SECRET

PROBLEM

1. To examine the present method of supervising U.S. Communications Security with special reference to the reporting of violations and the evaluation of the possible damage caused. The main purpose of the examination is to determine:

a. Whether any unjustified burden is being imposed on communications.

b. Whether any information is being submitted which can properly be dispensed with.

c. The security classification required for the reports of violations and the related materials submitted by mail.

FACTS BEARING ON THE PROBLEM AND DISCUSSION

2. It is essential to maintain a continuing appraisal of the security of cryptosystems in use by the Armed Forces and to take corrective action immediately upon the occurrence of any situation which may possibly cause the compromise of cryptomaterial. To assist in such action, AFSA has established a procedure which requires the reporting of violations of physical security and crypto-security.

3. Violations of both physical security and cryptosecurity vary over a wide range insofar as the seriousness of the violations is concerned, and all the circumstances must be considered in order to determine the probability that a violation, or the sum of a series of violations, has permitted cryptomaterial or the intelligence underlying the encrypted texts

[redacted]

of messages, to become available to unauthorized persons.

4. All instances of known or suspected physical compromise or loss are reported by message, as follows:

a. Action copy to ESAFSA.

b. Information copy to the Service Headquarters.

5. In the case of violations of cryptosecurity, AFSA has promulgated a set of guiding rules which permit observers to determine whether:

a. The violation is of a type which in itself is possibly serious enough to result in a compromise, or

b. The violation is of a type considered a practice dangerous to security, and which would have to be examined in conjunction with other violations to determine the resultant effect.

In connection with a. above, a further breakdown of the relative seriousness of cryptosecurity violations and the need of urgency in their evaluation has enabled ESAFSA to divide "possible compromises" into two subordinate categories which govern whether message reports shall be forwarded to ESAFSA with a PRIORITY or DEFERRED precedence.

6. The observer of a cryptoviolation first determines whether the case at hand falls under sub-paragraph a or b above, and then takes appropriate reporting action. If the violation is determined to fall under a, the violation is reported by message, sent as follows:

a. To the Director, Armed Forces Security Agency, Washington 25, D. C. for action.

b. To the station responsible for the violation for information, if a United States Armed Forces Command.

c. To the Service headquarters for information as indicated in Appendix A.

6. (Continued)

The message is classified SECRET, unless a TOP SECRET message is involved, in which case it is classified TOP SECRET. Copies of the message(s) involved in the violation are forwarded to ERRATUM by air mail. The texts are classified SECRET, unless a TOP SECRET message is involved, in which case the text is classified TOP SECRET. If the violation is determined to fall under b. reports are forwarded by mail as specified by the individual Service procedures, with a copy being sent to ERRATUM.

7. In addition to the reporting of all violations bearing on the security of cryptomaterial, Army and Air Force holders are required to submit to their respective Service Cryptologic Agencies, but not to ERRATUM, mail reports of procedural errors, i.e. those violations of instructions which affect the efficiency of operation by causing loss of time and extra work or cause doubt to exist as to the exact plain text in the message. An average of six to eight types of procedural violations is listed for each of the cryptosystems presently in use, and occurrences of such violations are reported by mail to the Army and Air Force Cryptologic Agencies. The U. S. Navy does not require the reporting of such procedural errors.

8. With regard to the investigation of circumstances surrounding losses of cryptomaterial or possible compromises resulting from violations of physical security regulations, and reports of violations of cryptosecurity which may result in possible compromise, the procedures within the three Services are as follows:

a. Within the Army and Air Force, an investigation is required to determine the circumstances and fix the responsibility, in each instance of loss or physical compromise, and in each instance where a compromise is declared as the result of a

~~SECRET~~

6. a. (Continued)

violation of cryptosecurity.

b. Within the Navy any case of a loss, or known or suspected physical compromise is investigated in accordance with Chapter 5 of EKP 4. Further, any cryptosecurity violation of a type requiring message report to DIRAFSA also requires an investigation and report to CNO.

c. Information copies of reports of investigation are furnished DIRAFSA.

