

USCIB: 13.5/81

3 September 1954

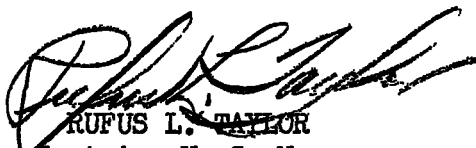
~~TOP SECRET~~MEMORANDUM FOR THE MEMBERS OF USCIB:

Subject: Corrective Measures for Control of COMINT Compromises
Due to Ineffective Communications Security.

Reference: USCIB 5.4/12 dated 15 June 1954.

1. The enclosed Report is submitted by the Director, NSA in implementation of the recommendation contained in paragraph II C.2. of the reference which was approved by USCIB as of 14 July 1954. The enclosure is for consideration in connection with item 4 of the agenda for the 106th Meeting of USCIB to be held Friday, 10 September 1954.

2. THE ENCLOSURE WITH THIS MEMORANDUM CONTAINS COMMUNICATIONS INTELLIGENCE INFORMATION AND SHALL BE HANDLED ONLY IN CHANNELS EXPRESSLY PROVIDED FOR COMINT.


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

Enclosure
a/s

USCIB: 13.5/81

~~TOP SECRET~~



NATIONAL SECURITY AGENCY
WASHINGTON 25, D. C.

Serial: 000407-S
3 Sep 1954

~~TOP SECRET~~

MEMORANDUM FOR THE MEMBERS OF USCIB

SUBJECT: Status Report on Action Taken by the Director, NSA, to Improve COMSEC in the COMINT Elements Under His Operational or Technical Control

- References:
- (a) USCIB 13/358 of 10 Aug 53
 - (b) USCIB 13/371 of 27 Aug 53
 - (c) USCIB 13.5/5 of 23 Sep 53
 - (d) USCIB 13.5/16 of 21 Oct 53
 - (e) USCIB 13.5/26 of 13 Nov 53
 - (f) USCIB 13.5/36 of 8 Feb 54
 - (g) USCIB 13.5/42 of 8 Mar 54
 - (h) USCIB 5.4/12 of 15 Jun 54
 - (i) USCIB 13.5/76 of 29 Jun 54
 - (j) USCIB 5.4/15 of 8 Jul 54
 - (k) NSCID No. 9

1. In forwarding the inclosed status report, it is considered appropriate that a review of events to date, and comments on them, be supplied as well.

2. In reference (a), the Executive Secretary, USCIB, expressed concern over the high percentage of COMINT compromises that were due to ineffective communications security, and recommended that the Director, NSA, be instructed to take certain specific actions, including inspections if necessary, to remedy the situation. Modifications to this proposal were recommended in references (b) and (c). A basic change proposed was the elimination of the inspection clause; instead, the Director would be requested to establish and submit for approval by the Board minimum standards governing communications security systems, procedures, practices and training programs to be

~~TOP SECRET CONTROL NUMBER~~ 54-2454-A

COPY OF 48 COPIES
PAGE 4 OF 4 PAGES

followed by all USCIB members in the transmission of COMINT by electrical means. A draft Directive #12 embodying the elements considered necessary to provide corrective action was circulated by reference (d). Reference (e) reported interim approval of this directive pending action by the Executive Secretary to combine Directives #6, 9 and 12 into one paper as recommended by the Director. This was done, and the new draft Directive #9, circulated to the members on 11 December 1953 for approval, was finally approved on 4 February 1954.

3. In the meantime, the Director had been requested to establish the minimum standards and to submit them to USCIB for approval. An initial effort in this direction was the submission by the Director of "Security Requirements for Transmission of COMINT by Electrical Means," which statement was circulated for approval to the members of USCIBEC as an inclosure to reference (f). As a result of divergent views on the part of the members of USCIBEC, a compromise draft was resubmitted as an inclosure to reference (g). This draft was approved by USCIBEC on 4 March 1954, and by the Board on 17 March 1954. Reference (h), the Annual Report of the Executive Secretary, USCIB, stated, however, that the minimum standards had not yet been submitted for USCIB approval, and contained a recommendation that the matter be expedited. At the 16th USCIBEC meeting on 25 June 1954, the NSA member pointed out that reference (g) was intended by NSA to serve as the minimum standards. By reference (i), therefore, the USCIB members were requested to indicate acceptance or non-acceptance of reference (g) as the minimum standards. Reference (j) reported acceptance.

