TOP SECRET

TOP SECRET

Compromises of COMINT Due to Ineffective COMSEC

Chief of Staff
THRU: PROD (Col. Marcy)
COMSEC (Col. Herrelko)

S/ASST, Mr. Friedman

3 November 54

References:
(a) USCIB: 13.5/85, 21 October 1954
(b) LSIB/338/54, 7 October 1954 [Incl. 1 of Ref. (a)]
(c) CIB #000273 [Incl. 2 of Ref. (a)]
(d) Part III of NSA Serial 000407, 3 Sept 1954 [Incl. 1 of Ref. (c)]
(e) NSC 168, 20 October 1953
(f) DOD Directive: Communications Security (COMSEC), 24 Apr 1954
(g) NSCID No. 9 Revised, 24 October 1952

1. Reference (a) cites once again the problem of ineffective communications security. Its inclosures recommend preventive and corrective actions.

2. a. In Reference (c) the Director is quoted as saying:

"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."

b. Again the Director is quoted from Reference (c):

"... 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."

3. Consistent with the Director's indicated sentiments in the matter, Reference (d) cites additional action contemplated by NSA to improve communications security in the COMINT elements under his operational and technical control. Basically these are:

a. Issuance of detailed check lists for field use.

b. Immediate inspection of activities by the Officers in Charge or by Commanding Officers, followed by similar inspections every six months, utilizing the check lists of a.

c. Unofficial Training Visit Teams provided by NSA on a qualified-personnel-available basis for explanation and discussion of the check list and its use at the field stations. ("Requests for training visits would be addressed to the Director, NSA, via the Head of the Service Cryptologic Agency concerned.")

TOP SECRET

d. The establishment of COMSEC training criteria for the guidance of Commanding Officers and Officers in Charge of COMINT activities.

4. Referring to the corresponding sub-paragraphs of paragraph 3 above, the following comments are offered:

a. Expanded, re-worked, and more inclusive check lists than those now in existence for field use is undoubtedly a fine idea. These check lists should be reviewed on a continuing basis.

b. An OIC of COMSEC functions whose personal and continuing SOP does not include an almost daily inspection of check list procedures is not doing his job. A once-secure procedure, whether governed by a check list or not, is not necessarily self-perpetuating--even on a day-to-day basis. This recommendation contains no new force. Furthermore, if the OIC's ever got the idea that inspections on a six-month basis were sufficient, it could be damaging. If the purpose of this recommendation is only to get a six-month report on COMSEC procedures from the field, then it has merit.

c. The idea of getting qualified NSA COMSEC people out to the field to explain and discuss is good, but this recommendation is weak. It is to be an unofficial program on a personnel-available basis, utilized on the request of the field activity; thus, it would constitute a hit-or-miss proposition at best.

d. Good. The training criteria should include sufficient cryptanalytic knowledge to assure that COMSEC people are consciously aware that improperly used cryptosystems can be read.

5. NSA's mission is such, and the compromises of COMINT due to ineffective communications security are such that the serious dangers to COMINT security can be reduced or eliminated only by some NSA actions beyond those which are already being taken by the respective Services. The idea that NSA actions would be superfluous in this situation is now a proven fallacy. It appears that NSA has little choice in the matter. We should and must assume a position of consistent, continuing, and agressive leadership in the realm of COMSEC and especially as regards the security of our COMINT communications. Where the tools needed to accomplish the mission are inadequate or lacking, they must be manufactured. This is especially true as far as training and inspection functions are concerned.

6. In accordance with the foregoing, the following suggestions are made:

a. Initiate action as soon as possible to have NSC 168 amended to include COMSEC training as a directly stated NSA responsibility.

b. Carry out the actions indicated in Reference (d) pertaining to the issuance of detailed check lists and the establishment of COMSEC training criteria.

c. Send appropriate letters to the Services and the Cryptologic Agencies, encouraging them (particularly the Army and the Air Force) to make cryptosecurity the primary duty of the responsible officer rather than an additional duty as is too often the case.

~~TOP SECRET~~

d. Send appropriate letters to the Services and Cryptologic Agencies to encourage a vigorous and continual on-the-job education of the operators and the responsible officers in the existence, availability and proper use of the AFSAC3, JANAPS, OI's, etc., and the machines themselves.

e. Recognize the fact that NSA has a world-wide, dual operational mission by deliberately assigning a COMSEC expert to each NSA overseas headquarters and charging him with the appropriate responsibilities so that he may advise and instruct the responsible cryptosecurity officers on the specific nature and causes of violations and the many tools and publications available to help prevent breaks if utilized properly. This NSA man could run a quarterly critique, based on the violations listed in the quarterly COMSEC Violations Reports, and trace each break to the operator and machine concerned and give on-the-spot guidance on the proper use of the available tools to avoid the possibility of such breaks in the future. /NSA is already charged (Ref. f.) with providing technical guidance and support for cryptosecurity training conducted by the military departments./

f. Cause a tactful study to be made of the ID functions of the Cryptologic Agencies to determine:

(1) To what extent they include inspection and assistance in the implementation of the operational and technical directives of NSA, and

(2) What steps need to be taken to develop a well-directed, coordinated, and continuing ID inspection and assistance system executed by the Cryptologic Agencies and guided by the NSA Inspector General to assure the implementation of all NSA's operational and technical directives.

g. Take the steps indicated as a result of f(2).

/In regard to inspections of COMSEC activities, the pertinent DOD Directive (Reference f) now merely states: "Nothing in this directive shall be construed to give the Board or any of its representatives the right to inspect the operation of COMSEC in any military department without approval by the head thereof."/

7. Some of the actions mentioned above are undoubtedly being carried out in some degree in one place or another. However, I do not believe there is a deliberate, well conceived, over-all effort with a singleness of purpose designed specifically to promote a vigorous and continual program of real leadership and follow-up action to reduce the compromises of COMINT and other classified material attributable to ineffective communications-security measures and actions. This is a major part of NSA's mission, stated explicitly or implied in the pertinent directives; we should take vigorous action to carry out that part of our mission.

WILLIAM F. FRIEDMAN
Special Assistant

~~TOP SECRET~~