~~TOP SECRET~~

National Security Agency

Fort George G. Meade, Maryland

REPORT OF REVIEW OF NATIONAL SECURITY AGENCY

SECURITY PROCEDURES AND STATUS

BACKGROUND INFORMATION

NSA TS CONTROL NO. 62-00175
COPY NUMBER 2
THIS DOCUMENT CONTAINS ~~150~~ 148 PAGES
IT IS SUBJECT TO SEMI-ANNUAL INVENTORY.

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~

~~TOP SECRET~~

REPORT OF REVIEW OF NATIONAL SECURITY AGENCY

SECURITY PROCEDURES AND STATUS

BACKGROUND INFORMATION

NSA TS CONTROL NO. 62-00175
COPY NUMBER 2
THIS DOCUMENT CONTAINS ~~150~~ 148 PAGES

IT IS SUBJECT TO SEMI-ANNUAL INVENTORY.

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~

1. Missions and Role of the National Security Agency

a. The resources of the National Security Agency (NSA) are organized to lead and participate in the accomplishment of two missions primary to the national interests.

(1) The Communications Intelligence (COMINT) and Electronics Intelligence (ELINT) missions of the NSA are, (a) to provide an effective, unified organization and control of the COMINT and ELINT intercept and processing activities of the United States, (b) to provide for integrated operational policies and procedures pertaining thereto, and (c) to produce COMINT and ELINT information in accordance with objectives, requirements and priorities established by the United States Intelligence Board (USIB).

(2) The Communications Security (COMSEC) mission of the NSA is to prescribe, under the policy guidance of the United States Communications Security Board (USCSB), the principles, doctrine, and practices, and to provide the cryptomaterial necessary, to ensure the maximum practicable degree of security for:

(a) U. S. Federal telecommunications, including those of the Military Establishment and

(b) Telecommunications of certain friendly foreign nations and international organizations, as authorized by higher authority.

In order to accomplish the first of these two missions, the Director, NSA, is given operational and technical control over the COMINT and ELINT processing activities of the United States, except for those COMINT and ELINT activities placed under control of specified military authorities by the Secretary of Defense, or conducted under provisions of NSCID 5.

b. Within these assigned fields of responsibility and subject to the supervision of the Director of Defense Research and Engineering, the National Security Agency is charged to (a) establish and conduct a research and engineering program to meet the needs of the NSA and the departments and agencies engaged in activities in these fields; (b) review and co-ordinate the research and engineering programs conducted by such departments and agencies; and (c) recommend controls and procedures to the Director of Defense Research and Engineering governing the conduct of research, development, test and evaluation.

c. In connection with the communications system established for timely transmission of critical intelligence (CRITICOMM), the Director, NSA, is responsible for controlling the traffic and cryptographic operations of the system, and for establishing operational procedures for handling COMINT and critical intelligence traffic within the system.

2. Authority and Responsibilities

a. General

(1) While the existence of the NSA has been recognized in Public Law 86-36, the Agency has no independent statutory origin. It was created as a separate Agency within the Department of Defense by an Intelligence Directive of the National Security Council (NSC) on 5 Dec 1952 to handle certain prescribed functions within the national intelligence effort. The authority for administration of the Agency, including civilian personnel, is delegated to the Director, NSA, by the Secretary of Defense.

(2) The authorities under which the NSA conducts its security program stem from applicable Federal Statutes such as Title 18, U. S. Code, Section 798 and Public Law 86-36, Executive Orders 10450, 10501 and other Presidential directives. Directives of the Director of Central Intelligence (DCI) issued under the authority vested in him by the National Security Act of 1947 (as amended, 1949), Department of Defense directives and internal regulations constitute the remaining authority.

(3) Since there is no statute assigning authority and responsibility directly to the NSA, the Agency powers are derived solely by administrative delegation from within the Executive Branch of the Government. The Agency's authority in the security field is limited generally by (a) the scope of the NSA's mission as defined by higher authority, (b) laws and regulations of general applicability, and (c) security authority and responsibility assigned to other agencies. The two basic documents chartering the NSA are National Security Council Intelligence Directive Number 9 (NSCID 9), subsequently revised and reissued as NSCID 6 on 15 Sep 1958, in the field of COMINT and ELINT, and National Security Council Directive on Communications Security Number 168 (NSC 168), subsequently reissued as NSC 5711 on 25 April 1957, in the field of COMSEC.

(4) It should be noted at the outset that other authorities in addition to the Director, NSA, have been delegated responsibilities for various phases of the broad field of security. These responsibilities to some extent overlap those of the Director, NSA. Any statutory enactment in conflict with NSA's administratively derived authorities would, of course, be paramount. Nothing in the directives establishing the NSA could override, for example, the statutory responsibility of the FBI for the investigation of espionage nor the responsibility of the Director of Central Intelligence for protecting intelligence sources and methods from unauthorized disclosures. The Director, NSA, therefore, must avoid issuing directives which conflict with the regulations of other authorities in the field of security.

(5) The authorities delegated to the Director, NSA, by the Secretary of Defense, as executive agent of the government for the conduct of COMINT and ELINT activities, appear somewhat more limited than those outlined in NSCID 6. Department of Defense Directive S-5100.20, The National Security Agency, dated 19 Mar 1959, (Tab A) provides (Para IV, 5) that as a function within its assigned fields of responsibility the NSA shall develop requisite security rules, regulations and standards governing operating practices in accordance with the policy of the United States Intelligence Board and the United States Communications Security Board. This directive also states (Para VI) that to carry out assigned responsibilities of the Agency, the Director, NSA, is specifically delegated authority to prescribe, or review and approve security rules, regulations and instructions, as appropriate. Several authorities are delegated to the Director, NSA, relative to security matters by the Secretary of Defense in DOD Directive 5100.23, Administrative Arrangements for the National Security Agency, dated 25 Aug 1959, (Tab B). These include:

(a) Authority to (1) authorize, in case of an emergency, the appointment of a person to a sensitive position for a limited period for whom a full field investigation or other appropriate investigation, including the National Agency Check (NAC) has not been completed, and (2) authorize the suspension, but not to terminate the services of an employee in the interest of national security in positions within the NSA in accordance with the provisions of the Act of August 26, 1950, as amended (5 USC 22-1), Executive Order 10450, dated 27 Apr 1953, as amended, and DOD Directive 5210.7, dated 12 Aug 1953, as revised, (Tab C).

(b) Authority to clear personnel of the NSA and such other individuals as may be appropriate for access to classified defense material and information in accordance with the provisions of DOD Directive 5210.8, dated 29 Jun 1955 (as revised), "Policy on Investigation and Clearance of Department of Defense Personnel for Access to Classified Defense Information", (Tab D) and Executive Order 10450, dated 27 Apr 1953, as amended.

(c) Authority to classify, declassify and down-grade or up-grade the classification of defense information or material which the NSA has responsibility pursuant to Executive Order 10501, dated 5 Nov 1953, as amended, and DOD Directive 5200.1, dated 8 Jul 1957, (Tab E), and to designate in writing, as may be necessary, officers and employees within the NSA to perform these functions.

(d) Authority to promulgate the necessary security regulations for the protection of property and places under the jurisdiction of the Director, NSA, pursuant to paragraphs III. A. and V. B. of DOD Directive 5200.8, dated 20 Aug 1954, (Tab F).

b. COMINT/ELINT Authorities and Responsibilities

(1) The Director, NSA, is vested by NSCID 6 with substantial, but not exclusive, responsibility and authority for the security of the COMINT activities of the United States. Paragraph 7 b (4) of NSCID 6 states that the Director's specific responsibilities include: "within the NSA's field of authorized operations prescribing requisite security regulations covering operating practices, including the transmission, handling and distribution of COMINT material within and among the COMINT elements under his operational or technical control; and exercising the necessary monitoring and supervisory control, including inspections, if necessary, to insure compliance with the regulations". This includes all COMINT collection and production resources of the United States.

(2) It is difficult to delineate the respective powers of USIB and the Director, NSA, for the protection of United States COMINT since there is a twilight zone where both authorities function. In paragraph 4, NSCID 6 states that USIB, in addition to its responsibilities under NSCID 1, shall study, in connection with its responsibilities for communications intelligence security, the standards and practices of the departments and agencies in utilizing and protecting COMINT; and establishing procedures whereby the departments and agencies not members of the USIB are enabled to receive and utilize COMINT. Also, USIB shall determine the degree and type of security protection to be given COMINT activities through the protection of information about them or derived from them, taking into full account that different levels of sensitivity obtain and applying balanced judgement between the need for exploitation of the COMINT produced and the need to protect the specific producing activity or activities. Further, USIB shall determine the degree and type of security protection to be given ELINT activities through the protection of information about them or derived from them. While it appears that the powers of USIB are policy making, and those of the Director, NSA, are executive in nature, both authorities have powers in their respective spheres to prescribe security regulations.

PL 86-36/50 USC 3605

(3) It is important to note that the Director, NSA, does not have authority for the administration of military or civilian personnel in the Service Cryptologic Agencies of the Department of Defense, nor does he have authority over personnel security programs governing approximately 85% of the U. S. personnel having clearance for access to COMINT.

For a breakdown of the distribution of indoctrinated personnel throughout the Federal Government reference may be made to TOP SECRET USIB Memorandum for the Secretary
Subject: U. S. COMINT Indoctrination Totals, dated 24 Aug 1961 (SIB 00017).

PL 86-36/50 USC 3605
EO 3.3(h)(2)

(4) The general policy governing activities of all persons dealing with COMINT and ELINT in foreign countries is determined by USIB. It is the responsibility of each member to ensure that COMINT and ELINT liaison conducted by his department or agency in foreign countries is consistent with Board policy and in accordance with procedures established therefor.

(a) The Director of Central Intelligence is responsible as executive agent of the Government for COMINT and ELINT arrangements with intelligence services of all foreign governments, except that such arrangements with the United Kingdom (UK), Canada and Australia are the responsibility of the Director, NSA, in general consultation with the DCI.

(b) The product or technical studies of any U. S. COMINT-producing organization may be exchanged with UK, Canadian or Australian COMINT-producing organizations only by or in accordance with procedures established by the Director, NSA.

(c) Procedures for SIGINT liaison with UK, Canada or Australia are outlined in DCID 6/3. A Senior U. S. Liaison Officer for COMINT (SUSLO) is appointed, as required, by the Director, NSA, with the approval of the USIB, to each of these countries. The SUSLO is responsible to the Director, NSA, and is accredited to the COMINT and ELINT Policy Authority or the country concerned. He is the appropriate authority for certifying the clearance status of U. S. nationals stationed in or visiting the country to which he is accredited. Arrangements for COMINT and ELINT liaison between USIB member organizations and UK, Canadian or Australian authorities must be made through the SUSLO.

EO 3.3(h)(2)
PL 86-36/50 USC 3605

(5) It is of the utmost importance that strictest secrecy be maintained regarding all

(a) On the basis of technical and operational considerations, the Director, NSA, is responsible for determining the individual items or types of

He provides guidance as required on the importance of the COMINT considerations involved.

(b) A special operation having as a planned objective the acquisition of [redacted] is undertaken only when authorized by the Director, NSA, or his field representative.

(c) The Director, NSA, is responsible for maintaining close cooperation [redacted] as appropriate, in planning of such special operations, and for coordination with NATO, when appropriate, through established channels in the major NATO headquarters concerned.

EO 3.3(h)(2)
PL 86-36/50 USC 3605

(d) In cases where the acquisition of [redacted] by the U. S. Armed Services, the Director, NSA, will issue appropriate guidance for the recognition, protection and disposition of [redacted]

(e) Insofar as practicable, COMINT channels are used for technical exchanges of information on the planning of [redacted]

(f) Exploitation of prisoners of war or defectors having cryptologic knowledge is to be accomplished by technically qualified COMINT-indoctrinated personnel whenever possible.

c. COMSEC Authority and Responsibility

(1) Upon turning to the COMSEC field, it is noted that COMSEC is, itself, basically a security function in contrast to the Signals Intelligence (SIGINT) mission where the protective aspects, however vital, are subordinate to the primary objective of the collection and production of intelligence information. The responsibility and powers of the Director, NSA, for the COMSEC activities of the United States are derived from the National Security Council Directive on Communications Security (NSC 5711), dated 25 April 1957 and DOD Directive C-5200.5, Communications Security (COMSEC), dated 27 Oct 1958 which implements NSC 5711 within the Department of Defense.

(2) The United States Communications Security Board (USCSB) was established by the National Security Council pursuant to a Presidential Directive of 24 Oct 1952 to integrate policies and procedures affecting the security of federal communications and

to coordinate COMSEC activities of the departments and agencies of the government to achieve the maximum practicable degree of security. NSC Directive 5711 outlines the COMSEC responsibilities of various elements of the government.

(3) NSC 5711 established the Department of Defense as Executive Agent of the Government for all COMSEC matters. The Director, NSA, has been designated to act for the Executive Agent in all COMSEC matters set forth in paragraphs 2d (1) through paragraph 2d (12) of the NSC Directive.

(4) Paragraph IV of Department of Defense Directive C-5200.5 establishes the responsibility of the Director, NSA. In fulfilling his COMSEC responsibilities, the Director, NSA, may take such actions as may be required to ensure continuing security of military communications subject to the provisions of this Directive. Among others, the Director, NSA, has the authority and responsibility specifically:

(a) To prescribe, or review and approve Cryptosecurity rules, regulations, and instructions for the secure operation and use of COMSEC equipments and systems.

(b) To formulate basic doctrine for transmission security and to recommend minimum standards for the application of this doctrine; and to review and evaluate procedures developed by the Military Departments to determine whether such procedures will provide and maintain transmission security.

(c) To prescribe minimum standards for the physical security of crypto material, in collaboration with the Military Departments, as appropriate.

(5) Certain special provisions are delineated in Paragraph V of the Department of Defense Directive on Communications Security. The Director, NSA, shall discharge responsibilities with respect to the Military Departments in accordance with his own judgement, subject to the provisions of the Directive. The cryptosecurity rules, regulations, and instructions promulgated by the Director, NSA, in accordance with his assigned responsibilities in the COMSEC field are excluded from the Department of Defense Directives System, are authoritative as published, and are binding upon the Military Departments.

3. Basis for a Special Security Program for COMINT

a. The principal reason for a special security program for Communications Intelligence is to preserve the capability to produce Communications Intelligence information, or, in other words, to conserve and safeguard the activities which produce Communications Intelligence. It is a fundamental premise of this system that exposure of the results, the nature, or the scope of the Communications Intelligence activities outside of the system, increases the risk of unauthorized disclosure, compromise and consequent damage to the activities themselves. While the security measures have been developed primarily to protect the sources of Communications Intelligence, the requirement for special protection actually derives from (1) the value of information obtained, and (2) the peculiar susceptibility of the Communications Intelligence source to loss. Information content, by itself, can warrant protection if, because of our knowing it secretly, we have an action advantage. Content, by itself, can also warrant protection if the knowledge of our possession of it would stimulate a potential enemy to deny us information of a similar nature in the future.

b. Since COMINT is derived from intercepted foreign communications, it is peculiarly susceptible to compromise inasmuch as any revelation of successful exploitation of their communications by intelligence activities of the United States tends to stimulate foreign governments to tighten the protective measures they provide for their communications. For this reason, the United States and the United Kingdom, with which the United States has collaborated closely in the protection of COMINT since World War II, have developed stringent security measures for the safeguarding of COMINT and information about COMINT.

c. Security for Communications Intelligence information is obtained through special handling of the material itself, through employment of special clearance and indoctrination procedures for the persons who will have access to it, through a strict application of the principle that an individual will receive only that information for which he has a valid need-to-know, and a continuing personnel security supervision program. The emphasis must be placed upon each individual who is to receive Communications Intelligence information or information about Communications Intelligence activities and the control of that knowledge which he acquires. All security devices and procedures in the system designed to protect Communications Intelligence information endeavor to provide assurance that this sensitive information is properly recognized and securely retained within the system.

d. While extreme care is taken to safeguard information concerning United States COMINT activities because a target country can increase its cryptographic or transmission security measures to the point where its communications are not longer susceptible to COMINT exploitation, the same degree of protection need not be given the U. S. ELINT effort. The reason for this is that the source, direction and nature of electronic emissions from ELINT target facilities, such as radars, cannot be concealed or disguised to prevent their interception. Although the special COMINT security standards and procedures generally are not applied to ELINT and ELINT activities, they are protected and controlled by the security regulations of the Government that cover handling of classified defense information in general.

PL 86-36/50 USC
EO 3.3(h)(2)

4. COMINT Security Regulations

a. The basic principles governing the safeguarding of COMINT and COMINT sources are outlined in a directive published by the Director of Central Intelligence, with the concurrence of the USIB (DCID 6/3, Communications Intelligence Regulations, 29 Dec 1959).

