the communications circuit carrying this transmission was composed of radio and wire links, the information must be considered compromised. The subject violation, if intercepted,

11. On 12 August 1954, a communications security violation occurred at the 15th Radio Squadron Mobile, Osan, Korea. On that date portions of two TOP SECRET CODEWORD messages were inadvertently enciphered in depth and transmitted over communications circuits composed of radio and wire links vulnerable to interception. Successful interception must be presumed and the information in depth considered compromised. The

~~TOP SECRET FROTH~~

12. On 19 August 1954, a communications security violation occurred at the Special Security Office, U.S. Air France Europe, Wiesbaden, Germany. On that date a portion of a TOP SECRET CODEWORD message entitled "USAFE Weekly Special Intelligence Summary No. 33-54", was inadvertently transmitted over a wire circuit, to the Air Force Major Relay Station Siegelbach, Germany. Since the circuit was vulnerable to interception, the information in the clear must be considered compromised.

13. On 14 September 1954, a communications security violation occurred at the Army Security Agency, Europe. On that date a portion of a TOP SECRET CODEWORD message was transmitted in mono-alphabetic substitution cipher over a wire circuit to the Special Security Office, Heidelberg, Germany. Since the relevant transmission was vulnerable to interception, the information must be considered compromised.

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

~~TOP SECRET CONTROL NUMBER~~ 54-3242
COPY ___ OF 61 COPIES
PAGE 4 OF 4 PAGES

~~TOP SECRET~~ NATIONAL SECURITY AGENCY

Summaries of Compromises Reported in NSA Serial 000519S

1. The following summaries complete action on the occurrences of compromises of COMINT information reported in NSA Serial 000519S, dated 29 November 1954:

a. Reference is made to two occurrences of compromise of COMINT information that occurred on 1 June 1954, and 9 June 1954, at the 1st Radio Squadron, Mobile, Misawa Air Base, Japan. In each instance, encipherment in depth resulted from faulty rotor stepping during encryption. An inspection of the faulty equipment revealed that a rotor stepping contact remained open when the periphery failed to close the swinger contact. The subsequent investigation of the circumstances surrounding these compromises further revealed that responsible personnel were negligent in their duties inasmuch as they failed to check decrypt the messages in accordance with prescribed procedures. Disciplinary action has been taken against the personnel concerned for noncompliance with Standard Operating Procedures, and for noncompliance with Communication Operating Instructions for COMINT Activities. Statements from the individuals concerned, and a description of the training program for communication security as applied to COMINT material were not included in the report received from the violating station.

b. Reference is made to the compromise of COMINT information which occurred at the First Weather Wing, Tokyo, Japan, on 7 June 1954. Transmission in the clear of the messages involved resulted from failure of the transmitting operator to comply with prescribed procedures upon receipt of a "break" signal from the receiving station. Because a shortage of personnel existed at the First Weather Wing at the time of this occurrence, each operator was responsible for monitoring three machines which normally run simultaneously. The investigating officer concluded that the work load of the cryptographic operator was a contributing factor to this compromise. Appropriate action has been taken to ensure that cryptographic operators receive comprehensive training in the systems in use, and in local procedures and requirements. The Special Weather Intelligence Security Officer, Headquarters, 1st Weather Wing, has requested that higher Air Force Headquarters make every effort to expedite Special Weather Intelligence clearances of personnel. Statements from the individuals concerned, and a description of the training program for communication security as applied to COMINT material, were not included in the report received from the violating station.

c. Reference is made to two occurrences of compromise of COMINT information that occurred on 8 June 1954 and 12 August 1954 at the 15th Radio Squadron, Mobile, Osan, Korea. In each instance, encipherment in depth resulted from use of incorrect enciphering procedures by the same individual.