4. The inclosed report is submitted in compliance with a second recommendation of the Executive Secretary in reference (h), viz., that the Director be asked to prepare and forward in time for USCIB consideration at its September meeting a status report on action taken to improve communications security in the COMINT elements under his operational or technical control together with any recommendations he might deem appropriate.

5. The problem of providing and maintaining communications security for COMINT is, essentially, not the formulation of new rules nor the establishment of new procedures, but rather the institution of positive checks and guarantees that existing rules will be meticulously observed, and prescribed procedures followed. Reference (a) outlined the basic problem with considerable clarity when it stated: "Experience in the Armed Forces has demonstrated that even if cryptographic systems and procedures are sound, good communications security can be achieved only through elimination of poor practices and personnel failures." The grave responsibility of command for the maintenance of communications security, with particular emphasis on adequate training and indoctrination of communications personnel, is outlined in detail in Communications Instructions, Part II-Security (ACP 122B) and Principles of Transmission Security (AFSAG 1248).

~~TOP SECRET~~ CONTROL NUMBER 54-2454-A
COPY _____ OF 48 COPIES
PAGE 2 OF 4 PAGES

~~TOP SECRET~~

Serial: 000407-S

6. Of the total compromises to date of COMINT information due to communications insecurities, a small number have been traceable to faulty equipment. A somewhat larger number have resulted from cryptographic violations, - either failure of the cryptographers to comply with the operating instructions for the cryptosystem concerned, or failure to perform properly and completely the check-decryption process. Errors in this category are ordinarily due to partial ignorance of the rules or insufficient training and experience in their application, and less frequently to inattention or carelessness. Additional training and experience, therefore, can be expected to result in a degree of technical competence that could virtually eliminate this type of error.

7. Technical competence in the operation of crypto-aids, however, is not enough. It is an alarming fact that more than half of all compromises of COMINT information continue to involve transmission in the clear on interceptible wire or radio circuits; and it is an additional cause for concern to note the high percentage of these clear text transmissions that are due directly to inattention or carelessness on the part of the operators. It will be noted that, in the corrective action outlined in the inclosed report, attention has in the past been focused on equipments and procedures, and the main effort has been expended in improving both. It is the Director's opinion that, in improving the tools, and issuing the instructions, too little attention perhaps has been given to the fallible human beings who must use the tools and follow the instructions. For this reason, preventive and corrective action in the future should place increased and continued emphasis on specific guides and criteria for the training and indoctrination of personnel, and on the basic responsibility of command to develop in subordinates a deep sense of personal responsibility for the maintenance of communications security.

8. The prosecution of a successful training and indoctrination program will require the exercise of continued and rigid administrative control, including strict disciplinary action when considered necessary. Subparagraph 2g of reference (k) appears to fully authorize such exercise by the Director, NSA, since it states: "The Director shall exercise such administrative control over COMINT activities as he deems necessary to the effective performance of his mission. Otherwise, administrative control of personnel and facilities will remain with the departments and agencies providing them." Although the exercise of administrative control by the Director, NSA, is contemplated in reference (k), assumption of such control by the Director would require a realignment of existing command and administrative processes. In the conviction that such a realignment should not be necessary, it is the Director's present intention to continue to act through and in collaboration with the military

~~TOP SECRET CONTROL NUMBER~~ 54-2454-A
COPY _____ OF 48 COPIES
PAGE 3 OF 4 PAGES

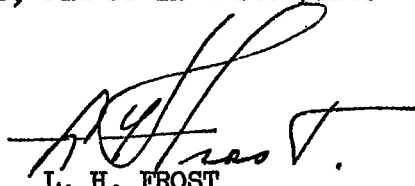
~~TOP SECRET~~

Serial: 000407-S

services to obtain the imposition of necessary administrative controls. The success of this cooperative effort in implementing an adequate program of indoctrination and training and in effecting the prompt adoption of all measures recommended for the maintenance and improvement of communications security will determine whether or not more direct control would be desirable or necessary.