[redacted]

b. The basic principle governing dissemination and use of COMINT is the need-to-know. A system of categorization, directly related to and responsive to sensitivity, is utilized as a basis upon which COMINT may be disseminated by a USIB member to persons indoctrinated for access to particular categories or sub-categories of COMINT. The Director, NSA, may approve the issuance of technical instructions to non-indoctrinated personnel under certain conditions. Provision is made for special or emergency use of COMINT in the event of hostilities or other specified conditions. If prior co-ordination with USIB [redacted] as appropriate, is not possible, the organization responsible for such usage will notify the Director, NSA, of actions taken; the Director, NSA, in turn, will be responsible for immediate notification of the Board and will keep the [redacted]

Gov

c. The nature of COMINT and COMINT activities and their susceptibility to compromise require that certain information regarding these activities and their product be restricted to persons who have been cleared and indoctrinated for access to COMINT. The classification of each document containing information related to COMINT or COMINT activities must be determined individually, after due consideration of the damage which unauthorized disclosure of its contents could cause to national security, national interests, and

the capability of the U.S. to continue to produce Communications Intelligence. Classification guidance is included in DCID 6/3. Materials containing information in certain categories may be released by the USIB member concerned with the prior approval of the originator -- which is usually the NSA. The NSA will inform

[redacted]

d. As outlined in DCID 6/3, elements of the procedure for granting access to COMINT are consecutively:

PL 86-36/50 USC 3605
EO 3.3(h)(2)

(1) Determination of the need-to-know.

(2) Investigation and evaluation in terms of USIB clearance standards.

(3) Approval for indoctrination.

(4) Indoctrination.

Responsibility for granting access to COMINT in the performance of duties under the direct cognizance of a USIB member rests with that Board member. The need-to-know of all other individuals is determined by USIB.

e. There are restrictions against assigning a COMINT indoctrinated individual to hazardous duties, based upon evaluation of his knowledge of COMINT or COMINT techniques and the advantage which would accrue to any foreign country through ability to institute COMINT countermeasures, resulting from disclosure of that knowledge through capture or interrogation of the individual in question. Exceptions may be granted by the Board, or by Board members, under certain conditions, which must be reported to the Board.

f. The protection of COMINT and, especially of COMINT technical information, requires extraordinary precautions. Board members are required to control access to COMINT areas and the dissemination of COMINT in accordance with policies, standards and procedures established by the Board.

g. Transmission of COMINT by electrical means must be accomplished in accordance with minimum standards established by the USCSB Board. The Director, NSA, may periodically perform technical analysis of electrical COMINT communications as may be necessary to ensure the continuing adequacy of these prescribed minimum standards. A member department or agency is required to provide data for such analysis, but is not required to disclose the contents of communications

if such disclosure would jeopardize other operations under his cognizance. The Director, NSA, cannot inspect any department or agency without the approval of its Chief.

h. Effective intercept of certain communications and effective COMINT support of field commanders may require COMINT collecting, processing or dissemination in exposed areas, with hazards involving possible loss of COMINT. The determination to conduct a COMINT activity in a given exposed area is the responsibility of the Director, NSA, based on certain criteria established in DCID 6/3 and consideration of the advantages to be gained by the national COMINT effort against disadvantages of the COMINT losses which might result if the area concerned were suddenly overrun. A decision to disseminate COMINT to consumers in exposed areas may be made, after due consideration of the advantages and risks involved, by individual Board members.

i. Any breach of COMINT security regulations or other circumstance which may be presumed to have revealed COMINT information or successes to unauthorized persons is reported to the Director, NSA, in accordance with procedures outlined in DCID 6/3. The Director, NSA, is responsible for informing the Board if, in his opinion, the compromise is significant, evaluating its effect upon the COMINT effort and informing the Board of any further actions he considers appropriate. The Director, NSA, is also responsible for notifying [redacted] if necessary and appropriate. Should intelligence services of other foreign governments be involved, the Director of Central Intelligence is responsible for such notification as may be appropriate.

PL 86-36/50 USC 3605
EO 3.3(h)(2)

5. The NSA Workforce

a. To fulfill its two primary missions as well as responsibilities in the areas of Critical Communications (CRITICOMM) and cryptologic research and development activities, the NSA workforce must be manned with many diverse specialties and skills. Requirements range from scientists, mathematicians, and engineers for SIGINT, COMSEC and R/D activities to blue-collar wage board employees in the cryptographic production elements. All of these employees must be cleared for access to TOP SECRET and cryptographic information. They must also meet the eligibility standards of the United States Intelligence Board for COMINT indoctrination.

PL 86-36/50 USC 3605

[redacted]

from the three Services. A distribution of this workforce by occupational category is presented in Tab G. The assignment of this workforce to the principal organizations of the Agency together with respective manning authorizations is displayed in Tab H.

c. The normal attrition rate, which is relatively low, averages

[redacted]

employees. Further increases in strength are in prospect for next year.

d. Personnel in the National Security Agency are employed in the Excepted Service and under the provisions of Public Law 86-36. Thus, they do not have the status of career employees in the competitive service. Although the Agency is no longer subject to the supervison of the Civil Service Commission under the Classification Act of 1949, its personnel policies are, in general, comparable to those of other Government Agencies with respect to job classification, promotion, rates of pay, conditions of work, and similar matters. All military and civilian positions of the NSA are designated as "sensitive positions" within the meaning of Executive Order 10450 as prescribed in Paragraph III E of the Department of Defense Directive No. 5100.23, Administrative Arrangements for the NSA, dated 25 August 1959. Employment and retention in the Agency, therefore, are governed by Executive Order 10450 and DOD Directive 5210.7, Department of Defense Civilian Applicant and Employee Security Program. Security clearances for NSA personnel, as for other employees of the Department of Defense, are accomplished under DOD Directive 5210.8, which states the Policy on Investigation and Clearance of Department of Defense Personnel for Access to Classified

Department of Defense Information. Because of the sensitive nature of the NSA activities, and because employment in the Agency requires access to very highly classified information, the NSA personnel must meet the strictest of all security standards in the Department, including those required for clearance for access to Cryptographic information. In particular, each employee, without exception, must be found to be of excellent character and discretion and of unquestioned loyalty to the United States. In setting standards for access to Communications Intelligence and information about Communications Intelligence activities, the United States Intelligence Board incorporates the standards set forth in Executive Order 10450 and the Department of Defense Directives, adding the requirement that individuals handling such material be native-born citizens of the United States. These are found in DCID 6/3.

(1) The Director, NSA, like other members of USIB, has authority to waive certain of these standards in cases where he has determined the risk involved is negligible and there is a compelling need for the services of the individual. However, in practice, waivers have been limited under these standards usually to cases where an employee's spouse, intended spouse, or relative was not yet a U. S. citizen.

(2) Should information be obtained at any time indicating that retention of an NSA employee was no longer clearly consistent with the interests of the national security, the Director, NSA, is empowered to suspend the employment of the individual, without pay, under the provisions of Public Law 733, Eighty-first Congress. After the individual has had the opportunity provided by law to answer the charges against him and received benefit of procedural rights afforded under that law, the Secretary of Defense may terminate his service. Separation from the NSA may be accomplished also for non-security reasons, under Rule 6 of the Civil Service Commission Rules and Regulations, although in such cases the Veterans Preference Act may also apply.

e. The successful accomplishment of the mission of NSA, so vital to the national defense, is in a large measure dependent upon the maintenance of a workforce of sufficient size and appropriate composition. This is a difficult task at best. It is rendered more difficult by the need to maintain a maximum degree of security. The security screening process is prolonged beyond minimum essential time by Agency dependence upon the Military Services for the conduct of the greater part of the background investigations needed for clearance determination. Selection experience has shown that three of every four applicants are rejected because of inadequate qualifications, unsuitability for federal employment or as a result of security consideration. In some special skill areas the rejection rate is much higher. At the very minimum, 6,000 applicants will receive some degree of processing to permit hiring [redacted] new employees under the current fiscal program.

PL 86-36/50 USC 3605

f. Despite the urgency of employing a large number of new personnel, the NSA observes every precaution and exercises every means within its capacity to insure that every individual employed fully meets the stringent security standards established for determining that access to sensitive information is in the best interests of the national security.

6. Identity of Major Program Elements

a. Basically, the overall security program falls into two major parts - physical security and personnel security. For the most part, this report will concern itself with physical security, personnel security and related personnel matters, excluding consideration of COMSEC and technical security matters which are closely interlaced with SIGINT operations such as categorization of COMINT.

b. Physical security is that component of security which results from all physical measures necessary to safeguard classified equipment, material, documents, and information from access to or observation by unauthorized persons. Physical security, therefore, supplements personnel security by insuring that authorized persons only have access to classified security information, and that, in receiving, handling, transmitting, and storing such information, the necessary facilities and procedures are employed to protect it. A physical security program encompasses installation security to include perimeter control, internal compartmentation, personnel identification, visitor control, and property control. Provision is made for safe storage facilities, including locked cabinets, safes, and vaults. It promulgates and employs secure means and procedures for the destruction of classified waste. It further prescribes and conducts such inspections and surveys as may be required to maintain high standards of physical security.

c. Personnel security is that security instituted to make certain that those persons who are acquiring knowledge or will have access to sensitive information and material, meet standards which indicate that they possess the character, discretion, and loyalty to be able to control the knowledge acquired. The personnel security program is composed of three phases. The first is a pre-employment, or pre-access check; the second is a clearance determination; and the third, personnel security supervision. The purpose of clearance screening processing is to provide assurance, within the limits of human frailties, that access to sensitive information by any individual or group is clearly consistent with the best interests of the nation. Whenever information is furnished one person by another, the donor must accept the fact that the recipient may not properly control the knowledge he so acquires. Pre-access checks and clearance determinations, then, are the means

by which the Government (a) endeavors to prejudge the ability and willingness of an individual to control the knowledge he will receive, and (b) tries to assure itself that the risk to the national security in permitting access to sensitive information is acceptable. After a person is cleared and receives access to highly classified sensitive information, the potential damage he can do becomes greater as his access becomes greater. It is necessary, therefore, that the utmost efforts be applied to ensure the continuing reliability and suitability of cleared personnel.

7. Organization for Administration of the Security Program

a. Insofar as the organization within the Agency is concerned regarding security administration, the Director of Security has been delegated certain distinct authorities by the Director of the NSA. Primarily, these authorities relate to security clearances and the control of access to classified information. In effect, the Office of Security Services is a staff or service element of the Agency providing support in those areas of security for which it has been expressly assigned cognizance.

b. The Director of Security is specifically charged with assisting and advising the Director, NSA, in the execution of security responsibilities; with providing the professional staff necessary to implement the Agency's security policies; with insuring that Agency material and space are protected from unauthorized persons; with obtaining all the information necessary to permit a determination that persons authorized access to Agency material meet and continue to meet prescribed clearance standards; and with providing security guidance, when requested, to U. S. activities under the operational and technical control of the Director, NSA.

c. To properly assume the responsibilities and accomplish assigned tasks, the Director, NSA, has organized the Office of Security Services into several operating entities, each charged with a specific portion of the security mission. The Office of Security Services has been structurally organized to consist of the directing element, a plans and management staff, a records processing and maintenance unit, and the following five divisions:

(1) Physical and Industrial Security Division

(2) Clearance Division

(3) Personnel Interview Division (Polygraph Screening)

(4) Special Operations Division (Personnel Security Investigations)

(5) Security Education Division

The organizational structure of the Office of Security Services and also of the Office of Personnel Services are displayed in greater detail and in a manner showing relationship to other segments of Management Organizations in Tabs I through K. Further, specific functional responsibilities of each of the organizational segments portrayed are specifically detailed in Tabs J and K.

Although this paper is based on pertinent directives, the wording of the original directives has, in many cases, been condensed or gisted for the purposes of this paper; it is not necessarily a complete statement or an exact transcription of the basic directive. None of this should be quoted for official purposes without reference to the original directives.

Table of Appendices


A

Change #2 entered 12 July 61, which superseded Ch #1.
CTB R.B. Brown
[illegible]

~~SECRET~~

March 19, 1959
NUMBER S-5100.20

Department of Defense Directive

SUBJECT The National Security Agency

I. GENERAL

Subject to the provisions of NSCID No. 6, dated September 15, 1958, and the provisions of the National Security Act of 1947, as amended, and pursuant to the authorities vested in the Secretary of Defense, the National Security Agency is established as a separately organized agency within the Department of Defense under the direction, authority and control of the Secretary of Defense.

II. ORGANIZATION

A. The National Security Agency shall consist of a Director, a Headquarters, and such subordinate units, facilities and activities as are specifically assigned to the National Security Agency by the Secretary of Defense or are established by the Director, NSA.

B. The National Technical Processing Center and the Electronic Intelligence Coordinating Group, established pursuant to DOD Directive S-3115.2, dated July 13, 1955, are abolished. Assigned functions, records, facilities and equipment are hereby transferred to the National Security Agency. Military and civilian personnel (including authorized personnel spaces), and supporting funds, are also transferred, as mutually agreed between the National Security Agency and the military services.

III. RESPONSIBILITIES

The National Security Agency, under the direction and control of the Director of the Agency, shall be responsible for the following functional fields as specifically prescribed in appropriate NSC and DOD Directives:

~~SECRET~~

EXCLUDED FROM AUTOMATIC REGRADING;
DOD DIR 5200.10 DOES NOT APPLY

1. Communications intelligence (COMINT).

2. Electronics intelligence (ELINT).

3. Other functional fields assigned by specific NSC and DOD Directives.

IV. FUNCTIONS

Under the direction and control of the Director of the National Security Agency, the Agency shall perform the following functions within its assigned fields of responsibilities:

1. Formulate plans, policies, procedures and principles.

2. Subject to the supervision of the Director of Defense Research and Engineering, conduct research and engineering activities to meet the needs of the National Security Agency and the departments and agencies and coordinate the related research, development, test and evaluation conducted by such departments and agencies.

3. Determine and submit to the Secretary of Defense logistic support requirements for the Agency, together with specific recommendations as to what each of the responsible departments and agencies of the Government should supply.

4. Prepare in collaboration with the military departments and submit to the Secretary of Defense a consolidated DOD budget, and requirements for military and civilian manpower, logistic and communications support, and research, development, test and evaluation, together with his recommendations pertaining thereto.

5. Develop requisite security rules, regulations and standards governing operating practices in accordance with the policies of the U.S. Intelligence Board and the U.S. Communications Security Board.

6. Make reports and furnish information to the U. S. Intelligence Board or the U.S. Communications Security Board, as required.

7. Produce and disseminate COMINT and ELINT information in accordance with objectives, requirements and priorities established by the U.S. Intelligence Board. (This function will not include the production and dissemination of finished intelligence which are the responsibilities of departments and agencies other than the National Security Agency.)

8. Perform such other functions as the Secretary of Defense or other proper authority assigns.

V. RELATIONSHIPS

A. In the performance of its functions, the Agency shall:

1. Coordinate actions, as appropriate, with the military departments, other DOD agencies, and other departments and agencies of the Government having collateral or related functions in the fields of its assigned responsibilities.

2. Maintain active liaison, as appropriate, for the exchange of information and advice in the field of its assigned responsibility with the military departments, other DOD agencies and other departments and agencies of the Government.

3. Make full use of established facilities in the military departments, other DOD agencies, and other departments and agencies of the Government, rather than unnecessarily duplicating such facilities.

4. Provide for participation by representatives of each of the members of the U.S. Intelligence Board in those offices of the National Security Agency where priorities of intercept and processing are established by the Director of the National Security Agency.

B. Officials of the military departments and other DOD agencies shall provide support, within their respective fields of responsibility, to the Director of the National Security Agency as may be necessary to carry out the assigned responsibilities of the Agency.

VI. AUTHORITIES

A. To carry out assigned responsibilities of the Agency, the Director of the National Security Agency is specifically delegated authority to:

1. Exercise operational and technical control of COMINT and ELINT intercept and processing activities of the United States to the extent prescribed in other specific DOD Directives.

2. Issue instructions pertaining to COMINT and ELINT to the Chiefs of the operating agencies of the Services or civilian departments or agencies when action by them is required. However, because of the unique technical character of COMINT and ELINT operations, the Director is authorized to issue direct to any operating elements under his operational control task assignments and pertinent instructions which are within the capacity of such elements to accomplish. Compliance with instructions issued by the Director is mandatory, subject only to appeal to the Secretary of Defense by the head of the department and agency concerned (military department, other DOD agency, or other department or agency of the Government).

3. Have direct access to, and direct communication with, any element of the department or agency (military department, other DOD agency, or other department or agency of the Government) performing COMINT and ELINT functions over which he exercises operational and technical control.

4. Centralize or consolidate the performance of COMINT and ELINT functions for which he is responsible to the extent he deems feasible, in consonance with the aims of maximum overall efficiency, economy and effectiveness.

5. Prescribe policies, procedures, principles, and issue instructions for activities under his operational or technical control, as appropriate.

6. Prescribe, or review and approve security rules, regulations and instructions, as appropriate.

7. Obtain such information and intelligence material from the departments and agencies (military departments, other DOD agencies, or other departments or agencies of the Government) as may be necessary for the performance of the Agency's functions.