9. The basic reasons for reporting violations of cryptosecurity and physical security are as follows:

a. Such a procedure permits an evaluation to be made of the effect which each violation has upon the security of the system, and a determination to be made of the probability that such violations permit unauthorized personnel to gain intelligence from U. S. communications.

b. Such a procedure permits DIRAFSA and the Service Cryptologic Agencies to evaluate the practicability and clarity of the rules and regulations governing physical security and cryptosecurity and to make necessary revisions in these rules. It calls attention to types of errors which may not have been originally foreseen and may jeopardize security. For example, the method of transmitting message indicators in the AJAX system was found to result in an abnormally large number of messages bearing the unenciphered rotor alignment at the beginning of the message and the message indicator at the end, thus flagging

[redacted]

9. b. (Continued)

one of these as the correct rotor alignment. Now the message indicator is phoneticised at the beginning of the message and is not repeated at the end.

c. Such a procedure serves as a means of evaluating the efficiency and status of training of cryptographic personnel, and of their awareness of and compliance with the regulations governing the handling, storage and use of crypto material. It permits corrective action to be taken in instances of abnormally frequent violations.

d. It should be pointed out that the procedure itself tends to increase the awareness of cryptopersonnel to the requirements of cryptosecurity and to that extent serves a useful purpose even in those instances where the probability of compromise may be low.

10. It may be seen, from the above discussion, that an effort has been made to segregate violations into categories and to establish several methods of reporting these violations, in accordance with the probability that the violation will result in declaration of compromise. This program is maintained under a continuing review and is revised as new cryptographic procedures are introduced or as new cryptanalytic techniques are developed. Even with such an approach, it has not been possible to draw up such exact rules that the users need only report those violations which always or nearly always result in a declaration of compromise. Attached as Inclosure 1 is a summary of the compromises actually declared by AFSA since 1 Nov 1950

SECRET

10. (Continued)

on the basis of reports of violations of cryptosecurity. It will be noted that approximately 12.2% of all violations reported by message result in compromise. A review of the types of violations to be reported by message could be made, with the object of including in the listings only those violations which have the greatest probability of resulting in compromise. Such a revision would diminish the number of message reports and increase the percentage of those violations which result in a declaration of compromise. On the other hand, such an approach introduces the risk that occasionally a violation would occur, under special circumstances which permit unauthorized persons to obtain intelligence from U. S. communications, and the violation would not be reported. On the other hand, the list of violations for each cryptosystem could be expanded, so that virtually all violations would be reported by message, thus minimizing the risk of any unreported violations and assuring rapid evaluation of each case. This approach introduces the problems of interference with operations, a greatly increased volume of message reports and, in the case of the Navy, a large increase in the number of investigations.

11. In the final analysis, the determination of what violations of the rules governing the physical and cryptosecurity of cryptomaterial shall be reported, and what urgency is to be given those violations determined as requiring a report, is based on the following considerations:

~~SECRET~~

11. (Continued)

a. A detailed knowledge of the cryptanalytic weaknesses of its own systems and crediting foreign nations with an equally advanced state in the cryptanalytic art.

b. Consideration of the effect of each violation upon the security of the system. Recognition that, as the number of types of violations to be reported is expanded, the number of compromises declared thereon is not correspondingly increased, i.e. the law of diminishing returns comes into play.

c. Probability of cryptomaterial having become available to unauthorized persons.

d. Assumption that every message transmitted by electrical means, other than over approved circuits, has been made available for interception by unauthorized persons.

12. On the basis of the above considerations, the violations to be reported for each system have been specified in Chapter 3 of AFSAG 1210. It is to be emphasized that these listings do not remain static. As procedures are improved it is possible to eliminate certain weaknesses, and thus to eliminate reports of violations in connection therewith. As the cryptanalytic art advances new weaknesses are occasionally uncovered, requiring reports of violations not previously considered as serious.