9. The inclosed status report is presented more as an itemized chronology than as a strict narrative, and is in three parts.

FOR THE DIRECTOR:



L. H. FROST
Rear Admiral, U. S. Navy
Chief of Staff

Incl:
a/s



~~TOP SECRET CONTROL NUMBER 54-2454-A~~
COPY _____ OF 48 COPIES
PAGE 4 OF 4 PAGES

~~TOP SECRET~~

1 September 1954

STATUS REPORT ON ACTION TAKEN BY THE DIRECTOR, NSA,
TO IMPROVE COMSEC IN THE COMINT ELEMENTS UNDER HIS
OPERATIONAL OR TECHNICAL CONTROL

PART I - Action Taken to Eliminate Plain Language Transmission
On-Line of Classified Information.

- A - Wiring Modification to 131B2 Subset and Model 19 Teletypewriter
- B - Torn-tape Stop Mechanism
- C - AFSAG 1262-1
- D - Modification for SSM-3 and TT-160/FG Equipment
- E - Summary

PART II - COMINT Cryptosystems and Communications Security.

- A - Research, Development and Improvement of Cryptosystems for COMINT Use.
- B - Authorization of COMINT Cryptosystems
- C - Communications Security Surveillance and Compromise Reporting Procedure

PART III - Additional Corrective Action Contemplated

~~TOP SECRET CONTROL NUMBER~~ 54-2454-B
COPY _____ OF 48 COPIES
PAGE 1 OF 12 PAGES

Incl

TOP SECRET

PART I

Action Taken to Eliminate Plain Language On-Line Transmission
of Classified Information

Initial Statement of Problem

On 31 July 1951, the Director, in serial 00390, invited the attention of the Service Cryptologic Agencies to the fact that plain language transmissions by intercept stations of classified material were increasing. He stated that most of the instances noted were directly attributable to errors committed by crypto-operating personnel as a result of failure to comply with existing crypto-operating instructions. He further requested that appropriate action be taken to remind all concerned personnel of the Service Cryptologic Agencies and their field activities of the potential seriousness of such plain language transmissions, and to insure that maximum alertness to prevent such occurrences was maintained.

Section A - Wiring Modification to 131B2 Subset and Model
19 Teletypewriter

1. On 31 March 1952, the Navy submitted to AFSA a proposed wiring modification to the subscriber set 131B2 and model 19 teletypewriter, to aid in eliminating inadvertent or accidental plain text tape transmission while still permitting plain language operation from the keyboard. The slight wiring modification, which could be accomplished in the field, utilized the tape-out button on the front of the military model 19 thus precluding the possibility of any plain text going to the line unless the tape-out button were deliberately depressed.

2. The Navy proposal was accepted by AFSA as a satisfactory aid toward solution of the problem, and, in June 1952, the first steps were taken toward preparing the necessary instructions for making the modification and designing modification kits for the commercial type model 19A table which has no tape-out button.

3. On 25 July 1952, the Director, in serial 1647, informed the Service Cryptologic Agencies that "the increased frequency of violations caused by the inadvertent transmission of classified plain language tape while utilizing on-line operation of the 131B2 subset has demonstrated the need for incorporation of a feature which will reduce this possibility." Instruction sheets and diagrams to effect the slight wiring modification were inclosed, with the recommendation that the modification be accomplished wherever feasible and appropriate. This recommendation was not limited to COMINT circuits.

~~TOP SECRET CONTROL NUMBER~~ 54-2454-B
COPY OF 48 COPIES
PAGE 2 OF 12 PAGES

~~TOP SECRET~~

~~TOP SECRET~~

4. The Navy took immediate action to make the modification a necessary condition for approval of on-line operation at all Navy terminals.