8. Maintain a departmental property account for the Agency.

B. In providing direct COMINT and ELINT support to the military departments, other DOD agencies and other departments and agencies of the Government, the Director of the National Security Agency is authorized to delegate operational control of specified COMINT and ELINT facilities and resources as he determines appropriate.

C. Other authorities specifically delegated by the Secretary of Defense or other proper authority to the Director of the National Security Agency in other directives or issuances will be referenced in an inclosure to this directive.

VII. ADMINISTRATION

A. The Director of the National Security Agency shall be a commissioned officer of the Armed Forces, on active duty, designated by the Secretary of Defense, after consultation with the Joint Chiefs of Staff, and shall have at least three-star rank while serving in this position. His appointment shall be for a term of four years. The Director shall report to the Secretary of Defense through the Assistant to the Secretary of Defense (Special Operations).

B. There shall be a civilian Deputy appointed by the Director of the Agency with the approval of the Secretary of Defense.

C. To the extent applicable and consistent with the functions assigned to the Agency, Department of Defense policies, regulations and procedures will govern the Agency's operations.

D. The Agency will be authorized such personnel, facilities, funds and other administrative support as the Secretary of Defense deems necessary for the performance of its functions. The military departments, other DOD agencies, or other departments and agencies of the Government, as appropriate, shall provide support for the Agency as prescribed in specific directives or support agreements.

~~SECRET~~

VIII. CANCELLATION

Secretary of Defense memorandum dated December 5, 1952, subject: "Implementation of NSCID No. 9, Revised" and DOD Directive S-3115.2, dated July 13, 1955, are hereby canceled. (NSCID No. 6, dated September 15, 1958, superseded NSCID No. 9, Revised, dated October 24, 1952).

IX. EFFECTIVE DATE

This Directive is effective upon publication.

Secretary of Defense

Inclosure - 1

Mar 19, 59#
S-5100.20 (Incl 1)

Listing of Specific Delegations of Authority by the Secretary of Defense to the Director of the National Security Agency

1. Administrative authorities required for the administration and operation of the National Security Agency, as prescribed in DoD Directive 5100.23, dated August 25, 1959.

2. Authority to authorize or request the procurement of cryptologic material and equipment by the military departments, as prescribed in DoD Directive 5160.13, dated March 20, 1956.

3. Authority to establish and administer programs of training, as prescribed in DoD Directive 1430.4, dated October 27, 1958.

4. Authority to assign the classification of TOP SECRET, as prescribed in DoD Directive 5200.1, dated July 8, 1957, and by Secretary of Defense memorandum, dated June 3, 1958.

* 5. Authority to determine the eligibility of individual civilian officers and employees to transport or store their privately owned motor vehicles at Government expense, in accordance with provisions of DoD Directive 1418.3, dated June 19, 1961. *

#Revised June 23, 1961

August 25, 1959
NUMBER 5100.23

Adm. Asst., S/D

Department of Defense Directive

SUBJECT Administrative Arrangements for the National Security Agency

References: (a) DoD Directive S-5100.20, "The National Security Agency"
(b) DoD Directive 5148.4, "Assistant to the Secretary of Defense (Special Operations)"

I. PURPOSE

The purpose of this directive is to prescribe certain administrative arrangements and to delegate the administrative authorities required for the administration and operation of the National Security Agency.

II. POLICY

A. The Director of the National Security Agency shall make maximum use of the established facilities in the military departments for procurement, accounting, disbursing, investigative and related administrative operations rather than unnecessarily duplicating such facilities in the Agency.

B. Officials of the military departments shall provide such support within their respective fields of responsibility, to the Director of the National Security Agency as may be necessary to carry out the assigned responsibilities of the Agency.

III. ADMINISTRATIVE ARRANGEMENTS

The following specific arrangements and provisions will be applied in the administration and operation of the National Security Agency:

A. The Department of the Army will act as fiscal agent for the Agency and in that capacity will:

1. Incorporate into its annual budget estimates the amounts determined by the Secretary of Defense to be necessary for operation and maintenance, procurement, and research, development, test and evaluation activities, including the amounts required for confidential expenses. Such amounts will be in addition to the budget of the Department of the Army for other functions.

2. Allocate appropriations, as approved by the Secretary of Defense, to accounts established for the National Security Agency.

3. Provide disbursing and financial accounting services, as appropriate, in connection with the expenditure of funds by the Agency.

The Agency, to the extent practicable, will conform to such budgetary and fiscal accounting procedures as may be required by the Department of the Army for similar activities. This arrangement, however, will not be construed or so utilized as to effect any administrative controls by the Department of the Army over the fund resources of the Agency other than those which may be imposed by the Secretary of Defense or required by law.

B. The Agency will utilize the established facilities and services of the three military departments, as appropriate, for effecting the procurement of equipment, supplies and services and for the disposition of excess equipment and supplies, including the disposal of surplus printing, binding and related equipment.

1. To the extent practicable and consistent with its purpose and objectives, the Agency will comply with the procurement regulations and practices of the individual military department furnishing this service. The need for and propriety of the items procured is a matter for determination by the Director of the National Security Agency and the military departments will assume no responsibility for such procurement, except when required by law as a part of the procurement process.

2. The costs of items purchased for the Agency will be charged to appropriations made available to the Agency, but no charge will be made for indirect or overhead

expenses for the procuring services unless such facility is operating under a Working Capital or Management Fund and it is the normal practice to include a charge for overhead.

3. Requests for procurement action made by the Agency to the military departments will bear an appropriate certificate indicating the funds that are properly chargeable and that such are available.

4. Although the Agency will operate its own printing plants, it will utilize the facilities of the military departments for the disposal of printing, binding and related equipment that is surplus to the needs of the Agency. Such equipment will be removed promptly from the Agency facility by the military department concerned. When such equipment is being replaced, it will be removed concurrently with or prior to, as appropriate, the delivery of the replacement items. In other instances, when it is necessary for the convenience of the Agency that surplus printing equipment be removed prior to its final disposition by a military department or the General Services Administration, the cost of the removal will be borne by the Agency.

5. Other excess or surplus equipment and supplies of the Agency will be disposed of in accordance with arrangements worked out between the military departments and the Agency.

* C. The Department of the Army will be responsible for the performance *
* of internal audits of the National Security Agency. These audits will be *
* performed for the Secretary of Defense in accordance with audit policies *
* established in DoD Directive 7600.2 and DoD Instruction 7600.3. Reports of *
* audit will be addressed to the Director, National Security Agency, with a *
* copy of each audit report being forwarded simultaneously by the Army Audit *
* Agency directly to the Assistant Secretary of Defense (Comptroller) and the *
* Assistant to the Secretary of Defense (Special Operations), respectively, *
* immediately upon issuance. Within sixty days from the date each report is *
* issued, the NSA will submit to the ASD(Comp), through the ATSD(SO), a state- *
* ment of actions taken, to be taken, or other comments, with respect to each *
* recommendation contained in the report. *

D. Statistics, reports or information which will disclose the organization of any function of the NSA, any of its activities, or the names, titles, salaries, or numbers of persons employed by the Agency will not be released outside the Department of Defense to any individual, organization, or government department or agency except when authorized by the Director, NSA, the Secretary of Defense, or other proper authority, or when required by law. Statistics, and progress or status reports, including those pertaining to personnel employed by or assigned to the National Security Agency, which are required by activities of the Office of the Secretary of Defense will be submitted by the Agency to the Directorate of Statistical Services, OASD(Comp), in accordance with the provisions of DoD Directive 7700.1

#Revised May 11, 1961

E. All military and civilian positions of the National Security Agency are hereby designated as "sensitive positions" and will be treated as such in connection with investigative, security clearance, and employment matters governed by DoD Directives 5210.7 and 5210.8.

F. The provisions of DoD Directive 1400.7 and related DoD instructions issued by the Assistant Secretary of Defense (Manpower) will apply to the NSA. The Director of the Agency will designate an "Employment Policy Officer" and will establish and administer the procedures for employment policy matters as required by the pertinent DoD directives and instructions.

IV. DELEGATION OF AUTHORITY

A. An inclosure to this directive contains a delegation of the various administrative authorities required by the Director of the National Security Agency to administer and direct the operations of the Agency, including those required as a result of the enactment of Public Law 86-36.

B. All civilian positions established in the National Security Agency under the authority of the Classification Act of 1949, as amended, and Section 1581(a) of Title 10, U.S. Code, which were in effect immediately prior to the effective date of Public Law 86-36 (73 Stat. 63), as well as the compensation for such positions and the appointments of the incumbents of such positions will continue in effect under Public Law 86-36 until other appropriate action is taken in accordance with the applicable provisions of this Directive and the attached delegation of authorities to the Director of the National Security Agency.

V. CANCELLATION

Secretary of Defense memoranda dated May 19, 1954, March 7, 1955, August 10, 1956, and July 10, 1958, delegating certain administrative authorities and prescribing arrangements for administrative services for the National Security Agency, and Secretary of Defense memorandum dated July 2, 1959, continuing all civilian positions in the Agency are hereby superseded and cancelled.

VI. EFFECTIVE DATE

This Directive is effective upon publication.

Deputy Secretary of Defense

Inclosure - 1
Delegation of Authority

DELEGATION OF AUTHORITY

Pursuant to the authority vested in the Secretary of Defense, the following authorities, as required in the administration and operations of the National Security Agency, are hereby delegated, subject to the authority, direction and control of the Secretary of Defense, to the Director of the National Security Agency, or in the event of the absence or incapacity of the Director, to the person acting for him:

1. Authority to exercise the powers vested in the Secretary of Defense by Section 204 of the National Security Act of 1947, as amended (5 USC 171d), Section 12 of the Administrative Expenses Act of 1946, as amended (5 USC 22a), and Section 2 of Public Law 86-36, dated May 29, 1959 (73 Stat. 63), pertaining to the establishment of positions, the fixing of rates of basic compensation, the employment, the direction and the general administration of civilian personnel of the National Security Agency, subject to the following:

a. For the positions established in the National Security Agency which ordinarily would be subject to the Classification Act of 1949, as amended (5 USC 1113):

(1) The general compensation rules governing positions under the Classification Act of 1949, as amended (5 USC 1132) will be applied.

(2) The rates of basic compensation shall be fixed at the same rates of basic compensation required for positions of corresponding levels under the Act.

(3) Appointments may be made at rates of basic compensation above the minimum rates only when higher rates of basic compensation for similar positions or categories of positions under the Classification Act of 1949, as amended, have been approved by the Civil Service Commission or when otherwise specifically approved by the Secretary of Defense. Such appointments will be made at the same advanced rates of basic compensation as are approved by the Civil Service Commission for similar positions except when otherwise specifically approved by the Secretary of Defense.

b. Positions established at rates of basic compensation equal to rates of basic compensation authorized for Grades 16, 17 and 18 of the General Schedule of the Classification Act of 1949, as amended (5 USC 1113(b)) are subject to approval by the Secretary of Defense.

2. Authority to establish in the National Security Agency not more than fifty civilian positions involving research and development functions which require the services of specially qualified scientific or professional personnel and to fix the rates of basic compensation for such positions at rates not in excess of the maximum rate of compensation authorized by Section 1581(b) of Title 10, U.S. Code. The rates of basic compensation for such positions will be subject to approval by the Secretary of Defense.

3. Authority to grant additional compensation to civilian officers and employees of the National Security Agency who are citizens or nationals of the United States, in accordance with and not to exceed additional compensation authorized by regulations of the State Department or the Civil Service Commission, whichever is applicable, for employees whose rates of basic compensation are fixed by statute.

4. Authority to establish such advisory committees and to employ such part-time advisers as the Director of the National Security Agency considers necessary for the performance of functions of the National Security Agency, pursuant to the provisions of Section 173 of Title 10, U.S. Code.

a. Also, authority to make findings when required to comply with rule 1 in paragraph V.A. of DOD Directive 5030.13, dated May 29, 1959, and to waive compliance with any part or all of the requirements of rules 3, 4 and 5 in paragraph V.A. of DOD Directive 5030.13 for any public advisory committee, other than an industry advisory committee, when the Director of the National Security Agency finds that compliance would render effective utilization of the committee impracticable and that such waiver would be in the public interest.

5. Authority to administer oaths of office incident to entrance into the Executive Branch of the Federal Government or any other oath required by law in connection with employment therein, in accordance with the provisions of the Act of June 26, 1943 (5 USC 16a) and to designate in writing, as may be necessary, officers and employees of the National Security Agency to perform this function.

6. Authority to establish an NSA Incentive Awards Board and to pay cash awards to, and to incur necessary expenses for the honorary recognition of, civilian employees of the Government whose suggestions, inventions, superior accomplishments, or other personal efforts, including special acts or services, benefit or affect the National Security Agency or its subordinate activities in accordance with the provisions of Public Law 763, 83rd Congress (5 USC 2123), Civil Service Regulations, and Department of Defense policies, criteria and standards.

7. Authority to (1) authorize, in case of an emergency, the appointment of a person to a sensitive position for a limited period for whom a full field investigation or other appropriate investigation, including the National Agency Check, has not been completed, and (2) authorize the suspension, but not to terminate the services of an employee in the interest of national security in positions within the National Security Agency in accordance with the provisions of the Act of August 26, 1950, as amended (5 USC 22-1), Executive Order 10450 dated April 27, 1953, as amended, and DOD Directive 5210.7 dated August 12, 1953 (as revised).

8. Authority to clear personnel of the National Security Agency and such other individuals as may be appropriate for access to classified Defense material and information in accordance with the provisions of DOD Directive 5210.8, June 29, 1955 (as revised), "Policy on Investigation and Clearance of Department of Defense Personnel for Access to Classified Defense Information", and Executive Order 10450 dated April 27, 1953, as amended.

9. Authority to act as agent for the collection and payment of taxes imposed by Chapter 9 of the Internal Revenue Code and, as such agent, to make all determinations and certifications required or provided for under Section 1420(e) of the Internal Revenue Code and Section 205 (p)(1) and (2) of the Social Security Act, as amended (42 USC 405(p)(1) and (2)) with respect to employees of the National Security Agency.

10. Authority to authorize and approve overtime work for civilian officers and employees of the National Security Agency in accordance with the provisions of Section 25.221 of the Federal Employees Pay Regulations.

11. Authority to authorize and approve travel for civilian officers and employees of the National Security Agency in accordance with the Standardized Government Travel Regulations, as amended (BOB Circular A-7, Revised) and applicable Department of Defense directives and instructions, and for temporary duty travel only of military personnel

assigned or detailed to the National Security Agency in accordance with Joint Travel Regulations for the Uniformed Services, April 1, 1951, as amended.

a. In addition, authority to authorize and approve invitational travel to persons serving without compensation whose consultive, advisory, or other highly specialized technical services are required in a capacity that is directly related to or in connection with activities of the National Security Agency pursuant to the provisions of Section 5 of the Administrative Expenses Act of 1946, as amended (5 USC 73b-2).

12. Authority to approve the expenditure of funds available for travel by military personnel assigned or detailed to the National Security Agency for expenses incident to attendance at meetings of technical, scientific, professional or other similar organizations in such instances where the approval of the Secretary of Defense or his designee is required by law (5 USC 174a). This authority cannot be redelegated.

13. Authority to develop, establish and maintain an active and continuing Records Management Program, pursuant to the provisions of Section 506(b) of the Federal Records Act of 1950 (64 Stat. 583), (44 USC 396(b)).

14. Authority to classify, declassify and down-grade or up-grade the classification of defense information or material for which the National Security Agency has responsibility pursuant to Executive Order 10501, dated November 5, 1953, as amended, and DOD Directive 5200.1, dated July 8, 1957, and to designate in writing, as may be necessary, officers and employees within the National Security Agency to perform these functions.

15. Authority to purchase or contract through a military department or a Government department or agency outside of the Department of Defense, as appropriate, for supplies, equipment and services for the National Security Agency or for which the National Security Agency is responsible.

16. Authority to establish and use an Imprest Fund for making small purchases of materiel and services other than personal when it is determined more advantageous and consistent with the best interests of the Government, in accordance with the provisions of DOD Directive 7200.1, dated October 28, 1957, and the Joint Regulation of the General Services Administration-Treasury Department-General Accounting Office for Small Purchases Utilizing Imprest Funds.

17. Authority to act for the Secretary of Defense before the Joint Committee on Printing, the Public Printer, and the Director of the Bureau of the Budget on all matters pertaining to printing, binding and publication requirements for the National Security Agency.

18. Authority to publish advertisements, notices or proposals in newspapers, magazines or other public periodicals as required for the effective administration and operation of the National Security Agency (44 USC 324).

19. Authority to appoint Boards of Survey, approve reports of survey, relieve personal liability and drop accountability for property of the National Security Agency reflected in the authorized Departmental Property Account which has been lost, damaged, stolen, destroyed or otherwise rendered unserviceable in accordance with applicable laws and regulations.

20. Authority to promulgate the necessary security regulations for the protection of property and places under the jurisdiction of the Director, National Security Agency, pursuant to paragraphs III.A. and V.B. of DOD Directive 5200.8 dated August 20, 1954.

In making this delegation it is intended that the Director of the National Security Agency utilize, to the maximum extent practicable and feasible, existing facilities of the military departments for procurement, accounting, disbursing, investigative and related administrative operations in lieu of duplicating such facilities in the National Security Agency.

