

~~CONFIDENTIAL~~

NATIONAL SECURITY AGENCY
WASHINGTON 25, D. C.



25 Feb 55

~~CONFIDENTIAL~~

MEMORANDUM FOR THE MEMBERS, USCSB

SUBJECT: Policy for Safeguarding Cryptologic Information Provided to Commercial Organizations

1. In order to meet the responsibilities which have been assigned to me for conducting integrated research and development programs and for formulating integrated procurement programs to meet the cryptographic requirements of the Military Departments, it is necessary that I execute many contracts with commercial organizations. It is often essential that these contractors be provided with models of classified cryptographic equipments, documents, techniques and other classified cryptographic matter and information. It is also occasionally necessary to provide contractors engaged in work on equipments used for communications intelligence purposes with limited information related to other cryptologic matters.

2. It is imperative that commercial organizations give all cryptographic and cryptologic matter the same degree of protection and control as is given by the Departments and Agencies of the Government.

3. The Military Departments, as well as the other Governmental Departments and Agencies concerned, have recognized the need and have established precise and detailed regulations for the handling and safeguarding of cryptologic matter and information within the Executive Branch of the Government. These regulations are substantially the same in each Department and Agency. However, the control of the security of cryptologic information within commercial organizations under contract to the Government has not been as well regulated as it has been within the Governmental Agencies. Minimum standards and precise requirements have not been clearly defined and have not been stated in industrial security regulations, or other form, which are entirely applicable or suitable for use by commercial organizations or by those units of the Government which are responsible for the administration and security of Government contracts.

4. Insofar as possible, commercial firms working on National Security Agency projects have been required to adhere to certain minimum standards for the protection of cryptologic matter and information, but accomplishment of this protection has been difficult because of the lack of clearly defined standards in existing industrial security regulations. Although the problem is of primary concern to the National Security Agency, under the terms of NSC 168, cryptologic contracts may be let by

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

the Military Departments and the other Federal Agencies concerned. In order to insure that uniform security standards are applied by all Agencies to their particular contracts, it is proposed that a policy which establishes minimum standards for the safeguarding of cryptologic information provided to commercial organizations be established by the USCSB.

5. A proposed policy for safeguarding cryptologic information provided to commercial organizations is inclosed. I recommend its approval. Copies of the policy have been forwarded to the members of the USCIB for their information.

6. Following USCSB approval of the inclosed policy statement, based on the general minimum standards set forth therein, I shall prepare an "Industrial Security Manual for Safeguarding Cryptologic Information" for use within the Department of Defense. In order that other Departments and Agencies also may make use of this manual, it will be designed to have fairly universal application to the security of cryptologic information and materials in the custody of commercial organizations, and copies will be made available to the Executive Secretary, USCIB/USCSB, for distribution to the members of both Boards.



RALPH J. CANINE
Lieutenant General, US Army
Director

Incl:
a/s

POLICY FOR SAFEGUARDING CRYPTOLOGIC INFORMATION
PROVIDED TO COMMERCIAL ORGANIZATIONS

1. Cryptologic information which is made available to commercial organizations by the various departments and agencies of the Government will be safeguarded in accordance with the minimum standards set forth herein.

DEFINITIONS

2. The following definitions are established for the purpose of this policy:

a. Cryptologic Information. - Any classified equipment, material, or information which is designated by the cognizant department or agency of the Government as being cryptographic or cryptologic because of its relationship to codes, ciphers, or cryptosystems of the United States or foreign nations, or because of its relationship to the communications intelligence activities of the United States.

b. Commercial Organization. - Any industrial plant, educational institution, or commercial company or organization which is not under the direct control of the Government but is engaged in performing services of a cryptologic nature for the Government, usually under contract to the Government or under subcontract to a prime contractor of the Government.

c. Cognizant Agency. - A department or agency of the Government which has a requirement for providing cryptologic information (either directly or indirectly through a Government procurement or contractual facility) to a commercial organization in order that the commercial organization can satisfactorily perform services for that department or agency.

ACCESS

3. Prior to providing any cryptologic information to a commercial organization, the cognizant agency will ascertain that the officers, directors, and key employees of the commercial organization are appropriately cleared in accordance with the standards of the cognizant agency for access to the particular cryptologic information concerned.

4. Within a commercial organization, access to cryptologic information shall be limited to those employees who need to know and who have been cleared in accordance with the standards of the cognizant agency.

5. The cognizant agency will insure that authorities of the commercial organization will take steps to make certain that all employees concerned are fully indoctrinated in all security requirements of this policy and are continuously aware of the necessity for safeguarding cryptologic information at all times and of the applicable Federal Statutes and Executive Orders, particularly the Espionage Laws, Title 18, U.S.C. Sections 793, 794 and 798.

6. Visitors to a commercial organization shall be permitted to have access to cryptologic information in the custody of that organization only when specifically authorized by the cognizant agency or other appropriate Government authority.