5. On 14 August 1952, the Army Security Agency stated that investigation had revealed that, within the Army, inadvertent plain language transmissions were extremely infrequent, and that, in view of operational difficulties attendant upon effecting the modification, the Army could not accept it and no action would be taken at that time.

6. On 2 September 1952, the Air Force Security Service stated: "Records of security violations compiled at this headquarters do not indicate a serious trend in the type of violation under consideration. Recurrence rate is not increasing but has remained stable at a low level." The possibility that all violations were not being reported was recognized, however. AFSS stated further that, since the proposed modification would reduce the probability of operator error, it was a desirable feature, provided the magnitude of the modification program was in consonance with the degree of protection afforded. A survey of the major users of model 19 on-line systems would be undertaken to determine the conditions under which modification would be desirable and necessary. In indorsing this reply, USAF Headquarters expressed the opinion that the magnitude of the additional equipment modification program would not be in consonance with the degree of protection afforded. Decision would be withheld until the survey of the major users was completed.

7. Between 1 August 1952 and 24 August 1953, the following number of compromises of COMINT information through inadvertent plain language transmissions were reported:

- ARMY - 7
- NAVY - 1
- AIR FORCE - 10
- NSA - 3

8. On 24 August 1953, the Director, in his serial 00681, addressed to the Service Cryptologic Agencies, made reference to his previous suggestion (see paragraph 3 above) that wiring modification be made to 131B2 subsets and model 19 teletypewriters to reduce the frequency of these violations. He stated that he was aware that the Army and Air Force had not accepted the suggested modification for general use within their Services; however, the fact that compromises of COMINT information were continuing to occur through operator error when using equipments that had not been modified revealed the necessity that the modification be made on all 131B2 - model 19 teletypewriter installations used in passing COMINT traffic. The addressees were requested to accomplish the modification as

~~TOP SECRET CONTROL NUMBER~~ 54-2454-B
COPY OF 48 COPIES
PAGE 3 OF 12 PAGES

~~TOP SECRET~~~~TOP SECRET~~

soon as possible at all COMINT activities under their administrative control, and to inform NSA when this action was completed.

9. On 4 September 1953, the Army Security Agency stated that action was being taken to complete the modifications. By February 1954, they were completed (see Section E- Summary).

10. On 9 September 1953, USAFSS Headquarters reported that the modifications would be completed as soon as the required information could be disseminated to COMINT activities under its administrative control. They have not yet been completed (see Section E- Summary).

Section B - Torn-Tape Stop Mechanism

1. In the meantime, on 25 July 1952, the Navy had also submitted to AFSA for security evaluation an additional safeguard against inadvertent clear text transmission--installation of the "torn-tape" mechanism devised by the Teletype Corporation to prevent transmission of clear or monoalphabetic substitution text due to malfunctioning of the SIGTOT equipment when the 131B2 subset is in the "CIPHER" position. This additional modification proposal was favorably received by AFSA, and the Navy was informed that the "torn-tape" device would be subjected to complete evaluation, including the economic and security viewpoints. After preliminary evaluation, the Director, on 6 November 1952, initiated action on a project which would insure production and delivery of the "torn-tape" or similar device as expeditiously as possible. Following further and more complete evaluation of the device from the standpoint of economy, practicability and installation, it was (on 6 January 1953) declared satisfactory and recommended for installation in the field.

2. On 30 January 1953, the Director, in his serial 092, notified the Service Cryptologic Agencies that the torn tape mechanism (which the Navy had demonstrated to the Air Force and Army in mid - 1952) was available for coordinated procurement by NSA during Fiscal Year 1953. He stated that a complete evaluation of the mechanism had been made by NSA, that it was deemed worthwhile from a security, operational and economic standpoint, and requested that requirements be forwarded to NSA no later than 1 March 1953.

3. On 10 February 1953, the Army Security Agency stated that the Army had no requirement for the mechanism.

4. On 16 February 1953, the Navy expressed a requirement for 300 units, provided the device referred to was that recommended by the Navy in July 1952. On 26 February 1953, the Director, in serial 0196, confirmed the fact that the device was the same.

