24

USCIB: 13.5/107

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~APPENDED DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

15 July 1955

MEMORANDUM FOR THE MEMBERS OF USCIB:

Subject: Compromises of COMINT Information.

Reference: CIBD #9 (Revised) dated 4 February 1954.

1. The enclosed summary of eleven (11) hitherto unreported compromises of COMINT information is circulated for information. Eight (8) of the above-mentioned compromises are due to ineffective communications security while three (3) are of a physical nature.

2. A brief study of all compromises due to ineffective communications security occurring during 1954 will be circulated as soon as all final reports for that period are received.

H. D. JONES
Acting Executive Secretary, USCIB

Enclosure
a/s

~~APPENDED DOCUMENT CONTAINS CODEWORD MATERIAL~~

USCIB: 13.5/107

~~HANDLE VIA COMINT CHANNELS ONLY~~

Declassified and approved for release by NSA on 09-05-2014 pursuant to E.O. 13526

NATIONAL SECURITY AGENCY

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

~~TOP SECRET EIDER~~

COMPROMISES OF COMINT INFORMATION

1. On 16 August 1954, a COMINT compromise occurred at Detachment 2, 3rd Radio Squadron, Mobile, Northeast Cape, Alaska. On that date a CONFIDENTIAL message was transmitted in the clear to Headquarters, 3rd Radio Squadron, Mobile, Elmendorf Air Force Base, Alaska over a radio circuit highly susceptible to interception. This compromise revealed an unevaluated listing of intercepted raw traffic, and is not considered a serious disclosure. For the transmission of this message Detachment 2 employed simultaneous keying of two radio frequencies in conjunction with the PYTHON cryptosystem, one in the low frequency band, and the other in the very high frequency band. The cryptographic equipment attached to the low frequency side of the circuit was in the "cipher" position, resulting in a correctly enciphered transmission. However, the equipment being used on the very high frequency side was in the "text" position, allowing a "clear" transmission of the message. The Commander, Detachment 2, 3rd Radio Squadron, Mobile has instituted a detailed training program designed to prevent recurrences of this type of violation. Statements from the individuals concerned have been received, and support the facts as presented by the Commanding Officer. A complete outline of the station's current communications security training program has also been received, and sufficient emphasis is placed on the communications procedures violated by this compromise.

2. On 5 October 1954, a COMINT compromise occurred at the Army Security Agency, Austria, due to the loss of two copies of a SECRET codeword message. A copy of the message is not available, but has been described as [redacted] from the Army Security Agency, Austria to the 6910th Security Group. From the description of the material involved, this is considered a serious breach of COMINT. Once again our [redacted] The loss was discovered on 12 October 1954 while a message center clerk was filing messages returned by the communications center. Investigation revealed that both copies of the message were receipted for by a communication center clerk, and that the message was logged in the outgoing message log as having been transmitted on 5 October. There was no evidence, however, of the copies ever having been returned to the message center after transmission. A thorough search of the communication center, message center, and operations division failed to uncover either copy of the message. A possibility exists that these copies were inadvertently burned with the classified trash. However, since the existence or disposition of the copies could not be definitely determined, the message was declared compromised. The Commanding Officer, Army Security Agency, Austria reports that all personnel involved in this

REF ID:A59211

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

compromise have been reimpressed with their responsibility in the handling and safeguarding of classified material. Statements from the individuals concerned have been received, and support the facts as presented by the Officer in Charge. A detailed summary of the station's training program has also been received, and that portion dealing with the proper handling of classified information is considered adequate.

3. On 24 November 1954, a COMINT compromise occurred at the 3rd Radio Squadron, Mobile, Elmendorf Air Force Base, Alaska. On that date a SECRET codeword message was discovered in an unrestricted trash area, where it could have been viewed by uncleared personnel. The compromised message contained organizational information connecting the National Security Agency and certain U. S. Military and Naval stations with intercept activity. [redacted] were also included. This compromise occurred as a result of the failure of an airman to thoroughly check supposedly empty boxes for classified material before removing them from the communications center. The Commander, 3rd Radio Squadron, Mobile reports that the responsible airman has been appropriately disciplined under Article 15 of the Uniform Code of Military Justice, and that renewed emphasis is being placed on the reorientation of communications personnel in the proper handling and safeguarding of classified information. Statements from the individuals concerned have been received, and support the facts as presented by the Commanding Officer. A comprehensive description of the station's COMSEC training program has also been received, and it adequately stresses the importance of secure storage and proper destruction of classified material.