All of the above authorities will be exercised by the Director of the National Security Agency in accordance with the provisions of applicable DOD directives and instructions. The Director of the National Security Agency may redelegate these authorities, as appropriate, and in writing, except as otherwise specifically indicated above or as otherwise provided by law.

This delegation of authorities is effective immediately and supersedes the delegations of authority from the Secretary of Defense to the Director, National Security Agency, dated March 7, 1955 and July 10, 1958.

C

DEPARTMENT OF DEFENSE
DIRECTIVES SYSTEM TRANSMITTAL

NUMBER	DATE	DISTRIBUTION
5210.7-Ch 4	August 4, 1955	5210.7

ATTACHMENTS

None

INSTRUCTIONS FOR RECIPIENTS

The following pen change to DoD Directive 5210.7, "Department of Defense Civilian Applicant and Employee Security Program", August 12, 1953 has been duly authorized:

PEN CHANGE

Revise the wording in Reference (a) to read as follows:

"Department of Defense Directive 5210.8, 'Policy on Investigation and Clearance of Department of Defense Personnel for Access to Classified Defense Information', dated June 29, 1955"

MAURICE W. ROCHE
Administrative Secretary

12 August 1953
NUMBER 5210.7

Department of Defense Directive

SUBJECT Department of Defense Civilian Applicant and Employee Security Program

References:

(a) Secretary of Defense memorandum, dated 14 June 1950, "Policy on Investigation and Clearance of Department of Defense Personnel for Handling Top Secret, Secret, and Confidential Material and Information," as amended by Secretary of Defense memorandum, dated 2 February 1951, and Department of Defense Directive R-5210.2, dated 5 June 1952.

(b) Secretary of Defense memorandum, dated 2 October 1950 "Elimination of Non-sensitive Areas of Employment" and attachment thereto, "Criteria for Determining Eligibility for Employment for Sensitive and Non-sensitive Duties in the Department of Defense"

(c) Secretary of Defense memorandum, dated 19 January 1951, "Loyalty and Security Policies and Procedures" and attachment thereto, "Uniform Criteria for Administration of Loyalty and Security Policies and Procedures for Civilian Personnel in the Department of Defense"

(d) Secretary of Defense memorandum, dated 13 February 1951, "Pre-employment Investigations" and attachment thereto, "Pre-Appointment Investigations"

(e) Department of Defense Directive 5210.7, dated 26 May 1953, "Department of Defense Civilian Applicant and Employee Security Program"

I. PURPOSE

To establish and maintain an effective program to insure that the employment and retention in employment of any civilian officer or employee within the Department of Defense is clearly consistent with the interests of the national security.

II. CANCELLATION

References (b) through (e) are cancelled.

III. AUTHORITY

A. This directive is issued pursuant to the authority vested in the Secretary of Defense by the following:

1. The National Security Act of 1947 (Public Law 253, 80th Congress, as amended).

2. The Act of August 26, 1950 (Public Law 733, 81st Congress).

3. Executive Order No. 10450, dated 27 April 1953, "Security Requirements for Government Employment," as amended.

IV. APPLICABILITY

A. This directive applies to the following persons in the Department of Defense:

1. Civilian applicants for employment

2. Civilian officers and employees

V. DEFINITIONS

A. National Security

As used herein, the term "national security" relates to the protection and preservation of the military, economic, and productive strength of the United States, including the security of the government in domestic and foreign affairs, against or from espionage, sabotage, and subversion, and any and all other illegal acts designed to weaken or destroy the United States.

B. Sensitive Position

A "sensitive position" is any position within the Department of Defense, the occupant of which could bring about,

by virtue of the nature of the position, a material adverse effect on the national security. Such positions shall include the following:

1. Any position, the duties or responsibilities of which require access to Top Secret, Secret, or Confidential security information or material.

2. Any other position so designated by authority of the Secretary of Defense or of the Secretary of a Military Department.

VI. POLICY

A. No civilian will be employed or retained in employment in the Department of Defense if his employment or retention in employment is not clearly consistent with the interests of the national security.

B. The use of the suspension and removal procedures authorized by Public Law 733 will be limited to cases in which the interests of the national security are involved. These procedures will be used to supplement, not to substitute for, normal civil service removal procedures. Maximum use will be made of normal civil service removal procedures where national security is not a consideration and such procedures are adequate and appropriate.

VII. STANDARD AND CRITERIA

A. Standard. The standard for the refusal of employment or the removal from employment in the interests of the national security shall be that, based on all the available information, it is determined that employment or retention in employment of the person concerned is not clearly consistent with the interests of the national security.

B. Criteria for Application of Standard. Information regarding an applicant for employment, or an employee, which may preclude a finding that his employment or retention is clearly consistent with the interests of the national security, shall relate, but shall not be limited, to the following:

1. Depending on the relation of the employment to the national security:

a. Any behavior, activities or associations which tend to show that the individual is not reliable or trustworthy.

b. Any deliberate misrepresentations, falsifications, or omission of material facts.

c. Any criminal, infamous, dishonest, immoral, or notoriously disgraceful conduct, habitual use of intoxicants to excess, drug addiction, or sexual perversion.

* d. Any illness, including any mental condition, of a nature which in the opinion of competent medical authority may cause significant defect in the judgment or reliability of the employee, with due regard to the transient or continuing effect of the illness and the medical findings in such case. *

e. Any facts which furnish reason to believe that the individual may be subjected to coercion, influence, or pressure which may cause him to act contrary to the best interests of the national security.

2. Commission of any act of sabotage, espionage, treason, or sedition, or attempts thereat or preparation therefor, or conspiring with, or aiding or abetting, another to commit or attempt to commit any act of sabotage, espionage, treason, or sedition.

3. Establishing or continuing a sympathetic association with a saboteur, spy, traitor, seditionist, anarchist, or revolutionist, or with an espionage or other secret agent or representative of a foreign nation, or any representative of a foreign nation whose interests may be inimical to the interests of the United States, or with any person who advocates the use of force or violence to overthrow the government of the United States or the alteration of the form of government of the United States by unconstitutional means.

Revised 26 Aug 54

12 Aug 53
5210.7

4. Advocacy of use of force or violence to overthrow the government of the United States, or of the alteration of the form of government of the United States by unconstitutional means.

5. Membership in, or affiliation or sympathetic association with, any foreign or domestic organization, association, movement, group, or combination of persons which is totalitarian, Fascist, Communist, or subversive, or which has adopted, or shows, a policy of advocating or approving the commission of acts of force or violence to deny other persons their rights under the Constitution of the United States, or which seeks to alter the form of government of the United States by unconstitutional means.

6. Intentional, unauthorized disclosure to any person of security information, or of other information disclosure of which is prohibited by law.

7. Performing or attempting to perform his duties, or otherwise acting, so as to serve the interests of another government in preference to the interests of the United States.

8. Participation in the activities of an organization established as a front for an organization referred to in subparagraph 5 above when his personal views were sympathetic to the subversive purposes of such organization.

9. Participation in the activities of an organization with knowledge that it had been infiltrated by members of subversive groups under circumstances indicating that the individual was a part of or sympathetic to the infiltrating element or sympathetic to its purposes.

10. Participation in the activities of an organization, referred to in subparagraph 5 above, in a capacity where he should reasonably have had knowledge of the subversive aims or purposes of the organization.

11. Sympathetic interest in totalitarian, Fascist, Communist, or similar subversive movements.

12. Sympathetic association with a member or members of an organization referred to in subparagraph 5 above.

(Ordinarily this will not include chance or occasional meetings, nor contacts limited to normal business or official relations.)

13. Currently maintaining a close continuing association with a person who has engaged in activities or associations of the type referred to in subparagraphs 2 through 11 above. A close continuing association may be deemed to exist if the individual lives at the same premises as, frequently visits, or frequently communicates with such person.

14. Close continuing association of the type described in subparagraph 13 above, even though later separated by distance, if the circumstances indicate that renewal of the association is probable.

15. The presence of a spouse, parent, brother, sister or offspring in a nation whose interests may be inimical to the interests of the United States or in satellites or occupied areas of such a nation, under circumstances permitting coercion or pressure to be brought on the individual through such relatives.

16. Willful violation or disregard of security regulations.

17. Acts of a reckless, irresponsible or wanton nature which indicate such poor judgment and instability as to suggest that the individual might disclose security information to unauthorized persons or otherwise assist such persons, whether deliberately or inadvertently, in activities inimical to the security of the United States.

* 18. Refusal by the individual, upon the ground of constitutional privilege against self-incrimination, to testify before a congressional committee regarding charges of his alleged disloyalty or other misconduct. *

C. The activities and associations listed in paragraph B above are of varying degrees of seriousness. Therefore, the ultimate determination of whether employment or retention in employment is clearly consistent with the interests of national security must be an over-all common-sense one based on all available information.

VIII. PERSONNEL SECURITY INVESTIGATIONS

A. Investigative Requirements

1. General

The appointment of each civilian officer or employee in the Department of Defense shall be made subject to investigation. The scope of the investigation shall be determined in the first instance according to the degree of adverse effect the occupant of the position sought to be filled could bring about, by virtue of the nature of the position, on the national security, but in no event shall the investigation include less than a national agency check (including a check of the fingerprint files of the Federal Bureau of Investigation), and written inquiries to appropriate local law-enforcement agencies, former employers and supervisors, references, and schools attended by the person under investigation; Provided, that to the extent authorized by the Civil Service Commission, a lesser investigation may suffice with respect to per-diem, intermittent, temporary, or seasonal employees, or aliens employed outside the United States. Should there develop at any stage of investigation information indicating that the employment of any such person may not be clearly consistent with the interests of the national security, the investigation will be extended as necessary to enable the Secretary concerned to determine whether retention of such person is clearly consistent with the interests of the national security.

2. Sensitive Positions

a. Pre-Appointment.

(1) No civilian will be appointed to a sensitive position designated by the Secretary of Defense, the Secretary of the Army, the Secretary of the Navy, or the Secretary of the Air Force, which involves responsibility for the development or approval of war plans, plans or particulars of future major or special operations of war, or critical and extremely important items of war, or policies and programs which affect the overall operations of the Department of Defense, the Department of the Army, the Department of the Navy, or the Department of the Air Force, prior to completion with satisfactory results

of a full field investigation, which in no event will be less than a Background Investigation as defined in Reference (a); Provided that, in case of emergency, such position may be filled for a limited period by a person with respect to whom a full field investigation has not been completed if the Secretary concerned or his designee finds that such action is necessary in the interests of national defense, which finding shall be made a part of the records of the department concerned; and provided further, that a national agency check with satisfactory results has first been completed.

(2) Civilian appointees for other sensitive positions in the Department of Defense will be subject to the investigative requirements as prescribed in Reference (a), but in no event shall include less than the investigation prescribed in A. 1 above; Provided that, as a minimum, a national agency check with satisfactory results shall be completed prior to appointment; and provided further that, in case of emergency, such position may be filled for a limited period by a person with respect to whom such investigation, including the national agency check, has not been completed if the Secretary concerned or his designee finds that such action is necessary in the interests of national defense, which finding shall be made a part of the records of the department concerned.

b. Incumbents

(1) No civilian officer or employee of the Department of Defense will continue to occupy positions designated in accordance with 2.a.(1) above unless there has been conducted with respect to such person a full field investigation with satisfactory results; Provided, that a person occupying such a position may continue to occupy the position pending the completion of a full field investigation.

(2) Civilian officers or employees of the Department of Defense occupying positions referred to in 2.a.(2) above will be subject to the investigative requirements prescribed in that sub-paragraph.

B. Referral to Federal Bureau of Investigation

Investigations which develop information indicating that an individual may have been subjected to coercion, influence, or pressure to act contrary to the interests of the national security or information relating to any of the matters described in Section VII B 2 through 16 shall be referred promptly to the Federal Bureau of Investigation for a full field investigation.

C. Security-Investigation Index

This index is maintained by the Civil Service Commission under Section 9(a) of Executive Order No. 10450. In order to comply with Section 9(b) of the said Executive Order, the investigative agencies, which conduct personnel security investigations, will prepare and submit, in triplicate, Standard Form 79 (Notice of Security Investigation) to the Investigations Division, United States Civil Service Commission, Washington 25, D. C., on the same day the investigation is initiated. Additionally, appropriate information concerning each person, who has been suspended or terminated under Public Law 733, will be furnished to the Civil Service Commission.

D. Custody of Investigative Information

The reports and other investigative material and information developed by investigations conducted pursuant to Public Law 733, Executive Order No. 9835, or any other security or loyalty program relating to officers or employees of the government, shall remain the property of the investigative agencies conducting the investigations, but may, subject to considerations of the national security, be retained by the department or agency concerned. Such reports and other investigative material and information shall be maintained in confidence, and no access shall be given thereto except, with the consent of the investigative agency concerned, to other departments and agencies conducting security programs under the authority granted by or in accordance with Public Law 733, as may be required for the efficient conduct of government business.

IX. CRITERIA GOVERNING APPLICATION OF PUBLIC LAW 733 AUTHORITY

A. Delegation of Authority

1. The authority contained in Public Law 733 to suspend an employee in the interest of national security may be delegated by the Secretaries to appropriate subordinate officials below the Secretarial level.

2. The authority contained in Public Law 733 to terminate the services of an employee in the interest of national security may not be exercised by subordinate officials below the Secretarial level.

B. Suspension and Termination

Should there develop at any stage of investigation information indicating that the employment of any officer or employee of the Department of Defense may not be clearly consistent with the interests of the national security, the Secretary concerned or his designee shall immediately suspend the employment of the person involved if he deems such suspension necessary in the interests of the national security and, following such investigation and review as he deems necessary, the Secretary concerned shall terminate the employment of such suspended officer or employee whenever he shall determine such termination necessary or advisable in the interests of the national security, in accordance with Public Law 733. However, employees should not be suspended under this authority pending further investigation when the available information indicates that retention in a duty status during such investigation would not be likely to have a material adverse effect on the security of the activity or of classified security information or material, nor on mere suspicion, nor for disciplinary reasons or any other reasons which can be appropriately handled under some other authority. When considered necessary in order to provide the maximum protection to the security of the activity or of classified security information or material pending determination under Public Law 733, interim action other than suspension should be used to the fullest practicable extent.

C. Procedural Benefits

1. An employee of the Department of Defense who has been suspended under Public Law 733 and whose termination under that Act is proposed will be granted procedural benefits in accordance with the provisions of that Act.

   a. The thirty-day time limits specified in Public Law 733 shall be construed to mean calendar days.

   b. Statements of charges given to an employee under Public Law 733 will be as specific as security considerations permit. No information which is relevant to the charges against him will be used as a basis for terminating his employment unless it has been excluded from the statement of charges and the hearing for valid security reasons, or unless it has been revealed to the employee during the adjudication process in such a manner that his ability to present a defense thereto has not been prejudiced.

c. The notice of suspension will set forth in detail the reasons for initiating the proceedings. Normally the employee will be entitled to all information except that which will reveal classified security information or material, investigative methods, or the identity of confidential informants.

d. The hearing "by a duly constituted authority for this purpose" provided for in Public Law 733 shall be construed to mean a hearing before a board composed of not less than three members, a majority of whom must be civilians.

e. A finding and recommendation by a hearing board which are unfavorable to the employee shall be promptly reviewed by the Secretary concerned or his designee, and the employee notified, in writing, of the Secretarial action on the case. A Secretarial decision favorable to the employee also will be promptly communicated to the employee.

D. Resignations

A resignation submitted by an employee after notice of suspension or other proposed adverse action under Public Law 733 has been communicated to him and before final action has been taken, will be accepted. However, the Standard Form 50 effecting the resignation will bear the notation that the resignation was accepted during action under Public Law 733.

E. Compensation

In case an employee whose employment has been suspended or terminated under Public Law 733 is reinstated or restored to duty by the Secretary concerned, he shall be allowed compensation for the entire period of such suspension or termination in an amount not to exceed the difference between the amount such employee would normally have earned during the period of such suspension or termination at the rate he was receiving on the date of suspension or termination, as appropriate, and the interim net earnings of such employee; provided that the employee shall not be compensated for any extension of the period of suspension or termination caused by his voluntary action and not the result of the action of the agency in suspending or terminating him.

X. REINSTATEMENT, RESTORATION TO DUTY, REEMPLOYMENT (WITHIN THE DEPARTMENT OF DEFENSE)

Any person whose employment is suspended or terminated under the authority granted to heads of departments and agencies by or in accordance with Public Law 733 or pursuant to Executive Order No. 9835 or any other security or loyalty program relating to officers or employees of the government, shall not be reinstated or restored to duty or reemployed in the same department or agency, and shall not be reemployed in any other department or agency, unless the head of the department or agency concerned finds that such reinstatement, restoration, or reemployment is clearly consistent with the interests of the national security, which finding shall be made a part of the records of such department or agency: Provided, that no person whose employment has been terminated under such authority thereafter may be employed by any other department or agency except after a determination by the Civil Service Commission that such person is eligible for such employment.