~~TOP SECRET~~ CONTROL NUMBER 54-2454-B
 COPY _____ OF 48 COPIES
 PAGE 4 OF 12 PAGES

~~TOP SECRET~~

~~TOP SECRET~~~~TOP SECRET~~

5. On 27 February 1953, Headquarters USAF confirmed the Air Force requirement (verbally indicated in December 1952) for 1600 units.

6. On 23 April 1953, a contract was let by NSA utilizing Navy and Air Force funds for 1900 Torn Tape Stop Mechanisms. Delivery was scheduled to commence in November 1954 at the rate of 200 per month.

7. On 1 September 1953, however, following receipt of USCIB 13/358 dated 10 August 1953, the Director took action to expedite procurement of 50 (tentative estimate) torn tape modification units for installation as soon as possible on COMINT on-line PYTHON equipments. Delivery of 500 units was promised in March 1954, the first 50 of which were planned for COMINT use.

8. Due to several shipment date changes made by the manufacturer (Teletype Corporation), delivery of the first 50 units to NSA was not made until 17 June 1954.

9. On 29 and 30 June 1954, in separate messages, the three Service Cryptologic Agencies were informed that initial shipments of the device (Army-15; AF-4; Navy-4) were being made, and that its installation was required on all terminal equipment used for on-line PYTHON COMINT communications. These 23 units will permit installation of the torn-tape mechanism on all Army, Navy and Air Force terminal equipments of circuits for PYTHON operation with NSA. A direct shipment by the manufacturers to the Air Force to permit additional installations was scheduled for early July.

10. Installation of the mechanism on all NSA terminals of on-line PYTHON COMINT circuits was completed on 6 July 1954.

11. On 7 July 1954, shipment was completed on 4 torn-tape mechanisms to SUSLO London for installation on the UK Terminals of combined on-line PYTHON COMINT circuits.

12. Post-installation study of the device was continued by NSA, and a malfunctioning of the latch on the tape retaining lid was observed. On 20 July 1954, the Service Cryptologic Agencies and NSA UK were notified by message of this malfunction, and advised that all torn-tape mechanisms should be inspected to insure that the latching surfaces were smooth and correctly aligned to prevent faulty sensing of the key tape. It was further stated that all operating personnel should be cautioned to insure that the tape retaining lid is completely down and firmly latched. In the meantime, the manufacturer has been advised to undertake modification of the assembly to eliminate the defect.

~~TOP SECRET CONTROL NUMBER~~ 54-2454-B
 COPY OF 48 COPIES
 PAGE 5 OF 12 PAGES

~~TOP SECRET~~

~~TOP SECRET~~

Section C - AFSAG 1262-1

1. On 12 September 1952, the Director, in his serial 000264, informed the Service Cryptologic Agencies that, in view of continuing expansion in the COMINT field and the attendant increase in associated communications, all possible steps had to be taken to avoid any communications security weaknesses, particularly those which would present evidence of the degree of success of the U.S. COMINT effort to foreign traffic analysts. Principles were summarized for the guidance of those concerned with planning for COMINT activities, or with distribution and use of special purpose cryptographic material for COMINT purposes. These principles were virtually identical with the now accepted "minimum standards" outlined in USCIB 13.5/42 dated 8 March 1954. One of the general principles enunciated was a statement that, because of the danger of inadvertent clear text transmissions through operator negligence, on-line APOLLO or PYTHON cryptographic operation for transmission of codeword material should be authorized only where absolutely essential for successful operations and only with the approval of the Director, AFSA, in each instance. In those cases where on-line communications operation was authorized, modification of equipment (see Part I, Section A, paragraph 3) to reduce the possibility of inadvertent plain language transmission was prescribed.

2. In the year that followed, during which time the Army and Air Force had neither accepted nor effected the suggested modification, compromises due to inadvertent plain language transmission continued to occur. In August 1953 (see Part I, Section A, paragraph 8) the Director notified the Service Cryptologic Agencies that the modification was required at all COMINT activities.