TOP SECRET

The subsequent investigation revealed that the circumstances surrounding the violations resulted from lack of close and/or proper supervision, failure to establish operator capabilities, improper cryptocenter procedures, and lack of, or improper, training of personnel. The investigation further revealed that the operator was under a severe emotional strain which was obviously a contributing factor to his inadvertent encipherment of the subject messages. The following remedial action has been taken to preclude or reduce the likelihood of a recurrence of similar incidents: (a) The cryptosecurity officer will personally interview each operator to attempt to establish his capabilities and experience. This interview will be closely coordinated with supervisory personnel. (b) A conclusive method of instruction will be implemented in the cryptocenter to ensure the use and understanding of proper cryptocenter procedures at all times. (c) Periodic interviews will be held with personnel to ascertain that they are not under undue emotional strain. The Commander, 15th Radio Squadron, Mobile, further reports that strict compliance with proper cryptographic procedures is a subject of special emphasis and attention with all personnel. No disciplinary action has been taken or is contemplated. Statements have been received from the individuals concerned and support the facts as reported by the officer in charge. However, a description of the training program for communication security as applied to COMINT material was not included in the report received from the violating station.

d. Reference is made to the compromise of COMINT information which occurred at the Army Security Agency, Europe, on 21 July 1954. In this instance, transmission of COMINT information in monoalphabetic substitution cipher resulted from an on-line cryptographic transmission without rotors in the ASAM 2-1. The subsequent investigation revealed that the operator was negligent in his duties in failing to properly prepare the cipher equipment for on-line operation. Instructions were issued to all cryptographic personnel which require that on-line ASAM 2-1 cipher equipment be provided with rotors at all times, regardless of circuit conditions. Supervisory personnel are now charged with personal examination of the cipher equipment to ensure adherence to these instructions. The responsible operator has been given six days additional instructions in cryptographic procedures, and an official letter of reprimand by the Chief, Army Security Agency, Europe. A description of the training program for communication security as applied to COMINT material has been received. However, statements from the individuals concerned were not included in the report of investigation received from the violating station.

TOP SECRET CONTROL NUMBER 55019-C
COPY 2 OF 50 COPIES
PAGE 2 OF 5 PAGES

~~TOP SECRET~~

e. Reference is made to the compromise of COMINT information which occurred at the 1st Wireless Regiment on 23 July 1954. A SECRET codeword message, originated by the 332nd Communications Reconnaissance Company. was being relayed by the 502nd Communications Reconnaissance Group to the 1st Wireless Regiment when cipher contact was temporarily lost. The receiving operator, failing to realize he was in the "text" position, transmitted a portion of the message in the clear to indicate to the transmitting operator from which point to resume transmission. GCHQ has been informed of this occurrence. Since the violating station is a British activity, this information is forwarded for whatever action may be deemed advisable.

f. Reference is made to the compromise of COMINT information which occurred at Flight A, 29th Radio Squadron, Mobile, Yontan, Okinawa, on 29 July 1954. The compromised information was enciphered in depth as a result of rotor failure during ORCUS cryptographic operation. In this instance, the cause of the rotor failure could not be determined. The violation was not detected due to failure of the operator to completely check decrypt the message because of a heavy backlog of incoming traffic. Only one ORCUS position was available for both the breaking of incoming traffic and the check decryption of outgoing messages. The Commander, FLT A, 29th Radio Squadron, Mobile, reports that operators have been instructed to completely check decrypt all messages regardless of the amount of traffic on hand. Statements from the individuals concerned and a description of the training program for communication security as applied to COMINT material were not included in the report received from the violating station.

g. Reference is made to the compromise of COMINT information which occurred at the Army Security Agency, Pacific, Tokyo, Japan, on 7 August 1954. In this instance, the clear text transmission resulted from failure of the automatic tape feed alarm to function when the end of the roll of one-time key tape, used in conjunction with 5UCO operation, had passed through the automatic keying head. Consequently, a portion of the message was transmitted in clear text before this condition was detected. An inspection of the equipment revealed excessive wear of the commutator wheel which activates the tape feed alarm. The Chief, Army Security Agency, Pacific, had requested replacement parts for this equipment prior to this occurrence. However, replacement parts for the commutator assembly were not available at that time. In view of the circumstances surrounding this compromise, statements from the individuals concerned, and a description of the training program for communication security as applied to COMINT material were not required from the violating station.