XI. REVIEW AND READJUDICATION OF PREVIOUS CASES

Each Secretary or his designee shall review the cases of all civilian officers and employees with respect to whom there has been conducted a full field investigation under Executive Order No. 9835, and after such further investigation as may be appropriate, shall readjudicate, in accordance with Public Law 733, such of those cases as have not been adjudicated under a security standard commensurate with that established under this directive.

XII. REFERRAL OF POSSIBLE DEROGATORY INFORMATION

Whenever there is developed or received by any department or agency of the Department of Defense information indicating that the retention in employment of any officer or employee of the government may not be clearly consistent with the interests of the national security, such information shall be forwarded to the head of the employing department or agency or his designee. In cases referred to the Department of Defense, the Secretary concerned or his designee, after such investigation as may be appropriate, shall review and, where necessary, readjudicate, in accordance with Public Law 733, the case of such officer or employee.

* XIII. REPORTING REQUIREMENTS *

* Pursuant to Executive Order 10550, which amended Executive *
* Order 10450, and in order to assist the Civil Service *
* Commission in discharging its responsibilities under Execu- *
* tive Order 10450, the Military Departments and the Office *
* of the Secretary of Defense will, as soon as possible and *
* in no event later than ninety (90) days after the receipt *
* of the final investigative report on a civilian officer or *
* employee subject to a full field investigation under the *
* provisions of Executive Order 10450, advise the Civil *
* Service Commission as to the action taken with respect to *
* such officer or employee. This report will be in accord- *
* ance with and conform to the reporting requirements of *
* the Civil Service Commission as stipulated in Departmental *
* Circular No. 771, dated 27 October 1954. No OSD Report *
* Control Symbol has been assigned to this requirement. *

XIV. EFFECTIVE DATE

This directive is effective immediately.

XV. IMPLEMENTATION

Existing regulations will be modified as necessary to conform to this directive, and copies of the revised regulations will be forwarded to the Secretary of Defense.

C. E. Wilson

Secretary of Defense

#Revised 16 May 55

D

June 29, 1955
NUMBER 5210.8

Department of Defense Directive

SUBJECT Policy on Investigation and Clearance of Department of Defense Personnel for Access to Classified Defense Information

References: (a) Secretary of Defense memorandum, dated 14 June 1950, subject: "Policy on Investigation and Clearance of Department of Defense Personnel for Handling Top Secret, Secret, and Confidential Material and Information."

(b) Secretary of Defense memorandum, dated 2 February 1951, subject: "Policy on Investigation and Clearance of Personnel within the Department of Defense, its Contractors, and Contractors' Employees for Access to Restricted Data as Defined in the Atomic Energy Act of 1946."

(c) Department of Defense Directive 5210.8, dated 5 June 1952, subject: "Eligibility Criteria for Cryptographic Clearances."

(d) Department of Defense Directive 5200.1, dated 19 November 1953, subject: "Safeguarding Official Information in the Interests of the Defense of the United States."

(e) Department of Defense Directive 5200.3, dated 21 December 1953, subject: "Department of Defense Policy for Assignment of Classification Categories to Official Defense Information," as amended on 15 April 1954.

(f) Department of Defense Directive 5210.7, dated 12 August 1953, subject: "Department of Defense Civilian Applicant and Employee Security Program."

I. PURPOSES

A. To prescribe the policy and general procedure relating to personnel security investigations and the clearance of military and civilian personnel for access to classified

defense information, including cryptographic information and "Restricted Data," when such personnel are citizens of the United States, or aliens in the United States with immigration visa for permanent residence, and are on duty with, employed by, hired on an individual contractual basis, or serving in an advisory capacity to, the Department of Defense or its components whether on a permanent, temporary, or part-time basis and whether or not they are compensated for their services rendered, or compensated from non-appropriated funds.

B. To define the minimum standards of investigation and the criteria upon which clearances may be granted.

C. To effect general uniformity in the field of personnel security investigations and clearances throughout the Military Departments and in all other agencies and activities of the Department of Defense, in order to facilitate the interchange of information pertaining to completed personnel security investigations and clearances granted or denied. Nothing in this directive, however, will be construed as authorizing the disclosure of classified defense information to any person even though a clearance for access may have been or may be granted such person.

II. CANCELLATION

References (a), (b), and (c) are hereby superseded and cancelled.

III. DEFINITIONS

A. Classified Defense Information. Official information which requires protection in the interests of national defense and which is classified for such purpose by appropriate classifying authority in accordance with the provisions of references (d) and (e).

B. National Security. This term relates to the protection and preservation of the military, economic, and productive strength of the United States, including the security of the government in domestic and foreign affairs, against or from espionage, sabotage, and subversion, and any and all other illegal acts designed to weaken or destroy the United States.

C. Alien. As used herein, the term "alien" means any person not a citizen or national of the United States.

D. Immigrant Alien. As used herein, this term means any alien lawfully admitted into the United States under an immigration visa for permanent residence.

IV. POLICY

No person shall be entitled to knowledge of, or possession of, or access to, classified defense information solely by virtue of his office, position, or security clearance. Such information may be entrusted only to those individuals whose official military or other governmental duties require such knowledge or possession and who have been investigated when required and cleared for access in accordance with the minimum standards prescribed by this directive. Clearances serve to indicate that the persons concerned are eligible for access to classified defense information should their official duties so require. As a general policy, no person will be granted a security clearance unless it is affirmatively determined as prescribed herein that such clearance is clearly consistent with the interests of national security.

V. CRITERIA FOR APPLICATION OF POLICY

A. The ultimate determination of whether the granting of a clearance is clearly consistent with the interests of national security must be an over-all common sense determination based on all available information. The activities and associations listed below, whether current or past and while not all inclusive, are of varying degrees of seriousness and warrant initiation of action to effect such determination:

1. Commission of any act of sabotage, espionage, treason or sedition, or attempts thereat or preparation therefor, or conspiring with or aiding or abetting another to commit or attempt to commit any act of sabotage, espionage, treason or sedition.

2. Establishing or continuing a sympathetic association with a saboteur, spy, traitor, seditionist, anarchist, or revolutionist, or with an espionage or other secret agent or representative of a foreign nation, or any representative of a foreign nation whose interests are inimical to the interests of the United States, or with any person who advocates the use of force or violence to overthrow the government of the United States or the alteration of the form of government of the United States by unconstitutional means.

3. Advocacy of use of force or violence to overthrow the government of the United States, or of the alteration of the form of government of the United States by unconstitutional means.

4. Membership in, or affiliation or sympathetic association with, any foreign or domestic organization, association, movement, group, or combination of persons which is totalitarian, Fascist, Communist, or subversive, or which has adopted, or shows, a policy of advocating or approving the commission of acts of force or violence to deny other persons their rights, under the Constitution of the United States, or which seeks to alter the form of government of the United States by unconstitutional means. (An organization, movement, or group, officially designated by the Attorney General of the United States to be totalitarian, Fascist, Communist, or subversive, to advocate or approve forcible or violent denial of Constitutional rights, or to seek alteration of the form of government of the United States by unconstitutional means, shall be presumed to be of a character thus designated until the contrary be established.)

5. Performing or attempting to perform his duties, or otherwise acting, so as to serve the interests of another government in preference to the interests of the United States.

6. Failure or refusal to sign a loyalty certificate, or pleading protection of the Fifth Amendment or of Article 31, Uniform Code of Military Justice, in refusing to completely answer questions contained in required security forms or personal history statements; pleading protection of the Fifth Amendment or of Article 31, Uniform Code of Military Justice, or otherwise failing or refusing to answer any pertinent question propounded in the course of an official investigation, interrogation, or examination, conducted for the purpose of ascertaining the existence or extent, or both, of conduct of the nature described in 1 through 5 above and 7 through 13 below.

7. Participation in the activities of an organization established as a front for an organization referred to in 4 above, when his personal views were sympathetic to the subversive purposes of such organization.

8. Participation in the activities of an organization with knowledge that it had been infiltrated by members of subversive groups under circumstances indicating that the individual was a part of, or sympathetic to, the infiltrating element or sympathetic to its purposes.

9. Participation in the activities of an organization, referred to in 4 above, in a capacity where he should

reasonably have had knowledge of the subversive aims or purposes of the organization.

10. Sympathetic association with a member or members of an organization referred to in 4 above, or sympathetic interest in totalitarian, Fascist, Communist, or similar subversive movements.

11. Currently maintaining a close continuing association with a person who has engaged in activities or associations of the type referred to in 1 through 9 above. A close continuing association may be considered to exist if the individual lives at the same premises as, frequently visits, or frequently communicates with such person.

12. Close continuing association of the type described in 11 above, even though later separated by distance, if the circumstances indicate that renewal of the association is probable.

13. Any facts, other than as set forth in 14 through 19 below, which furnish reason to believe that the individual may be subjected to coercion, influence, or pressure which may cause him to act contrary to the best interests of national security. Among matters which should be considered in this category would be the presence of a spouse, parent, brother, sister, or offspring in a nation, a satellite thereof, or an occupied area thereof, whose interests are inimical to the interests of the United States.

14. Willful violation or disregard of security regulations.

15. Intentional unauthorized disclosure to any person of classified information, or of other information disclosure of which is prohibited by law.

16. Any deliberate misrepresentation, falsification, or omission of material fact.

17. Any criminal, infamous, dishonest, immoral, or notoriously disgraceful conduct, habitual use of intoxicants to excess, drug addiction, or sexual perversion.

18. Acts of a reckless, irresponsible or wanton nature which indicate such poor judgment and instability as to suggest that the individual might disclose security information to unauthorized persons or otherwise assist such persons, whether deliberately or inadvertently, in activities inimical to the security of the United States.

19. All other behavior, activities, or associations which tend to show that the person is not reliable or trustworthy.

20. Any illness, including any mental condition, of a nature which in the opinion of competent medical authority may cause significant defect in the judgment or

reliability of the individual, with due regard to the transient or continuing effect of the illness and the medical findings in such case.

VI. TYPES OF INVESTIGATIONS

A. Personnel security investigations shall be of two types, as follows:

1. National Agency Check.

2. Background Investigation.

B. The type of investigation required in any instance will depend on the category of classified defense information to which a clearance for access is required and on the citizenship status of the individual concerned.

C. The minimum standards prescribed herein may be raised in any particular case or category of cases, if deemed desirable by the Military Department or agency concerned.

VII. NATIONAL AGENCY CHECK

A. Components of a National Agency Check. A National Agency Check consists of a check with the following agencies, as indicated, for pertinent facts having a bearing on the loyalty and trustworthiness of the individual:

1. Federal Bureau of Investigation (FBI). The FBI headquarters criminal and subversive files will be checked in every case. A properly completed non-criminal type fingerprint chart will be submitted with each request.

2. Assistant Chief of Staff, G-2, Department of the Army (G-2). Will be checked when the individual is or has been in the Army or a civilian employee of the Department of the Army.

3. Office of Naval Intelligence, Department of the Navy (ONI). Will be checked when the individual is or has been in the Navy, Marine Corps, or Merchant Marine, or a civilian employee of such agencies. (In the case of Coast Guard personnel, or personnel with Merchant Marine background, the files of the U. S. Coast Guard will also be checked.)

4. Office of Special Investigations, The Inspector General, USAF, Department of the Air Force (OSI). Will be checked when the individual is or has been in the Air Force or a civilian employee of the Department of the Air Force.

5. Civil Service Commission (CSC). Will be checked in all cases where the individual is or has been an employee of the United States Government.

6. Immigration and Naturalization Service (I&NS). Will be checked in all cases in which the individual is an alien in the United States, an immigrant alien, or naturalized citizen.

7. House Committee on Un-American Activities (HCUA). Will be checked when pertinent to the inquiry.

8. Central Index Personnel and Facility Security Clearance File (Department of the Army). Will be checked when the Personal History Statement or other available information concerning the individual indicates that he is, or has been, an officer, owner, or employee of a firm which has, or has had, a Department of Defense classified contract.

9. Other Agencies. Will be checked when pertinent to the purpose for which the investigation is being conducted. Investigative agencies concerned will determine when such other agencies should be checked.

B. Extension of Inquiry. In the event derogatory or questionable information concerning an individual is disclosed by a National Agency Check, the inquiry will be extended as necessary to obtain such additional information as may be required to substantiate or disprove the information.

C. Personnel Who Require a National Agency Check. National Agency Checks will be conducted on the following categories of personnel within the Department of Defense, except as otherwise provided in this Directive:

1. U. S. citizen civilian personnel whose employment requires:

   a. Interim clearance for access to Top Secret and cryptographic defense information pending final clearance.

   b. Interim clearance on an emergency basis as a prerequisite for occupancy of those sensitive positions set forth in Section VIII.D.1.b. below. (See reference (f), Section VIII.A.2.a.(1).)

2. U. S. citizen military personnel whose assignment, duty or training requires:

   a. Final clearance for access to Top Secret and cryptographic information, provided that such personnel have had continuous honorable active duty, or a combination of such active duty and civilian employment in government service for ten consecutive years with no break greater than ninety days.

   b. Interim clearance for access to Top Secret and cryptographic defense information.

   c. Final clearance for access to Secret defense information.

   d. Final clearance for access to Secret defense information in connection with short periods of active duty for training purposes, as members of the active National Guard and reserve forces.

   e. Final clearance for access to Secret defense information in connection with training activities, as members of National Guard units and reserve components not on active duty.

3. Civilian and military personnel within the Department of Defense selected for duties in connection with programs involving information, education, and orientation of service personnel, including training for such duties.

VIII. BACKGROUND INVESTIGATION

A. Scope of a Background Investigation. A Background Investigation which is conducted for clearance purposes is designed to develop information as to whether the access to classified material by the person being investigated is clearly consistent with the interests of national security. It shall make inquiry into the pertinent facts bearing on the loyalty and trustworthiness of the individual. It will normally cover the period of his life ~~from 1 January 1937 to the date of the investigation, or from the date of his eighteenth (18th) birthday, whichever is the shorter period, unless:~~ during the last 15 years.

1. Derogatory information is developed in the course of the investigation, in which event the investigation will be extended to any period of the individual's life necessary to substantiate or disprove the information or, unless

2. Additional investigation is specifically required by competent authority.

B. Referral to Federal Bureau of Investigation (FBI). In the event that derogatory information is developed concerning civilians which relates to any of the activities described in Section V.A.1. through 15, it shall be referred immediately to the FBI.

C. Components of a Background Investigation:

1. National Agency Check as outlined in Section VII above.

2. Birth Records. The individual's date and place of birth will be verified through school, employment or other records examined during other investigations. Only if a discrepancy appears, need vital statistics records and any other necessary to establish the individual's correct date and place of birth be examined.

3. Education. Attendance at last school or college will be verified, except that verification of attendance at primary schools is not required in any circumstance; neither is verification of attendance at secondary schools ~~prior to 1937 required~~. Results of attendance at Service schools will, as a rule, appear in the individual's service record and need not be confirmed. In addition to examining school records, persons in a position to know the individual's activities while in attendance should be interviewed, if available.

attended more than 15 years ago.

4. Employment. The records of present and former employers ~~since 1 January 1937,~~ or eighteenth (18th) birthday, whichever involves the shorter period, will be examined to verify the period of employment and efficiency record. Former employers and co-workers will be interviewed, if available, to ascertain the loyalty, character, and reputation of the individual.

during the last 15 years or since

5. References. References will be interviewed. Interviews will also be had with persons (not relatives or former employers) who have knowledge of the individual's background and activities, but who are not given as references by the individual.

6. Neighborhood Investigations. These investigations will be conducted when deemed necessary or expedient in substantiating or disproving derogatory information.

7. Criminal Record. The records of police departments and other law enforcement agencies in the vicinities where the individual has resided or been employed for substantial periods of time will be checked whenever considered appropriate, or if information developed from a National Agency Check is not considered adequate. The records of local FBI offices need not be checked unless special circumstances warrant the advisability of so doing.

8. Military Service. The service of the individual in the armed forces and type of discharge will be verified.

9. Foreign Connections. Any connections the individual has had with foreigners in the United States or abroad will be reported. The extent and purpose of any such connections will be ascertained as well as the relationship of the individual to such persons or organizations.

10. Citizenship Status. In all cases the citizenship status of the individual will be established.

    a. United States Citizens. (See 2 above.)

    b. Immigrant Aliens. The records of the Immigration and Naturalization Service, Washington, D. C., will be searched to verify date and place of birth, legal entry into the United States, and to ascertain whether the individual has indicated an intention to become a citizen of the United States.

    c. Naturalized Citizens. The naturalization and date and place of birth will be verified through records of the appropriate U. S. District Court. If the place of naturalization cannot be determined, I&NS Records, Washington, D. C., will be examined.

11. Foreign Travel. If the individual has travelled outside the United States ~~since 1 January 1937~~ during the last 15 years, except in military or naval service, the Department of State records will be checked to determine reasons for such travel. If such travel occurred after 1 July 1946, records of the Central Intelligence Agency (CIA) will also be checked.