4. On 10 December 1954, a COMINT compromise occurred at the 3rd Radio Squadron, Mobile, Elmendorf Air Force Base, Alaska. On that date a copy of a TOP SECRET codeword message was discovered in an unrestricted area by an airman who was policing the grounds. This compromise revealed our [redacted] Exactly how the message was removed from the operations area to the unrestricted area in which it was found could not be definitely established. However, it is believed to have occurred while trash was being carried to an alternate burn area located in the unrestricted zone. The alternate site was being used because the incinerator located in the operations area was temporarily inoperative. The Commander, 3rd Radio Squadron, Mobile reports that if it again becomes necessary to remove classified matter from the operations area for burning, a commissioned officer will be designated to examine the condition of each container prior to removal. In addition, permission to burn classified material outside the operations area must be obtained from the Squadron Security Officer in all cases. Statements from the individuals concerned have been received, and support the facts as presented by the Commanding Officer. A complete description of the station's security training program has also been

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

received, and it provides sufficient training in the proper handling of classified material.

5. On 16 December 1954, a COMINT compromise occurred at the 8610th Administrative Area Unit, Kyoto, Japan during on-line DAPHNE operation. On that date a portion of a CONFIDENTIAL message was transmitted in the clear to the Army Security Agency, Far East over a land-line circuit presumed vulnerable to interception. This compromise [redacted] and is not considered serious. After the message had been completely transmitted from the 8610th Administrative Area Unit to the Army Security Agency, Far East, the receiving operator requested a correction. This correction request was received partially garbled, and both stations switched to the "text" position for a circuit check. Upon being informed that the test was being properly received, the 8610th Administrative Area Unit operator transmitted a tape containing the correction without switching his equipment back to the "cipher" position. The Commanding Officer, 8610th Administrative Area Unit reports that a modification, designed to prevent transmissions through the transmitter distributor while the equipment is in "text", has been installed. In addition, operators are now receiving more frequent tests to determine their knowledge and understanding of proper security procedures. Statements from the individuals involved have been received, and support the facts as presented by the Commanding Officer. A brief summary of the station's COMSEC training program has also been received, and appears to provide adequate training in the proper operation of on-line circuits.

6. On 21 December 1954, a COMINT compromise occurred at the Army Security Agency, Far East, Tokyo, Japan during ORCUS cryptographic operation. On that date portions of two CONFIDENTIAL messages were enciphered in depth as a result of the use of an incorrect message rotor alignment. The messages were subsequently transmitted over a circuit composed of radio and wire links vulnerable to interception. This compromise [redacted] Little information can be gleaned from the portions compromised. While encrypting the message the operator properly advanced the rotors from the ending rotor alignment of the previous message. However, he misread the resulting beginning rotor alignment, and entered it incorrectly in the cryptolog. He then attempted to encrypt the message, but the clear text tape was not in a usable condition, necessitating a reencryption of the message. For the reencryption, the enciphering operator manually set the rotors at the incorrect beginning alignment entered in the cryptolog, which caused the rotors to repeat a rotor alignment reached during a previous encipherment. The operator performing check decryption, after twice attempting to decrypt the message, also used the beginning alignment shown in the cryptolog instead of investigating the reason for failure of the message to decipher properly. The Commanding Officer, Army Security Agency, Far East reports that the encrypting operator has received further training in ORCUS procedures,

REF ID:A59211

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

and that the check decryption operator has been relieved as a trick chief and has received additional training, not only in procedures of each system used by the communications center, but also in the importance of these procedures to the security of the system. Statements from the individuals concerned have been received, and support the facts as presented by the Commanding Officer. A description of the station's training program for communications security has also been received, and appears to sufficiently stress the importance of strict adherence to existing instructions and procedures.

7. On 29 December 1954, a COMINT compromise occurred at the 10th Radio Squadron, Mobile, Chicksands Priory, England during on-line PYTHON operation. On that date a portion of a SECRET codeword message was transmitted partially in clear text and partially in monoalphabetic substitution cipher to the 6961st Communications Squadron, San Antonio, Texas over a circuit composed of radio and wire links vulnerable to interception. This compromise [redacted] The compromise resulted from the use of a one-time key tape containing a long stretch of "letters" characters followed by a shorter stretch of "carriage returns". The key tape involved was manufactured at a time when only limited checking facilities were available. Since that time, however, all one-time key tapes receive a one-hundred percent electronic check which should preclude future shipment of tapes containing such non-random defects. Due to the fact that this compromise was the result of a production deficiency, a statement regarding remedial action and a description of the training program of the 10th Radio Squadron, Mobile were not required.