3. On 21 October 1953, the Director, in his serial 00812, took additional action in this matter. He informed the Service Cryptologic Agencies that, due partially to the increasing demand for and use of on-line systems for COMINT, and the continued high rate of inadvertent plain language transmissions occurring in on-line operation, there existed a requirement to extend and clarify the on-line policy summarized in paragraph 1 above. The letter requested specific information concerning each on-line circuit requested or already approved and in operation, and inclosed a list of authorized terminal arrangements including equipment, general cryptosystems, and operating instructions. He stated that these terminal arrangements represented the minimum security safeguards currently acceptable for on-line operation in COMINT communications. He indicated that it was planned to publish the inclosure as a registered cryptopublication for dissemination to COMINT units.

4. In February 1954, the inclosure, modified somewhat in accordance with comments and suggestions by the Services, was published as AFSAG 1262-1 (Terminal Arrangements Authorized for On-line Cryptographic Operation in Communication Intelligence Activities - Joint).

~~TOP SECRET CONTROL NUMBER~~ 54-2454-B
COPY _____ OF 48 COPIES
PAGE 6 OF 12 PAGES

~~TOP SECRET~~~~TOP SECRET~~Section D - Modification for SSM-3 and TT-160/FG Equipment

1. On 19 March 1954, the Director, in his serial 0336, notified the Service Cryptologic Agencies that, as a further aid in reducing the likelihood of inadvertent plain language transmissions in on-line cryptographic operation, a modification had been devised for the SSM-3 and TT-160/FG (SAMSON) equipments. The modification, similar to the wiring modification to the 131B2 subset and model 19 teletypewriter described in Section A above, would require the depression of a spring-loaded switch for transmission from the transmitter-distributor except when the mixer was in the "CIPHER" position. Draft instructions for the modification were inclosed, and early comment by the addressees was requested in view of the plan to publish the modification instructions as Appendices to AFSAG 1262-1.

2. Replies to the above serial were submitted by the Navy on 29 March 1954, the Army on 6 April 1954, and the Air Force on 23 April 1954. In their replies, each of the Services suggested specific changes to the proposed modification instructions.

3. The various Service comments and recommendations have been carefully considered and evaluated and, in general, accepted; and draft Appendices to AFSAG 1262-1 have been prepared incorporating accepted changes.

Section E - SUMMARY

1. The directives of 24 August 1953 (see Part I, Section A, paragraphs 8, 9, 10) and 21 October 1953 (see Part I, Section C, paragraph 3) required, respectively, that a wiring modification be made to 131B2 subsets and model 19 teletypewriters employed for COMINT, and that specific information concerning COMINT on-line terminal arrangements (including modifications effected) be submitted to NSA.

2. The Navy reported on 9 December 1953 that the required modification had been made. The Army reported the same on 3 February 1954. Each report supplied the on-line terminal arrangement information requested. The Army has since (on 28 July 1954) submitted voluntarily a second report indicating the current status.

3. The Air Force, on 15 December 1953, stated that action was being taken to review existing COMINT circuits operating on-line, and that the information requested by NSA serial 00812 of 21 October 1953 (see paragraph 1 above) would be compiled and forwarded in approximately 90 days. Since then, interim and partial reports have been submitted from time to time, but, to date, the complete report has not been received. The only area on which complete information is available is Alaska; all modifications on Air Force circuits in that area were finally completed on 6 July 1954.

~~TOP SECRET CONTROL NUMBER~~ 54-2454-B
 COPY _____ OF 48 COPIES
 PAGE 7 OF 12 PAGES

~~TOP SECRET~~

~~TOP SECRET~~

4. A tabulation of the number of compromises due to inadvertent plain language transmissions reported during the period 1 October 1953 through 31 July 1954 appears below. Although it is quite conceivable that the figures represent an increase not in actual number of occurrences, but in the number of reports (see Part II, Section C, paragraph 2), they undoubtedly also reflect to some degree the speed of compliance by the Services with the modification instructions. The following compromise reports were received during the periods indicated:

Army (1 Oct 53-31 Jan 54)	5
(1 Feb 54-31 Jul 54)	<u>12</u>
	17
Navy (1 Oct 53-31 Jul 54)	1 (on 1 Feb 54)
Air Force (1 Oct 53-31 Jul 54)	34
NSA (1 Oct 53-31 Jul 54)	6

5. It will be noted that a number of Army compromises occurred after the wiring modification was effected. This is evidence of the fact that equipment modifications alone are not a panacea. It is also considered a further corroboration of the statement by the Executive Secretary, USCIB, in USCIB 13/358 that "even if cryptographic systems and procedures are sound, good communications security can be achieved only through elimination of poor practices and personnel failures."

6. It is too early as yet to determine or evaluate what effect installation of the Torn Tape Stop Mechanism and the modification described in Part I, Section D will have in reducing the number of compromises. It is, however, reasonable to forecast a reduction in personnel errors, provided that reliance for this reduction is placed not on the modifications alone, but also on a comprehensive and realistic program of training and indoctrination (see Part III).



~~TOP SECRET CONTROL NUMBER 54-2454-B~~
COPY _____ OF 48 COPIES
PAGE 8 OF 12 PAGES

~~TOP SECRET~~

PART II

COMINT Cryptosystems and Communication Security

Section A - Research, Development and Improvement of
Cryptosystems for COMINT Use

1. In October 1952, the cryptographic security and flexibility of COMINT communications was greatly increased by the introduction of ORCUS cryptosystems for use with ASAM 2-1. ORCUS replaced all MINERVA and most APOLLO systems.

2. Early in 1953, a new ASAM 2-1 cryptosystem, designated GALATEA, was introduced. It had definite operational advantages over on-line APOLLO, but required extreme care and rigid procedural control in order to avoid compromise through re-use of key.

3. On 31 August 1953, the Director, in his serial 00695, informed the Service Cryptologic Agencies that another new ASAM 2-1 cryptosystem, designated DAPHNE, had been devised and that, in addition to overcoming the ORCUS and GALATEA security hazard of messages in depth, it would provide considerable advantages over earlier ASAM 2-1 systems in most of their applications. A draft of DAPHNE operating instructions was inclosed, and early comment by the addressees was requested.

4. Comments from the three Services indicated general concurrence with the application of the DAPHNE cryptosystem as described. Accordingly, the conversion of all on-line ASAM 2-1 operation to DAPHNE was begun.

5. During the period 16 February through 17 March 1954, a test of DAPHNE off-line operation between USM 4 (ASMARA) and NSA was conducted to determine what problems would be encountered in the field stations and in the NSA CommCenter in the event that DAPHNE replaced ORCUS for the forwarding of raw traffic off-line. The test revealed that DAPHNE has definite advantages from a security viewpoint and, in general, meets requirements for processing raw traffic.

6. In the meantime, an improvement to the DAPHNE cryptosystem, embodying a modification to the ASAM 2-1 machine itself in the form of a pluggable endplate, has been under development. The procedures for both on-line and off-line operation will be similar to DAPHNE and the cryptosystem will be known as GORGON. The pluggable endplate

~~TOP SECRET CONTROL NUMBER 54-2454-B~~
COPY _____ OF 48 COPIES
PAGE 9 OF 12 PAGES

~~TOP SECRET~~

will materially increase the security of the ASAM 2-1 against crypt-analytic exhaustion attack, and will also allow the transmission of pure key. The latter feature will be of assistance in establishing and maintaining synchronization and in facilitating traffic flow security operation.

Section B - Authorization of COMINT Cryptosystems

1. In furtherance of one of the requirements of NSA serial 000264 of 12 September 1952 (see Part I, Section C, paragraph 1) and paragraph 8 of USCIB 13.5/42, viz. that cryptosystems for use in COMINT communications be specifically authorized, the Director periodically forwards to each of the Services lists of cryptosystems so authorized and the current holders of each. Similar listings for the State Department, CIA and FBI are now in preparation.