12. Credit Record. Whenever necessary, credit agencies and/or credit references will be contacted in those places where the individual has resided for substantial periods of time ~~since 1 January 1937 or~~ eighteenth (18th) birthday, whichever is the shorter period.

during the last 15 years or since

13. Organizations. During the course of the investigation, as set forth above and by examination of personal history statements and other records examined, efforts will be made to determine if the individual had:

"Membership in, or affiliation or sympathetic association with, any foreign or domestic organization, association, movement, group, or combination of persons which is totalitarian, Fascist, Communist, or subversive, or which has adopted, or shows, a policy of advocating or approving the commission of acts of force or violence to deny other persons their rights under the Constitution of the United States, or which seeks to alter the form of government of the United States by unconstitutional means." (Section 8(a)(5), Executive Order 10450)

D. Personnel Required to Receive Background Investigation:

1. The following persons in the Department of Defense are required to be given a Background Investigation, except as otherwise provided in this Directive:

a. Civilian and military personnel whose assignment, duty, training or employment requires that they have access to Top Secret defense information, including members of the organized National Guard and reserve forces not on active duty whose training activities require access to Top Secret defense information.

b. Civilian employees assigned to any position which involves responsibility for the:

(1) Development or approval of war plans.

(2) Development or approval of plans or particulars of future major or special operations of war.

(3) Development or approval of critical and extremely important items of war.

(4) Development or approval of policies and programs which affect the over-all operations of the

Office of the Secretary of Defense, Department of Army, Department of Navy, or Department of Air Force.

c. Members of Security Screening, Hearing and Review Boards.--Military personnel who have been granted final Top Secret clearances under the criteria established in Section IX.A.1.a.(2)(b) below, and upon whom a Background Investigation has been initiated, may be appointed as members of boards which pass upon alleged disloyal, subversive, or disaffected military personnel constituting a security risk.

d. Immigrant aliens who require access to classified defense information classified Confidential or higher.

e. Consultants, temporary or part-time employees and civilians paid from non-appropriated funds, whose duties require access to Top Secret defense information.

f. Civilian and military personnel assigned to duties in connection with or having access to prescribed classified cryptographic systems, but subject to additional qualifications as set forth in Section XV below.

IX. CLEARANCES

A. Civilian and military personnel and immigrant aliens who are employed by, hired on a contractual basis by, or serving in an advisory capacity to the Department of Defense, whether on a permanent, temporary, or part-time basis, and whether or not they are compensated for their services rendered, or compensated from non-appropriated funds, may be declared eligible for access to classified defense information by being granted a final or interim clearance under the minimum requirements set forth below for each category of defense information, and provided that no derogatory information based on criteria set forth in Section V is developed indicating that the clearance of the individual is not clearly consistent with the interests of national security. In addition, an immigrant alien to be eligible for clearance shall have formally declared his intent to become a U. S. citizen. (For cryptographic clearances, see Section XV below.) Any activity granting an interim clearance must insure that the additional investigative procedure necessary to satisfy the final clearance requirements is in progress.

1. Top Secret

a. Final Clearance

(1) Civilian Personnel - U. S. Citizens

(a) Background Investigation, or

(b) When the individual occupies a specific office in the Department of Defense, to which he has been appointed by the President by and with the advice and consent of the Senate.

(2) Military Personnel - U. S. Citizens

(a) Background Investigation, or

(b) National Agency Check plus

(i) Continuous honorable active duty as a member of the armed forces, or a combination of such active duty and civilian employment in government service on a continuous basis, for a minimum of ten consecutive years (with no break greater than ninety days) immediately preceding the date of the current investigation, plus

(ii) Check of Unit Personnel Records, 201 File, or Bureau of Naval Personnel File, Intelligence Field File or Special File or ONI Case History File, to determine if any derogatory information exists concerning the individual, or

(c) When the individual occupies a specific office in the Department of Defense to which he has been appointed by the President by and with the advice and consent of the Senate.

(3) Immigrant Aliens

Background Investigation.

b. Interim Clearance

(1) Civilian Personnel - U. S. Citizens

(a) National Agency Check, except that only in

case of emergency as set forth in Section VIII of Reference (f), may an interim clearance be granted to employees occupying positions involving responsibilities listed in Section VIII D.1.b, hereof.

(2) Military Personnel - U. S. Citizens

(a) National Agency Check, or

(b) Continuous honorable active duty as a member of the armed forces, or a combination of such active duty and civilian employment in government service on a continuous basis for a minimum of five consecutive years (with no break greater than ninety days), immediately preceding the date of the current investigation, plus a check of files required in Subparagraph a(2)(b)(ii) above.

(3) Immigrant Aliens

No interim clearance authorized.

2. Secret

a. Final Clearance

(1) Civilian Personnel - U. S. Citizens

National Agency Check and, in addition, written inquiries to appropriate local law enforcement agencies, former employers and supervisors, references, and schools attended as required by Section VIII of Department of Defense Directive 5210.7 pursuant to Executive Order 10450; except that a Background Investigation is required for employees occupying positions involving responsibilities listed in Section VIII.D.1.b, hereof.

(2) Military Personnel - U. S. Citizens

National Agency Check.

(3) Immigrant Aliens

Background Investigation.

b. Interim Clearance

(1) Civilian Personnel - U. S. Citizens

(a) National Agency Check.

(b) In case of emergency, interim clearance for access to Secret may be granted for a limited period without a National Agency Check provided responsible authority finds that such action is necessary in the interests of national defense. (See Section VIII A.2.a(2) of Department of Defense Directive 5210.7.) This action shall be based upon a check of available records.

(2) Military Personnel - U. S. Citizens

Check of files required in Subparagraph 1.a(2)(b)(ii) above.

(3) Immigrant Aliens

No interim clearance authorized.

3. Confidential

a. Final Clearance

(1) Civilian Personnel - U. S. Citizens

National Agency Check and, in addition, written inquiries to appropriate local law enforcement agencies, former employers and supervisors, references, and schools attended, as required by Section VIII of Department of Defense Directive 5210.7 pursuant to Executive Order 10450.

(2) Military Personnel - U. S. Citizens

Formal investigation will not be required, but a check of the files required in Subparagraph 1.a(2)(b)(ii) above will be conducted.

(3) Immigrant Aliens

Background Investigation.

b. Interim Clearance

(1) Civilian Personnel - U. S. Citizens

(a) National Agency Check.

(b) In case of emergency, interim clearance for access to Confidential may be granted for a limited period without a National Agency Check provided responsible authority finds that such action is necessary in the interests of national defense. (See Section VIII A.2.a.(2) of Department of Defense Directive 5210.7.) This action shall be based upon a check of available records.

(2) Military Personnel - U. S. Citizens

None required.

(3) Immigrant Aliens

No interim clearance authorized.

4. Access Pending Clearance Requirements - U. S. Citizens

When immediate access to classified defense information is required in order for the individual concerned to carry out his assigned task, and because of exceptional circumstances the delay caused by awaiting interim clearance would be harmful to the national interest, the commander or responsible authority empowered to grant clearances may authorize such access to U. S. citizens, based on the records immediately available, except for employees occupying positions involving responsibilities listed in Section VIII D.1.b. In each such case of granting immediate access, a record of the authorization shall be made and the commander or responsible authority concerned will immediately institute the procedures necessary to satisfy clearance requirements. This authority does not abrogate any of the civilian employment requirements set forth in Reference (f).

5. Access by Aliens

a. Aliens, other than immigrant aliens, employed by, hired on a contractual basis by, or serving in an advisory capacity to the Department of Defense, whether on a permanent, temporary, or part-time basis, and whether or not they are compensated for their services rendered, are not eligible for

security clearances but may be granted access to classified defense information under the following conditions:

(1) Appropriate authority may grant an alien a "Limited Access Authorization" in cases when it is determined that employment of the alien in duties requiring access to certain classified defense information is necessary in the interest of furthering the mission of the command or installation. However, in the interests of national security, it is essential that strict limitations be placed on the types of positions in which aliens may be utilized and the types of classified defense information which may be disclosed. Every effort will be made to insure that aliens are not employed in duties involving access to classified defense information except in exceptional cases and when the need is clearly established.

(2) For granting an alien a Limited Access Authorization, there shall have been completed with satisfactory results a Background Investigation. If geographic and political situations prevent the full completion of a Background Investigation, as described in Section VIII, access by the alien shall not be authorized unless the investigative information obtainable is sufficiently complete and reliable to enable the authority empowered to grant access to determine that such access is clearly consistent with the interests of national security.

(3) In addition to the above, access to Top Secret defense information may be granted only upon the specific authorization of the Secretary of the Department concerned.

X. INVESTIGATIONS BY OTHER GOVERNMENTAL AGENCIES

A. Whenever a prior investigation by any investigative agency of the Federal Government meets the standards prescribed in this Directive, clearance may be granted upon the review of the prior investigation, provided that service with the Federal Government has been continuous or no break in service longer than ninety (90) days, since completion of this prior investigation, and an inquiry of the agency of prior employment discloses no reason why clearance should not be granted. If the prior investigation does not meet such standards, supplemental or additional investigation will be conducted.

B. Acceptance of Investigations Conducted for Civilian Employment

1. The following investigations may be accepted for investigative or clearance purposes within the Department of Defense as indicated, provided the person has been continually in the employ of the Executive Branch of the Federal Government or no break longer than ninety (90) days since the completion of the investigations, and an inquiry to the agency of prior employment discloses no reason why clearance should not be granted.

   a. "Record check and inquiry" conducted by the Civil Service Commission pursuant to Section 3, Part 1, Executive Order 9835, may be accepted as the equivalent of the National Agency Check plus written inquiries.

   b. "Preappointment loyalty check" conducted by the Civil Service Commission pursuant to Executive Order 9835, provided an FBI fingerprint check is included, may be accepted as the equivalent of a National Agency Check. This does not include the record checks conducted by the FBI under Part VI, Executive Order 9835, since such checks are not the equivalent of a National Agency Check.

   c. National Agency Check including FBI fingerprint check, conducted by a U. S. Governmental agency pursuant to Executive Order 10450, may be accepted as the equivalent of a National Agency Check, as defined in Section VII.

   d. Full field investigation conducted pursuant to Executive Order 10450 by a U. S. Governmental agency may be accepted provided it is determined upon review of the investigative report that it meets the standards prescribed in Section VIII for a Background Investigation.

2. Where a Background Investigation of a civilian employee is required under the provisions of this Directive, the National Agency Check component of the Background Investigation will not be duplicated if it is determined that a U. S. Governmental agency is conducting or has completed a National Agency Check.

C. Reports of Investigation to the Civil Service Commission

In order to comply with Section 9(b) of Executive Order 10450, when the investigative agencies of the Department of Defense conduct Background Investigations on civilian employees for

personnel security purposes, the investigative agency will prepare Civil Service Commission Standard Form 79 and will submit it to the Civil Service Commission on the same day the investigation is initiated.

XI. RECORD OF INVESTIGATION AND CLEARANCE

Final and interim security clearances granted must be made a matter of record and made a permanent part of the individual's personnel file or other appropriate record so as to avoid duplication of investigations and clearances. Records should reflect the date of investigation; the type of investigation conducted; the agency which conducted the investigation; the location of the investigative file; the date clearance was granted; the name of the authorized person granting clearance; and the degree of access to which the individual is authorized.

XII. DELEGATION OF AUTHORITY

A. The Secretary of the Army, the Secretary of the Navy, the Secretary of the Air Force, and the Chairman, Joint Chiefs of Staff are authorized to clear personnel within their specific areas of jurisdiction for access to classified defense information. Authority may be delegated within each area of specific jurisdiction, but the persons holding the above-named positions shall be responsible in all cases within their respective jurisdiction and shall not by virtue of said delegation be relieved of their responsibility under this paragraph.

B. Where such authority has been delegated, the person so authorized to grant clearances to others must himself have been appropriately cleared for access to Top Secret defense information.

C. The Assistant Secretary of Defense (Manpower and Personnel) will promulgate procedures implementing this Directive within the Office of the Secretary of Defense (except the Joint Chiefs of Staff).

XIII. RECIPROCAL ACCEPTANCE OF PREVIOUS INVESTIGATIONS AND CLEARANCES

A. It is highly desirable that responsible authorities within the Armed Services and other agencies of the Department of Defense accept from each other on a mutual and reciprocal basis (1) the results of previous investigations and (2) previous clearances which have been granted by appropriate authority provided the previous clearances have been based on investigative requirements consonant with present standards. Such reciprocation will avoid the repetitious filing of personal history statements, the time and expense of multiple investigations and multiple clearances. However, this applies only where a prior investigation by an investigative agency

of the government meets the standards prescribed herein. If the prior investigation does not meet such standards, supplemental or additional investigation shall be conducted.

B. It is understood, however, that the prior clearance of an individual by an appropriate authority of one Service or agency will not be considered binding on another Service or agency. Except as otherwise provided in Section XII immediately preceding, the ultimate authority to grant clearance in any case will rest with the head of the Service or agency who is responsible for the security of the information or material to which the individual in question may be granted access. This ultimate authority will include the right to review the investigative and personnel files pertaining to the case in question and, if deemed necessary, to request additional investigation before granting a clearance.

C. Whenever it becomes necessary for one Service or agency to grant a clearance to a member of another Service who has not been previously investigated, the necessary investigation will be conducted by the parent Service of the individual requiring access to the classified defense information. The using Service or agency will grant or deny the clearance and will notify the parent Service as to the action taken in order that the appropriate entry may be made in permanent personnel and security records of the individual concerned.

XIV. ACCESS TO RESTRICTED DATA

Access to Restricted Data as defined in the Atomic Energy Act of 1954 (Public Law 703, 83rd Congress) bearing the classification Top Secret, Secret, and Confidential, will be governed by the clearance procedures prescribed for Top Secret, Secret, and Confidential defense information as set forth in this Directive.

XV. CRYPTOGRAPHIC CLEARANCES

A. While Background Investigations, National Agency Checks, and clearances for other duties may contribute to cryptographic clearances and warrant due consideration, they do not, per se, constitute clearance for cryptographic material and information. Evaluation of eligibility for access to cryptographic material and information is the responsibility of the person to whom this authority has been delegated under the provisions of Section XII. This evaluation is based upon the results of

investigation, and knowledge of the individual's qualifications obtained either through interview by competent personnel or from prior knowledge of these qualifications. The person authorized to grant cryptographic clearances shall revoke such clearance of any person under his jurisdiction who for any reason appears no longer eligible to handle cryptographic material and information.

B. In order for a person to be eligible for a clearance for access to cryptographic material and information pertaining to the cryptographic systems of the United States, he shall:

1. Be of excellent character and discretion and of unquestioned loyalty to the United States. There shall be no exception to this requirement.

2. Be a citizen of the United States; preferably by birth. If he is a citizen by naturalization, final papers must have been held for a ten-year period. The members of his immediate family should also be U. S. citizens.

3. Be a person no member of whose immediate family nor any person to whom he may reasonably be considered to be bound by ties of affection, kinship, or obligation shall be of dubious loyalty to the United States nor a resident of a foreign country having basic or critical national interests opposed to those of the United States.

4. Be investigated in accordance with the provisions of Section IX.A.1. above.

C. Whenever practicable, cryptographic duties shall be performed by carefully selected military personnel. When there are insufficient military personnel, civilians cleared in accordance with the criteria of Paragraph B above may perform cryptographic duties under the supervision of commissioned officers.

D. Exception to any of the foregoing requirements except for Paragraph B.1 may be made only after every reasonable assurance has been obtained that, in the circumstance, the security risk involved is negligible. In cases where exception to the provisions of Paragraph B.4 are deemed necessary, the provisions of Section IX.A.4 shall apply.

E. No cryptographic clearance is required for personnel to have access to certain types of material which have been designated by the National Security Agency as non-critical from the security viewpoint. Examples of such material are authentication systems, operation codes, call sign ciphers, and similar

systems, which are normally used in forward tactical echelons, in aircraft, or in small surface craft. The fact that no cryptographic clearance is required does not obviate the necessity of appropriate investigation and selection of personnel authorized to handle the classified information which may be encrypted in these cryptosystems.

F. The authority for evaluation of eligibility for access to cryptographic material and information is final and is invested entirely within the Military Departments and the Office of the Secretary of Defense.

XVI. COMBAT OPERATIONS

Under combat conditions or other military exigencies, competent authority may waive such provisions of this Directive as is warranted in the circumstances.

XVII. IMPLEMENTATION

A. All directives, regulations, manuals, letters, bulletins, circulars, or memoranda published or issued by the Services and agencies concerned pertaining to this subject, which stipulate policies or procedures not consistent or in accord with these specified herein, will be rescinded, amended, or republished to conform with the provisions of this Directive.

B. It is requested that copies of implementing directives be furnished this office.

XVIII. EFFECTIVE DATE

This Directive is effective immediately and shall be implemented by the Military Departments at the earliest practicable date within ninety days from the date hereof.