8. On 15 January 1955, a COMINT compromise occurred at the Naval Security Group Detachment, Bremerhaven, Germany. On that date a TOP SECRET codeword message was inadvertently transmitted in the clear over a circuit composed of radio and wire links terminating at a [redacted] It could not be determined at which point the transmission terminated since it was not received at either of the receive terminals. It is believed, however, that the transmission was patched through Cuxhaven. This compromise is considered serious since it revealed the following information:

[redacted]

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

notation.

d. Our TOP SECRET COMINT codeword.

An operator at the Naval Security Group Detachment, Bremerhaven, in order to obtain a good copy of a garbled message he had just received from the Army Security Agency, Europe, used the terminal position which was normally kept as a spare position. However, the equipment ordinarily assigned to the [redacted] line. The Commanding Officer, Naval Security Group Detachment, Bremerhaven reports that all terminal positions are now numbered, with no single position designated as a spare. When a position is mechanically inoperative, the position not being used at the time immediately replaces the inoperative position and remains that circuit's terminal until further trouble is encountered. The circuits are identified by cards with large block letters specifying the distant station, and these cards, along with the appropriate keys and rotors, are transferred from position to position by the supervisor when terminal changes are necessary. Statements from the individuals concerned have been received, and support the facts as presented by the Officer in Charge. A brief description of the station's training program for communications security has also been received, and appears to provide adequate training in that phase of circuit operation applicable to this particular type of violation.

9. On 1 February 1955, a COMINT compromise occurred at the National Security Agency Communications Center during on-line PYTHON operation. On that date a portion of a SECRET codeword message was transmitted in the clear to the Army Security Agency, Europe over a circuit composed of landline and underwater cable links presumed vulnerable to interception. This compromise reveals [redacted] During receipt of the message from the Army Security Agency, Europe, cipher contact was lost on the National Security Agency side of the circuit. The operator at the National Security Agency, in an effort to regain cipher contact, switched his send side of the circuit to the "text" position, and stopped the transmission. He then transmitted a short portion of the message, while still in the "text" position, to indicate to the distant operator from which point retransmission was required. The Chief, Operations Division, reports that the operator responsible has been reindoctrinated in the proper method of making on-line correction requests, and that all operators have been alerted to the seriousness of such an occurrence. Statements from the individuals concerned support the facts as presented by the Officer in Charge. The Communications Center's COMSEC training program provides operators with adequate training in correct on-line communications procedures.

10. On 14 February 1955, a COMINT compromise occurred at Detachment 2,

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

34th Radio Squadron, Mobile, Iraklion, Crete during on-line PYTHON operation. On that date a portion of a SECRET codeword message was transmitted in the clear to Headquarters, 34th Radio Squadron, Mobile, Wheelus Air Force Base, Tripoli over a radio circuit vulnerable to interception. This compromise [redacted] While the message was being transmitted, poor cipher contact was encountered and the circuit was temporarily shut down. Upon reactivating the circuit approximately thirty minutes later, the operator at Detachment 2, 34th Radio Squadron, Mobile, thinking he had previously replaced the message tape with a test tape, turned on the transmitter distributor and transmitted the remaining portion of the message in the clear. The Commander, 34th Radio Squadron, Mobile reports that the operator responsible has been given precise instructions on all pertinent operating procedures and all techniques utilized by the Communications Center. In addition, all plain language tapes are now colored red to insure positive identification, the teletype page printer will be turned on whenever a message is being transmitted so that the operator can easily check its contents, and the communications training program has been revised with particular emphasis on the importance of strict adherence to proper procedures. Statements from the individuals concerned have been received, and support the facts as presented by the Commanding Officer. A complete outline of the revised communications security training program has also been received, and it provides operators with sufficient instruction in the operation of on-line circuits.

11. On 17 March 1955, a COMINT compromise occurred at the National Security Agency Communications Center during on-line PYTHON operation. On that date a portion of a TOP SECRET codeword message was transmitted in monoalphabetic substitution cipher to Fort Meade, Maryland over a landline circuit presumed vulnerable to interception. This compromise is considered serious since it revealed the following aspects of the COMINT effort:

[redacted]

During transmission of the message, the one-time key tape stuck over

the sensing pins of the transmitter distributor. Ordinarily this would activate the torn tape stop mechanism which would shut off the transmitting equipment. A maintenance inspection of the mechanism, however, revealed that the end of tape contacts were not functioning properly due to insufficient spring tension. To prevent future mechanical failures, maintenance personnel are required to run operational and visual checks of the torn tape stop mechanism each time they are asked to check a circuit, as well as on a regular weekly basis. Statements from the individuals concerned have been received, and support the facts as presented by the Officer in Charge. Since this violation resulted from a mechanical failure, no statement regarding communications training is included. The frequent inspections of the torn tape stop mechanism now required greatly reduce the likelihood of a recurrence.