

**SECRET***Dir*

**NATIONAL SECURITY AGENCY  
FORT GEORGE G. MEADE, MARYLAND**

Serial: N 0971  
20 March 1961

**SECRET**

MEMORANDUM FOR THE MEMBERS OF USIB

SUBJECT: Industrial Security Program (U)

1. NSCID No. 6 prescribes for COMINT and ELINT and their associated activities "an organization and management which will . . . insure the necessary degree of protection"; but it omits any wording easily construed as providing the necessary authority to prescribe security standards and safeguards for COMINT contracts awarded to industry on behalf of NSA. Accordingly, the NSA industrial security program is based largely on DOD Directive No. S-5100.20, "The National Security Agency," dated 19 March 1959. In Section IV, Paragraph 5, that directive specifies that, "within its assigned fields of responsibilities," the Agency shall develop requisite security rules, regulations, and standards governing operating practices in accordance with the policies of the U. S. Intelligence Board. In Section VI, Paragraph A. 6., of the same directive, the Director, NSA, is specifically delegated authority to prescribe or review and approve security rules, regulations, and instructions "as appropriate." A careful examination of the authorities cited above, and of some other directives stemming from the Secretary of Defense, leads to the conclusion that a clarification by USIB of its policy concerning the release of COMINT to contractors is needed. While the existing directives do not expressly prohibit such release (but rather, by implication, encourage it), they do not make explicit provision for the handling of COMINT information in non-governmental establishments. Therefore, while it is believed that the present program is consistent with the intent of Board policy, it is felt that there is a need for the Board to confirm this interpretation.

2. Because of the necessity to utilize industrial potential in the pursuit of our COMINT effort, our industrial security program has been gradually developed — in coordination with the Office of the Assistant Secretary of Defense (Manpower, Personnel and Reserve) and with other agencies as appropriate. The Department of Defense has established a "cognizant security office" system to insure that all classified information in the custody of a contractor is properly safeguarded. Because of its COMINT responsibilities,

HANDLE VIA COMINT CHANNELS ONLY**SECRET**

~~SECRET~~~~SECRET~~

Serial: N 0971

NSA has undertaken, for each of its COMINT contracts, to assume the security responsibilities of the Department of Defense "cognizant security office" for that portion of the contractor's facility being utilized on the COMINT contract. It is felt that such an approach, within the framework of the Department of Defense industrial security program, has certain advantages. Some of these advantages are:

a. The contractor as such can be held responsible for a violation of established security procedures.

b. Action can be taken insofar as the contractor's facility clearance is concerned, if the contractor violates the prescribed security regulations.

c. The contractor is in a position to have COMINT material in his possession, if this is necessary to meet the operational requirements of the contract.

3. At the present time, this Agency has certain contracts for which some degree of COMINT access has been considered requisite to fulfilling the contractual requirements. The contract management activities of this Agency authorize such access at a contractor's facility only when it is considered absolutely necessary to meet an operational requirement. For some other contracts, contractor personnel are given COMINT-related (but non-codeword) background information. It has been our experience that this is a realistic approach to the problem; and industry has willingly accepted the security responsibilities associated with this type of procurement.

4. It should be noted that in many cases, particularly where devices are being built for specific problems, COMINT information can be evidenced in some degree during design, development and construction, as well as testing prior to acceptance by the government. In some cases, moreover, even though COMINT information is not directly involved during these phases, the devices themselves have obvious COMINT overtones. In addition, it is felt that, in those contracts for which COMINT access is deemed essential, so-called sanitization of the COMINT material is a futile gesture. It has been our experience, in those cases where sanitization has been attempted, that the contractor employees directly involved are technically capable of inferring the COMINT underlying the sanitized version. The majority of the contractors, moreover, are generating

~~HANDLE VIA COMINT CHANNELS ONLY~~~~SECRET~~

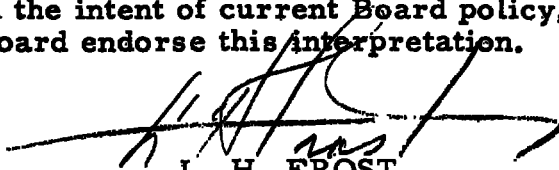
**SECRET**SECRET

Serial: N 0971

COMINT as a condition of the contract; and it would be difficult, if not impossible, to conceal this fact from them. It should also be noted, however, that all of the COMINT material, either furnished to or generated by the contractor, is accounted for by this Agency through an inventory and control system which includes verification by inspection.

5. The nearest approach to a USIB policy statement in this area appears to be Paragraph 44 of DCID No. 6/3, which places "upon the Board member, or his properly designated representative, of that department or agency directing the project" the responsibility for determining the need-to-know of civilians under contract and employees and representatives of commercial firms and civilian research institutions which are to engage in technical or intelligence research or in manufacture of equipment for COMINT activities, as well as personnel from non-member government departments or agencies involved in such pursuits. In lieu of the promulgation of a more comprehensive and explicit USIB policy statement, this paragraph, plus Paragraph 56 concerning indoctrination and Paragraph 77 concerning physical security through control of access and dissemination, provide the only USIB-derived basis for the corresponding aspects of the NSA industrial security program.

6. In brief, the NSA industrial security program is believed to be consistent with the intent of current Board policy, and it is requested that the Board endorse this interpretation.




L. H. FROST  
Vice Admiral, USN  
Director

~~HANDLE VIA COMINT CHANNELS ONLY~~

**SECRET**

~~SECRET~~~~SECRET~~

Serial: N 0971

cc: DIR   
AG  
Reading File  
Legal Advisor  
PROD-03  
R/D  
SEC  
OPS (3)

M/R: Largely self-explanatory. The NSA industrial security program has been developed within the framework of the DOD (OASD, MP&R) industrial security program, and is believed to be consistent with the intent of current USIB policies. However, since DOD Directive No. S-5100.20 requires that "within its assigned fields of responsibilities," NSA shall develop requisite security rules, etc., in accordance with the policies of USIB, instant correspondence required to get USIB confirmation with respect to the NSA industrial security program (an area in which no comprehensive and explicit statement of USIB policy exists). This memorandum for the members of USIB prepared at direction of Director, NSA. Coordinated with and concurred in by Legal Advisor (Mr. Banner), SEC (Mr. Lewe), and PROD-03 (Mrs. Brewer). Discussed with R/D (Mrs. Haig), who reported that Director, R/D, in general concurs in the wording of this memorandum, but that he believes the Director, NSA, has adequate authority under existing directives.



ROBERT H. DARBY/OPS/3671-S/8 Mar 61/mlo

~~SECRET~~