Secretary of Defense

E

July 8, 1957
NUMBER 5200.1

ASD(M)

Department of Defense Directive

SUBJECT: Safeguarding Official Information in the Interests of the Defense of the United States

Ref: (a) Department of Defense Directive 5200.1, subject: Safeguarding Official Information in the Interest of the Defense of the United States, dated 19 November 1953. (Cancelled herein)

(b) Department of Defense Directive 5200.2, subject: Classification of Aerial Photography, dated 5 November 1951. (Cancelled herein)

(c) Department of Defense Directive 5200.3, subject: Department of Defense Policy for Assignment of Classification Categories to Official Defense Information, dated 21 December 1953, as amended by ASD (M&P) Memo, Subject: Classification of Compiled Data, dated 4 May 1954, and as further amended on 9 April 1957. (Cancelled herein)

(d) Department of Defense Directive 5200.4, subject: Department of Defense Policy and Procedure Governing Use of Code Words, dated 16 April 1954. (Cancelled herein)

(e) Department of Defense Directive 5200.7, subject: Policy Governing the Transmission and Safe Keeping of Defense Information Classified "Confidential - Modified Handling Authorized", dated 15 July 1954. (Cancelled herein)

(f) Department of Defense Directive 5210.1, subject: Photographing or Sketching Vital Installations or Equipment During FBI Investigations, dated 12 March 1952. (Cancelled herein)

(g) Department of Defense Directive 5210.6, subject: Control of Classified Documents within the Department of Defense, dated 6 December 1953. (Cancelled herein)

(h) Secretary of Defense Memorandum dated 4 May 1950, subject: Classification of Maps, Charts, Aeronautical Publications and Other Documents Pertaining to Military Installations. (Cancelled herein)

(i) Secretary of Defense Memorandum dated 29 October 1952, subject: Unwarranted Dissemination of Classified Material. (Cancelled herein)

(j) Secretary of Defense Memorandum dated 26 March 1953, subject: Improvement of Security Procedures Within the Department of Defense. (Cancelled herein)

(k) Secretary of Defense Memorandum dated 26 March 1953, subject: Security Violations in the Department of Defense. (Cancelled herein)

(l) Secretary of Defense Memorandum dated 5 March 1954, relating to designation of those Office of Secretary of Defense officials authorized to assign the Top Secret Classification; as amended on 12 July 1954, 27 December 1954 and 7 December 1955. (Cancelled herein)

(m) Department of Defense Directive 5200.6, subject: Policy Governing the Custody, Use and Preservation of Department of Defense Official Information Which Requires Protection in the Public Interest

(n) Department of Defense Directive 5145.2, subject: Unauthorized Disclosures of Classified Defense Information

(o) Department of Defense Directive 5400.4, subject: Provision of Information to the Congress

(p) Department of Defense Directive 5210.2, subject: Access to and Dissemination of Restricted Data

#Revised Aug 17, 61

5200.1
July 8, 57 #

Encl: (1) Instructions for the Safeguarding of Classified Defense Information in the Department of Defense.

Part 1. Definitions.

Part 2. Classification of Defense Information.

Part 3. Classification of Defense Information in connection with Combat or Combat-Related Operations.

Part 4. Control of Classified Defense Information.

Part 5. Protection of Classified Information Received from International Sources.

Part 6. Security of Classified Communications Information.

Part 7. Protection of Restricted Data (Atomic Energy Information).

Part 8. Classification of Photography.

Appendix: (1) (a) Executive Order 10501

* (b) Executive Order 10816 *

(2) Department of Defense - Government Printing Office Security Agreement

(3) Audit Activities of the General Accounting Office

(4) Policy and Procedures Governing the Use of Code Words

I. PURPOSE

To implement within the Department of Defense the provisions of
* Executive Order 10501, dated 5 November 1953 and Executive Order 10816, *
* dated 7 May 1959, [See Appendix (1) of the attached Instructions]. In *
implementing this Executive Order, all concerned must recognize that it is essential that the citizens of the United States be informed concerning the activities of their Government. Accordingly, unnecessary classification and over-classification shall be scrupulously avoided. These objectives are not deemed inconsistent

#Revised November 20, 1959

with the need for protection of certain official information affecting the national defense against unauthorized disclosure in order to preserve the ability of the United States to protect and defend itself against all hostile or destructive action by covert or overt means, including espionage as well as military action. In the attainment of these objectives this directive is designed:

A. To achieve uniformity within the Department of Defense in the assignment of the classification categories Top Secret, Secret and Confidential to official defense information and in the transmission thereof by establishing standard definitions and procedures in consonance with Executive Order 10501 and Executive Order 10816.

B. To prescribe the circumstances for use of certain special markings for classified information which is not releasable to foreign nationals, or which relates to atomic energy.

C. Pursuant to authority contained in Section 14 of Executive Order 10501, to prescribe regulations for the transmission and safekeeping of defense information classified Confidential disseminated in connection with certain combat or combat-related operations, and to identify this type of information by establishing the term "Confidential - Modified Handling Authorized".

D. To insure positive control of important classified documents, particularly those in the Top Secret and Secret category.

II. CANCELLATION

The substance of reference (a) through (l) has either been included in the attached Instructions or has been superseded by revised policy. References (a) through (l) are therefore cancelled.

III. CLASSIFICATION CATEGORIES

A. As defined in Section 1 of Executive Order 10501, the only three authorized categories of classified information are Top Secret, Secret and Confidential. Certain types of Confidential defense information which pertain to combat or combat-related operations may be designated "Confidential - Modified Handling Authorized" pursuant to the authority of

#Revised November 20, 1959

Section 14 of Executive Order 10501. The Policy for the use of this term is set forth in Part 3 of the attached Instructions.

B. The term "Security Information" which was required prior to the issuance of Executive Order 10501 will not be used as an integral part of the three classification categories.

IV. PROCEDURES PERTAINING TO "RESTRICTED-SECURITY INFORMATION"

The category of "Restricted-Security Information" used prior to the issuance of Executive Order 10501 was eliminated from the classification system by that Executive Order. All Department of Defense information and material classified "Restricted-Security Information", except as provided in Parts 5 and 6 of the attached Instructions, are declassified. In those specific instances where upgrading to "Confidential" is absolutely essential to protect information affecting the national defense, the definition of "Confidential" set forth in Section 1 (c) of Executive Order 10501 will be strictly complied with. Inasmuch as material so marked may still be encountered in the review of record material this policy is continued in effect.

V. IMPLEMENTATION

All directives, regulations, manuals, letters, bulletins, circulars, or memoranda published or issued by the Services and agencies concerned pertaining to this subject, which stipulate policies or procedures not consistent with the provisions of Executive Order 10501, and its implementation herein, will be revised, amended, or republished to conform with the provisions thereof.

VI. EFFECTIVE DATE

This directive is effective immediately.

Enclosure

C. E. Wilson

Secretary of Defense

INSTRUCTIONS FOR THE SAFEGUARDING OF CLASSIFIED DEFENSE INFORMATION IN THE DEPARTMENT OF DEFENSE

Part 1. DEFINITIONS

I. For the purpose of this Directive, the following definitions apply:

A. Classification Categories: Official information which requires protection in the interests of national defense shall be limited to three categories of classification, which in descending order of importance shall carry one of the following designations: Top Secret, Secret, or Confidential (including Confidential - Modified Handling Authorized; see Part 3 of these Instructions). No other designation shall be used to classify defense information, including military information, as requiring protection in the interests of national defense, except as expressly provided by statute.

B. Classification Guide: An instruction indicating the classification that may be assigned to subjects within a specific area of Defense activity.

C. Combat or Combat-Related Operations: Combat or combat-related operations, actual or simulated, relate to military planning, operations, training, communications, intelligence and the logistical support thereof.

D. Compartmentalization (Circulation Control): The rules and regulations established by responsible authority to insure that access to classified information will be granted only to trustworthy persons who require such information in performance of their official duties and classified information is restricted to specific physical confines when feasible.

E. Document: As used herein means any recorded information regardless of its physical form or characteristics, and includes but is not limited to the following:

1. Written material whether handwritten, printed, or typed;

2. All painted, drawn or engraved material;

3. All sound or voice recordings;

4. All printed photographs and exposed or printed film, still or moving; and

5. All reproductions of the foregoing by whatever process.

F. Formerly Restricted Data: Atomic Energy information that has been removed from the Restricted Data category for military use that can be protected as defense information, but that cannot be released to any nation or regional defense organization except as provided under Section 142d, Atomic Energy Act, 1954, as amended.

G. Material: As used herein means any document, product or substance on or in which information may be recorded or embodied.

H. Munitions of War: Any and all items required for war inclusive of food as well as all other supplies and equipment, but exclusive of manpower, are classed as munitions of war.

I. Original Classification Authority: Original classification authority is that authority required to classify independently any type of material; this contrasts with derivative classification authority, which is the authority to classify material created as a result of, in connection with, or in response to other material dealing with the same subject which already bears a classification.

J. Restricted Data (Atomic Information): Pursuant to the provisions of the Atomic Energy Act of 1954, as amended, the term "Restricted Data" is defined as all data concerning (1) design, manufacture or utilization of atomic weapons; (2) the production of special nuclear material; or

(3) the use of special nuclear material in production of energy, but shall not include data declassified or removed from the Restricted Data category which the Atomic Energy Commission from time to time determines may be published without undue risk to the common defense and security.

K. Technical Information: That which applies to data concerning munitions and equipment, engineering performance, instructions on maintenance and operation and any descriptive matter or components thereof. This includes means of operation, manufacture, use, techniques and processes. Information pertaining to the various sciences which may be employed directly or indirectly in warfare are also so classed. Data of a strategic or tactical nature is specifically excluded from the meaning of this term.

Part 2. CLASSIFICATION OF DEFENSE INFORMATION

I. SCOPE

A. It is to be emphasized that the designations "Top Secret", "Secret", "Confidential" (including "Confidential - Modified Handling Authorized"), may only be used in safeguarding official information which requires protection in the interests of national defense. Official information not affecting the national defense, which pursuant to statutory or constitutional authority may be deemed to require protection in the public interest for other reasons, shall be handled in accordance with reference (m).

B. Nothing in this Directive shall be deemed to authorize the withholding of information, otherwise releasable, because its release might tend to reveal administrative error, or inefficiency, or might be embarrassing.

II. OVERCLASSIFICATION AND UNNECESSARY CLASSIFICATION

A. It is essential that the general public be kept informed as to the programs and policies of the Department of Defense to the maximum extent permitted by considerations of national security. To accomplish this, unnecessary classification or overclassification must be scrupulously avoided.

B. The Secretaries of the Military Departments, the Chairman, JCS, and the Administrative Assistant to the Secretary of Defense will take appropriate steps to insure that all personnel of the Department of Defense, both military and civilian, are made aware of the importance of avoiding unnecessary classification or overclassification. Responsible authorities at the time of signature or approval of any document will carefully review its content in light of the category definition of the classification affixed and in all cases in which security considerations fail to support fully this classification direct the assignment of a lower classification.

III. APPLICATION OF POLICY

A. Classification Guides

Classification guides shall be used to achieve uniformity in the application of this policy. In every practicable instance, classification guides pertaining to each area of operation, planning, technical development, or research shall be developed and maintained in current status. The examples of classification categories set forth in Section IV below shall be the basic guidance in the preparation of these guides.

B. Advance Security Planning

Advance security planning is an essential part of any plan, program, or project wherein security is a major factor. To the extent feasible, the responsible official charged with developing any broad plan, program, or project in which Top Secret or Secret material is involved will insure that arrangements for giving due consideration to security aspects are incorporated therein from the beginning. The basic study or project will include appropriate security guidance, which may be included in a special annex, covering such points as:

1. Issuance of guides for the assignment of classification categories to various portions of the project, as appropriate.

2. Requirements for specific special security control measures, including stipulations as to the special precautions to be observed and giving the maximum amount of guidance to achieve compartmentalization.

3. Planning for phased downgrading, declassification, and public release of information concerning the project when practicable.

IV. CLASSIFICATION CATEGORIES

A. Top Secret

Executive Order 10501 specifies that the use of the classification Top Secret shall be limited to defense information or material which requires the highest degree of protection. The Top Secret classification shall be applied only to that information or material the defense aspect of which is paramount, and the unauthorized disclosure of which could result in exceptionally grave damage to the Nation, such as:

1. Leading to a definite break in diplomatic relations affecting the defense of the United States, an armed attack against the United States or its Allies, a war, or

2. The compromise of military or defense plans, or intelligence operations, or scientific or technological developments vital to the national defense.

Examples of the type of material described in subparagraphs 1 and 2 above might include the following:

a. A strategic plan documenting the overall conduct of a war.

b. War planning documents which contain worldwide:

   (1) Planning data and assumptions.

   (2) Wartime planning factors for the use of nuclear weapons.

   (3) Intelligence estimates of enemy capabilities.

   (4) Force composition and deployment, and

   (5) Real estate requirements and utilization by geographical area which are time phased for a period of months.

c. An operations plan either for a single operation or a series of connected operations containing any of the factors in subparagraph b above and with sortie rates or target data.

d. A document containing any of the considerations in subparagraph b above directly related to a Top Secret war planning document, the unauthorized disclosure of which standing alone could result in actual compromise of a particular Top Secret plan. (This does not necessarily include proposed budgets, current peacetime deployment of units or munitions, or peacetime manpower and organization programs for future years. Normally such information is too general in nature to reveal Top Secret plans.)

e. Intelligence documents that contain completed intelligence of such scope that it reveals a major intelligence production effort on the part of the United States and which would permit an evaluation by unauthorized recipients of the success attained by, or the capabilities of, the United States intelligence services. (Normally, a broad and complete intelligence annex or a summary of similar importance. Not a report or a digest of reported items of information, except as covered in subparagraph f below.)

f. A plan or policy for conducting intelligence or other special operations and information revealing a particular intelligence operation or other special operation, provided that the compromise of such plan, policy, or particular operation could result in exceptionally grave damage to the Nation -- not just to individuals or groups of individuals. Intelligence operations may include certain specifically designated and controlled collection projects.

g. Critical information concerning radically new and extremely important equipment (munitions of war), such as nuclear weapons, atomic weapons stockpile data, and any other munitions of comparable importance the scientific or technological development aspects of which are vital to the national defense. (The DOD-AEC Classification Guide

distributed by the Atomic Energy Commission, applies to Restricted Data, and also indicates the proper defense classification for the same information.)

B. Secret

Executive Order 10501 specifies that the use of the classification Secret shall be limited to defense information or material the unauthorized disclosure of which could result in serious damage to the Nation, such as:

1. Jeopardizing the international relations of the United States.

2. Endangering the effectiveness of a program or policy of vital importance to the national defense.

3. Compromising important military or defense plans, scientific or technological developments important to national defense.

4. Revealing important intelligence operations.

5. Examples of the type of material described in subparagraphs 1 through 4 above might be the following:

   a. A war plan or a complete plan for a future operation of war not included under Top Secret, and documents showing the disposition of our forces the unauthorized disclosure of which, standing alone, could result in actual compromise of such Secret plans.

   b. Defense or other military plans not included under Top Secret or subparagraph a, above, including certain development and procurement plans and programs, but not necessarily including all emergency plans.

   c. Specific information which, standing alone, reveals the military capabilities or state of preparedness of the Armed Forces, but not including information the unauthorized disclosure of which could result in compromise of a Top Secret plan.

d. Information that reveals the strength of our forces engaged in hostilities; quantities or nature of their equipment; or the identity or composition of units in an active theater of operations or other geographic area where our forces are engaged in hostilities, except that mailing addresses may include organization designations. (During periods of peace, information revealing the strength, identity, composition, or location of units normally does not require classification as Secret.)

e. Intelligence and other information, the value of which depends upon concealing the fact that the United States possesses it.

f. Particulars of scientific or research projects which incorporate new technological developments or techniques having direct military application of vital importance to the national defense.

g. Specific details or data relating to new material or important modifications of material which reveal significant military advances or new technological developments having direct military application of vital importance to the national defense.

h. Communications security devices and cryptographic material that reveals information of vital importance to the national defense.

i. Information of vital importance to the national defense concerning specific quantities of war reserves.

C. Confidential

Executive Order 10501 specifies that the use of the classification Confidential shall be limited to defense information or material the unauthorized disclosure of which could be prejudicial to the defense interests of the Nation. The same limitation applies to the use of Confidential - Modified Handling Authorized as described in these Instructions. Examples of the type of material described might include the following:

1. Operational and battle reports which contain information of value to the enemy.

2. Intelligence reports.

3. Military radio frequency and call sign allocations of special significance or those which are changed frequently for security reasons.

4. Devices and material relating to communications security.

5. Information which indicates strength of our ground, air and naval forces in United States and overseas areas, identity or composition of units, or quantity of specific items of equipment pertaining thereto. (During periods of peace, a defense classification is not necessarily required, unless such information reflects the overall strength figures or quantities of weapons whose characteristics are themselves classified, or additional factors necessitate security protection.)

6. Documents and manuals containing technical information used for training, maintenance and inspection of classified munitions of war.

7. Operational and tactical doctrine.

8. Research, development, production; and procurement of munitions of war.

9. Mobilization plans.

*10. Personnel security investigations and other investigations which require protection against unauthorized disclosure.