Section C- Communications Security Surveillance and
Compromise Reporting Procedure

1. Concurrent with the introduction of ORCUS in October 1952, NSA began studies and analyses of the COMINT communications of the three Services. Compilations of violations of communications security as applied to COMINT were made, and, early in 1953, the first of a series of summary reports of violations were forwarded to the Heads of the Service Cryptologic Agencies. These reports covered the period October, November and December 1952, and were provided with the expressed primary purpose of providing guidance in improving the security of COMINT communications.

2. On 29 April 1954, the Director published NSA Circulars 90-1 and 120-2 containing instructions for reporting compromises and possible compromises of COMINT information and COMINT codewords. the Circulars establish reporting responsibilities and procedures for elements under the operational and technical control of the Director, NSA. It was recently determined that Circular 90-1 was insufficiently detailed and possibly open to misinterpretation; it has therefore been amplified and clarified, and a revision was distributed to the Services.

3. On 6 May 1954, in serial 00143S, the Director supplied the Executive Secretary, USCIB, with similar reporting procedures for the guidance of all activities which are engaged in electrical transmission of COMINT information, but which are not under the Director's technical or operational control. This serial was circulated to the USCIB members as an inclosure to USCIB 13.5/61 dated 10 May 1954.

~~TOP SECRET CONTROL NUMBER 54-2454-B~~
COPY _____ OF 48 COPIES
PAGE 10 OF 12 PAGES

~~TOP SECRET~~

PART III

Additional Action Contemplated

1. Issue to the Service Cryptologic Agencies for further issue to the elements under the operational or technical control of the Director, NSA, of detailed check-off lists covering general, cryptographic and transmission security and the physical security of cryptographic material, with separate detailed check items for each cryptosystem authorized for use by the field stations. It is intended that these check-off lists be used on receipt by the Commanding Officer or Officer in Charge of each COMINT activity in the conduct of an immediate inspection of his activity, and that the completed check-off list be returned to NSA and a copy furnished the Headquarters of the Service Cryptologic Agency concerned. A statement of any corrective action indicated and contemplated as a result of this inspection should accompany the completed check-off list. These inspections should be repeated at least every six months. It is intended also that these inspections by local command authorities are to be conducted in addition to, and not in lieu of, any scheduled or periodic inspections now conducted by higher authorities within the Service concerned.

2. An additional plan, utilizing the same check-off list as above, is also under consideration. The extent to which this plan would be developed would be dependent on the availability in NSA of qualified personnel who could be spared for the purpose. Under this plan, the Service Field Activities would be notified of the availability of Training Visit Teams provided by NSA. An officer fully qualified in all phases of COMSEC as applied to COMINT would, on request, conduct an informal instructional visit to the field station. In order to preserve the unofficial nature of the visit, it would be emphasized that its purpose primarily was instruction, not inspection. The check-off list would be covered in detail, the reasons behind the various rules would be discussed and explained, and specific recommendations for improvement of COMSEC at the station would be made to the Commanding Officer or Officer in Charge. The check-off list, after explanation and discussion, would be left at the station for future guidance and reference. Requests for training visits would be addressed to the Director, NSA, via the Head of the Service Cryptologic Agency concerned.

3. Specific COMSEC training criteria for the guidance of Commanding Officers and Officers in Charge of COMINT activities will be established and forwarded to the Service Cryptologic Agencies for implementation in all activities under their administrative control.

~~TOP SECRET CONTROL NUMBER~~ 54-2454-B
COPY _____ OF 48 COPIES
PAGE 11 OF 12 PAGES

~~TOP SECRET~~~~TOP SECRET~~

4. The approved minimum standards as outlined in USCIB 13.5/42 dated 8 March 1954 will be summarized in an NSA Circular for the information and guidance of COMINT field activities. In addition to the listing of the standards themselves, specific recommendations and suggestions will be included to facilitate conformance with these standards.

9
9

~~TOP SECRET CONTROL NUMBER 54-2454-B~~
COPY OF 48 COPIES
PAGE 12 OF 12 PAGES

~~TOP SECRET~~