PHYSICAL SECURITY

7. Prior to providing any cryptologic information to a commercial organization the cognizant agency will ascertain that the organization is capable of and fully prepared to physically safeguard the information in accordance with the minimum standards set forth herein and such further standards as may be required by the cognizant agency. The cognizant agency will also ascertain that adequate means exist for over-all supervision and constant surveillance of those security practices and procedures established.

8. All cryptologic matter provided to or handled by a commercial organization will, if practicable, be marked with the appropriate classification and, if deemed necessary by the cognizant agency to insure adequate control and handling, will be further marked as being cryptologic. If this is not practical, the commercial organization will be advised in writing of those specific items which are cryptologic and the classification of each.

9. Commercial organizations will receipt for and maintain a record of all cryptologic matter received. Within the commercial organization, the dissemination of cryptologic information will be carefully controlled and will be limited to those employees who are authorized to receive it and who have a need for the information. Transmission means employed within a commercial organization will be such as to insure that only authorized employees will have access to cryptologic information.

10. Cryptologic information which is classified TOP SECRET or which is specified by the cognizant agency as requiring registered accountability will be strictly accounted for at all times within the commercial organization in accordance with the standards specified by the cognizant agency. As a minimum, transmittal and custody of all such matter will be covered by a hand receipt system and a record will be maintained of the exact location of each item.

11. Copies or reproductions of cryptologic matter and extracts from cryptologic documents will be made by commercial organizations only as authorized by the cognizant agency. The same accountability as accorded the original documents or materials will be provided for all such copies, reproductions or extracts.

12. Cryptologic matter in the custody of a commercial organization will be transmitted outside that organization only when authorized by the cognizant agency and in accordance with the following minimum standards:

a. Printed matter and documents will be double wrapped and sealed. The outer wrapper will contain no indication of the fact that the package contains cryptologic or classified matter. Equipments and bulky items will be similarly securely packaged or crated as specified by the cognizant agency.

b. The means of transmission used will be one of the following: messenger approved by the cognizant agency; United States registered mail; or protected commercial express. The exact means will be specified in accordance with the standards of the cognizant agency for the particular cryptologic matter concerned. Under no circumstances will cryptologic information be transmitted by non-registered mail. TOP SECRET cryptologic matter will be transmitted only by direct contact whenever possible.

13. Within a commercial organization, cryptologic information will, when in use, be maintained in a physically segregated area which is so designed and constructed as to prevent observation or entrance by other than authorized personnel. All entrances to the area will be kept under continuous guard.

14. During non-working hours and when cryptologic information is not in use, it will be stored in three-position dial-type combination lock safes or vaults, the size, weight and construction of which is such as to minimize the possibility of physical removal. Only a minimum number of authorized personnel will have keys or combinations to storage facilities. Combinations to storage facilities will always be changed upon transfer of personnel having knowledge of same. When because of its size or nature it is not possible to store cryptologic matter in a safe or vault, the cryptologic matter will be kept under armed guard. Full-time guards or roving patrols will be employed as deemed necessary by the cognizant agency in order to adequately protect the cryptologic matter involved. Guards will be United States citizens of undoubted loyalty.

15. Commercial organizations will not destroy any cryptologic matter in their custody unless such destruction is authorized by the cognizant agency. When authorized, destruction will be carried out in accordance with the following minimum standards:

a. Documents and printed matter will be destroyed by burning or by pulping methods if approved by the cognizant agency. Cryptologic equipments shall be melted or otherwise destroyed beyond recognition as specified by the cognizant agency.

b. Destruction will be performed by an appropriately cleared and authorized employee of the commercial organization and will be witnessed by at least one other such person. Destruction of all TOP SECRET and registered cryptologic matter, as well as such other cryptologic matter as may be specified by the cognizant agency, will be recorded and certified.

c. Cryptologic waste materials will be carefully and securely disposed of as specified by the cognizant agency. The cognizant agency will insure that commercial organizations are provided complete guidance concerning the secure disposition of all cryptologic waste materials.

16. The cognizant agency will ascertain that commercial organizations are prepared, in the event of fire or other emergency, to provide adequate protection to cryptologic information in their custody in order to insure that such information will not be accessible to unauthorized persons.

APPLICABILITY

17. The minimum standards set forth herein will apply to all sub-contractors as well as to prime contractors of the Government who have access to cryptologic information. The cognizant agency and the prime contractor are responsible for insuring that cryptologic information provided to sub-contractors is protected in accordance with the foregoing minimum standards, and that sub-contractors establish such procedures as may be required to accomplish this.

18. It is not intended that the minimum standards set forth herein will apply without exception to those parts and components of cryptologic equipments or extracts from cryptologic documents which, when considered individually, could provide no cryptologic information. It is the responsibility of the cognizant agency to furnish guidance to commercial organizations as required concerning the safeguarding standards to be applied to individual parts or components of cryptologic items.