TOP SECRET

h. Reference is made to the compromise of COMINT information which occurred at the 6961st Communications Squadron, San Antonio, Texas, on 7 August 1954. In this instance transmission in monoalphabetic substitution cipher resulted from mechanical malfunctioning of the ASAM 2-1. An inspection of the faulty equipment revealed that malfunctioning was caused by worn parts which required replacing. The machine had been given a normal 10 day maintenance inspection on 5 August 1954, and a regular 30 day maintenance inspection on 15 July 1954. Action has been taken by the Commander, 6961st Communications Squadron, to ensure a more detailed monthly maintenance inspection of the equipment. Statements have been received from the individuals concerned and support the facts as reported by the officer in charge. However, a description of the training program for communication security as applied to COMINT material was not included in the report received from the violating station.

i. Reference is made to the compromise of COMINT information which occurred at the 6961st Communications Squadron, San Antonio, Texas, on 8 August 1954. This clear text transmission resulted from failure of the operator, after receiving a garble, to adhere to the prescribed on-line break procedure while advising the transmitting operator at which point to resume transmission. The operator, not realizing he was in the "text" position, made reference to the point of correction by using actual message text rather that the appropriate line number. This compromise occurred during the evening meal, at which time an operator who normally operates only one full duplex circuit is required to operate two. The Commander, 6961st Communications Squadron, has reported that the operator responsible has been disciplined under Article 15 of the Uniform Code of Military Justice, and that an operator will never be assigned more than one full duplex circuit. A statement has been received from the individual concerned and supports the facts as reported by the officer in charge. However, a description of the training program for communication security as applied to COMINT material was not included in the report received from the violating station.

j. Reference is made to the compromise of COMINT information which occurred at the Special Security Office, U. S. Air Force, Europe, Wiesbaden, Germany, on 18 August 1954. In this instance, a newly assigned operator was performing on-line cryptographic operation under the supervision of a senior operator. The violation occurred when the operator began preparation of a tape for transmission prior to disestablishing the circuit over which a portion of the subject tape was transmitted. The responsibility for this compromise was assumed by the senior operator to whom the inexperienced operator was assigned for training. Senior operators have been given a special training course in order to

improve their instructing ability. The portion of the training program devoted to establishment and disestablishment of circuits is being emphasized. Further, the patch box lamp, which indicates the operational status of the circuit involved, has been moved to a position directly in front of the teletype operator position. A description of the training program for communication security as applied to COMINT material has been received. Statements have also been received from the individuals concerned and support the facts as reported by the officer in charge.

k. Reference is made to the compromise of COMINT information which occurred at the Army Security Agency, Europe, on 14 September 1954. The transmission in monoalphabetic substitution cipher resulted from the use of a key tape reel containing an undersized hub. This defect prevented the tape reel from rotating freely on the axle of the reel holder, and did not allow the key tape to step normally through the transmitter distributor. Since this created tension on the key tape, the feed holes became torn and caused the tape to stick over the sensing pins of the transmitter distributor. The Chief, Army Security Agency, Europe, has reported that all operators have been warned to check the fit of tape reels before use in order to ensure free rotation. The torn tape stop mechanism, which is specifically designed to prevent occurrences of this nature, is now installed on the circuit involved. A description of the training program for communication security as applied to COMINT material has been received. Statements from the individuals concerned were not required.

NOTE: In all of the above instances where it is stated that statements have not been received from the individuals concerned or that a description of the training program for communication security as applied to COMINT material was not included, the final report by the violating station was prepared prior to receipt of the National Security Agency Circular which requires this information.

TOP SECRET CONTROL NUMBER 550019-C
COPY ____ OF 50 COPIES
PAGE 5 OF 5 PAGES