*11. Matters and documents of a personal and disciplinary nature, the disclosure of which could be prejudicial to discipline and morale of the Armed Forces.

*12. Documents used in connection with procurement, selection and promotions of military personnel, the disclosure of which could violate the integrity of the competitive system.

/ *While in all of the above cases, the assignment of Confidential must be justified, particular care must be exercised with respect to paragraphs 10, 11 and 12 above to make certain that such matters are assigned to the Confidential category only if in fact the unauthorized disclosure of such information could be prejudicial to the defense interests of the nation. If such information is not

strictly defense information but nevertheless requires protection, it will be safeguarded by the application of the provisions of reference (m)7

D. Classification of Subject or Title

Where reference to, or the contents of, the subject or title of a classified document originating in the DOD is determined to be classified, the classification of such subject or title shall be indicated by the appropriate classification designation in parenthesis; where such reference and content is determined to be unclassified, that fact will be indicated in parenthesis. For these purposes, the initials "T.S.", "S", "C" or "U" may be used where appropriate.

E. Classification of Compilations of Defense Information

Separate sections, chapters, or similar components of documents not permanently bound may bear different classifications or not be classified. However, compilations of items of defense information shall be classified in accordance with the definitions set forth in paragraphs A, B, and C above, even though the individual classified items may separately bear a lower classification than that warranted by the aggregate.

F. Special Procedure for Safeguarding Certain Documents from Disclosure to Foreign Nationals.

1. a. Classified Defense Information

Whenever an originator or recipient of classified documents determines that information is contained therein which should be withheld from foreign nationals and the anticipated distribution, transmission or handling by the addressee will make it liable to inadvertent disclosure to foreign nationals, he will attach a special handling notice to it. The notice may be included in the document if the originator knows that the information is not releasable to any foreign government. It should read:

SPECIAL HANDLING REQUIRED
NOT RELEASABLE TO FOREIGN NATIONALS 1/

The information contained in the attached document will not be disclosed to foreign nationals without express approval of the _____ _____ (Director of Intelligence of Command concerned). Approval shall refer specifically to this document or to specific information contained therein.

1/ The abbreviated term "NOFORN" is authorized for use in lieu of the above Special Handling notice when the use of this notice is impractical.

b. Atomic Energy Information

In accordance with the provisions of subsection 142d of the Atomic Energy Act of 1954, as amended, the Atomic Energy Commission may from time to time remove from the Restricted Data category such data as the Commission and the Department of Defense jointly determine relates primarily to the military utilization of atomic weapons and which the Commission and the Department of Defense jointly determine can be adequately safeguarded as defense information. The Act also provides however, that no such data so removed from the Restricted Data category shall be transmitted or otherwise made available to any nation or regional defense organization, while such data remains defense information, except pursuant to an agreement for cooperation entered into in accordance with subsection 144b, of said Act. Therefore, information so removed from the Restricted Data category and safeguarded as defense information in addition to bearing the appropriate classification designation pursuant to this Directive, shall be marked as follows:

FORMERLY RESTRICTED DATA

(Handle as Restricted Data in Foreign Dissemination, Section 144b, Atomic Energy Act of 1954)

2. General Restrictions

Under no circumstances, however, will classified documents not having a special handling notice attached be released or disclosed to foreign nationals without proper authorization in accordance with policies prescribed within the military departments and other agencies of the Department of Defense. Special handling notices will be used solely for the purpose of indicating to holders and other handling personnel that the documents involved have already been reviewed by the office of origin or other responsible authority, and that disclosure to foreign nationals is not authorized.

Part 3. CLASSIFICATION OF DEFENSE INFORMATION IN CONNECTION WITH COMBAT OR COMBAT-RELATED OPERATIONS

I. BACKGROUND

A considerable volume of defense information classified Confidential concerns military operations related to planning, operations, training, communications, and the logistical support thereof. This information is connected with combat or combat-related operations, and requires the means for transmission and safekeeping compatible with the necessary dissemination and use required for the proper and effective accomplishment of the mission of the Department of Defense. The procedures for transmission and safekeeping of Confidential defense information as set forth in Executive Order 10501 need modification to meet the above requirement. Section 14 of the Executive Order recognizes the possible necessity for modification and authorizes the Secretary of Defense to prescribe such regulations as he may consider necessary.

II. POLICY

A. Pursuant to Section 14 of Executive Order 10501, in combat or combat-related operations, actual or simulated, the commander of the unit concerned will insure that all classified materials are given the maximum security possible under the circumstances. Classified materials will not be taken farther forward in combat areas than is absolutely necessary.

B. The provisions of Executive Order 10501 regarding the transmission and safekeeping of defense information classified Confidential are modified in accordance with the following:

1. Scope

a. Designation

Confidential defense information as described in subparagraph b below shall be identified by the term "Confidential - Modified Handling Authorized".

b. Applicability

Information so designated is that (1) which pertains to combat or combat-related operations, actual or

simulated, and (2) which will be adequately protected by the procedures for transmission and safekeeping set forth in subparagraph 2, below. Examples of such information might include the following:

(1) Training, Field and Technical Manuals and related material.

(2) Photographs, negatives, photostats, diagrams or material.

(3) Defense procurement plans, including procurement contracts and related matters.

(4) Communications material and messages.

(5) Certain documents regarding engineering plans and design details, computation, method of processing or assembling, which are essential to the functioning or use of an article of material.

(6) Military maps and aerial photography, and related material, which require wide dissemination for military purposes.

(7) Information received from foreign nations under existing international exchange of information agreements and policies, and classified "Restricted" by them.

2. Procedures

a. Transmission (E.O. 10501, Sec 8(d) modified accordingly)

Documents and material designated Confidential - Modified Handling Authorized will normally be transmitted by ordinary mail within the United States, but without precluding a more secure means if desired. Outside the Continental United States, Confidential - Modified Handling Authorized defense material will be

transmitted by ordinary first class mail which is under the control of the United States and Canadian governments, or transmitted by unaccompanied State Department air or surface pouch under diplomatic seal. Such documents and material will be securely sealed, enclosed, or wrapped in a manner and with such materials as will insure arrival at destination in good condition. Wrappings or envelopes will bear no markings indicative of the classification or identification of its contents. The above does not preclude a more secure means if desired.

b. Safekeeping (E.O. 10501, Sec 6(b) modified accordingly)

Documents and material designated Confidential - Modified Handling Authorized will normally be stored in the same manner as other Confidential material. When this is not feasible, such documents and material will be stored in a container equipped with a reasonable secure locking device or in any other manner determined by proper authority which will afford adequate protection. This does not preclude a more secure means of storage if desired.

Part 4. CONTROL OF CLASSIFIED DEFENSE INFORMATION

I. POLICY

A. Responsibility

The loss of control over highly classified planning and operational documents can prevent a clear determination of the degree of security being obtained or of the extent of possible compromise of classified plans and intentions. The conditions contributing mostly to this possible loss of control appears to be (1) over-classification, (2) too wide dissemination, and (3) loss of accountability. To prevent such conditions the Secretaries of the Military Departments and heads of other Department of Defense activities shall prescribe in affirmative and unequivocal language to all personnel under their jurisdiction the mandatory requirements of this directive as it applies to

1. Rules for proper classification,

2. Necessity for declassification and downgrading, as appropriate,

3. Dissemination, and

4. Safekeeping

B. Disciplinary Action

1. Particular emphasis shall be placed upon the consequences of unauthorized disclosure of classified information. Instructions shall provide for continuity of investigative jurisdiction and review pursuant to reference (n) to insure prompt and appropriate disciplinary action regardless of rank or position. Even where it is impossible to identify the specific individual source of an unauthorized disclosure of classified information, disciplinary action is not necessarily precluded. Where the source can be traced to a specific command or office, the commander or official in charge shall be held responsible for any derelictions or ineffectiveness in the discharge of his responsibilities in such manner as may be warranted in the circumstances.

2. Similar emphasis shall be placed on the necessity of preventing overclassification and to adherence to departmental policies on review of classified material for downgrading and declassification.

II. PROCEDURES

A. Authority to Classify

1. Except as stated herein, original classification authority for assignment of the Top Secret classification may not be delegated, and shall be limited to:

   a. The Secretary and Deputy Secretary of Defense.

   b. The Secretaries, Under Secretaries and Assistant Secretaries of the Military Departments.

   c. The Chairman and Members of Joint Chiefs of Staff (including the Commandant of the Marine Corps) and the directors of its subordinate agencies including the commanders of unified and specified commands, and the Chief, Defense Atomic Support Agency, his deputies and commanders of DASA commands or facilities. *

   d. The Director of Defense Research and Engineering, the Assistant Secretaries of Defense and the General Counsel, OSD. *

   e. The Assistants to the Secretary of Defense and the Chairman, Military Liaison Committee and the Chairman, Military-Civilian Liaison Committee. *

   f. The Director, Advanced Research Projects Agency and the Directors of Research and Development Programs, including the Chiefs of the Technical Services or Bureaus, as designated by the Service Secretaries concerned, by the Director of Defense Research and Engineering, or by the Director, Advanced Research Projects Agency. *

   g. The Chiefs of the Military Services and the Chiefs of their Headquarters Staff elements responsible for the development of strategic and operational plans that meet the requirements for Top Secret classification, as designated by the Secretary concerned.

#Revised November 20, 1959

h. The Commanders of major field and fleet commands or forces (including the Commandant of the Coast Guard when acting as part of the Navy, the Commanders of Naval Sea Frontiers and Commandants of Naval Districts) as designated by the Service Secretary concerned.

i. The Director, National Security Agency, the Chiefs of the Military Service elements under his operational control, and the Chiefs of the NSA staff elements.

2. Derivative classification authority for assignment of Top Secret classification shall be granted by those officials designated in paragraph 1 above to subordinate commanders or heads of subordinate echelons only in those instances where the use of the Top Secret classification is required to respond to a communication that necessitates a Top Secret response.

3. The original classification authority for assignment of the Secret classification shall, in addition to those officials designated in paragraph 1 above, be limited to:

a. Directors or chiefs of headquarters staff divisions of the military departments, major field commanders and heads of their staff sections, and commanders of major subordinate elements designated by the major field commanders.

b. Directors of Offices in the Office of the Secretary of Defense and of Offices under the jurisdiction of the Secretaries of the Military Departments.

c. Chiefs of technical Services or Bureaus and designated heads of their major headquarters staff sections.

d. Heads of independent agencies not falling within the scope of a through c above, as designated by the Secretary concerned.

e. Commanders of major subordinate elements of and heads of the staff sections within the headquarters of the unified and specified commands.

In designating subordinate echelons, such designations will be limited to those persons whose functional requirements clearly demonstrate a real necessity for them to exercise original classification authority for Secret.

4. The original classification authority for assignment of the Confidential classification, including Confidential - Modified Handling Authorized may be delegated by those

#Revised November 20, 1959

officials designated in subparagraphs 1 and 3 above, who will limit the exercise of this authority as severely as is consistent with the orderly and expeditious transaction of official business.

B. Preparation

At the time of issuance (signature) of any document which qualifies for assignment to the Top Secret or Secret category, the signature authority will insure:

1. That all preliminary drafts, stenographic notes and working papers used during the preparation of the document, which are not required for retention, are destroyed in accordance with appropriate regulations.

2. That all formal papers of a classified nature relating to the coordination of the document or other aspects of its preparation which require retention are itemized, assembled into a single file, and forwarded for custody to the official files of the preparing agency.

C. Reproduction

At the time of issuance (signature) of any document which qualifies for assignment to the Top Secret category, the signature authority will insure that each copy of the document is serially numbered for accounting purposes and contains a notation, substantially in one of the following forms:

1. Reproduction of this document in whole or in part is prohibited except with permission of the issuing office, or higher authority.

2. Reproduction of paragraph(s)____ of this document is prohibited except with permission of the issuing office, or higher authority.

D. Accountability

In addition to the maintenance of Top Secret control ledgers and classified document logs within offices, each originator or holder of a Top Secret document will keep a record, by

document title, name and date, of all individuals, including stenographic and clerical personnel, who are afforded access to information contained in the document. Upon dispatch or transfer of the document from control of an office, these records will be filed locally for a period of one year, or such longer period as deemed necessary by appropriate authority. Accountability of Secret and Confidential documents will be maintained in such manner as prescribed by the Secretaries of the Military Departments, Chairman, JCS, and the Administrative Assistant to the Secretary of Defense. *

E. Exception of National Security Agency

In lieu of the requirements of Sections II.C. and II.D. above, * the Director, National Security Agency, shall prescribe, for * the internal handling of material under his special cognizance, * such special procedures as may be necessary to conform to poli- * cies and standards prescribed for NSA by higher authority out- * side the Department of Defense. With respect to material not * within the special cognizance of the Director, NSA, the provi- * sions of the Directive shall control the transmission of material * between NSA and other agencies which come within the purview of * Executive Order 10501. *

III. DISSEMINATION

A. General

1. The dissemination of classified defense information will be limited strictly to those persons whose official duties require knowledge or possession thereof. Responsibility for determining whether a person's official duties require that he possess or have access to any element or item of classified defense information and whether he is authorized to receive it rests upon each individual who has possession, knowledge, or command control of the information involved and not upon the prospective recipient. These principles are equally applicable if the prospective recipient is an organizational entity, including commands, other Federal Agencies, a foreign government, or an individual.

2. Properly classified Top Secret information, whenever severable from lower classified portion, will be accorded separate distribution on a considerably more selective and limited basis than the balance of the document.

3. All individuals having knowledge of Department of Defense information classified as Top Secret will be identifiable at all times. If dissemination is approved to activities outside the Department of Defense or to a foreign government, the recipients of Top Secret documents will be similarly identifiable. In addition, the office of issuance of the Top Secret document will be informed of this outside dissemination.

* #Revised November 20, 1959

4. Debriefing of civilians leaving Department of Defense employment, or leaving the employment of Department of Defense contractors having classified contracts, must incorporate positive instructions against unlawful disclosures of classified information. Similar positive procedures are required in the cases of military personnel retiring and separating from the Service.

B. To Congress

Dissemination of classified defense information to Congress, its committees, members, and staff representatives shall be in accordance with reference (o).

C. To the Government Printing Office

In order to efficiently utilize the most appropriate government facilities for large scale reproduction of Department of Defense printed materials, arrangements have been made with the Government Printing Office whereby material of all classifications may be processed by that facility. The specific conditions under which classified defense information is disseminated to the Government Printing Office are set forth in the Department of Defense-Government Printing Office Security Agreement, Appendix (2).

D. To Representatives of the General Accounting Office

Representatives of the General Accounting Office shall be granted access to classified defense information originated by and in possession of organizations of the Department of Defense when such information is relevant to the performance of the statutory responsibilities of that office as outlined in Department of Defense Directive 7650.1.

1. Certification of the Degree of Security Clearance Granted and the basis for such Clearance by One of the Officials Listed in Appendix (3).

Officials of the General Accounting Office as designated in Appendix 3, are authorized to certify security clearances of General Accounting Office representatives. Certifications will be made by these officials pursuant to arrangements with the Department of Defense and the military department concerned. The General Accounting Office has adopted Department of Defense standards for granting personnel security clearances.

#Revised November 20, 1959

2. Identification of General Accounting Office Personnel by Credential Cards or Personal Recognition.

The official credential cards issued by the General Accounting Office to its personnel are acceptable for identification purposes.

3. Additional Safeguards

a. The Comptroller General has agreed to hold each individual of the General Accounting Office to whom classified information is disclosed personally responsible for its proper safeguarding.

b. The Comptroller General has agreed to establish a system for insuring the proper safeguarding of classified matter received, at least equal to that prescribed in Executive Order 10501, and has agreed to obtain prior approval from the cognizant military department or other Department of Defense agency having cognizance in the matter under consideration before dissemination outside the General Accounting Office.

E. To Historians

Access to classified defense information which is sought by persons outside the executive branch in connection with bona-fide historical research projects may be permitted by the head of the military department and other DOD agencies concerned in accordance with the provisions of Section 15, Executive Order 10501, as amended by paragraph 2, Executive Order 10816, provided that such access is clearly consistent with the interests of national defense. (See sections a and b of Appendix 1, Enclosure 1, of this Directive for the full texts of Executive Order 10501 and Executive Order 10816.)

IV. TRANSMISSION

Preparation of classified defense material for transmission, and the transmission thereof, shall be accomplished in accordance with the provisions of and subject to the limitations prescribed by Section 8, Executive Order 10501, as amended by paragraph 3, Executive Order 10816. Any and all of the means authorized within each classification category shall be utilized for transmitting classified material, except that first-class mail shall not be used for the transmittal of Confidential information. The means selected shall be based upon the sensitivity of the information within the particular classification category. (In this connection, see: (1) Section II B (2), Part 3 of Enclosure 1 for transmission of information classified Confidential - Modified Handling Authorized; (2) Section I, Part 5 of Enclosure 1 for protection of information received from international sources; and (3) Section 1, Part 6 of Enclosure 1 for security of classified communications information).

Part 5. PROTECTION OF INFORMATION RECEIVED FROM INTERNATIONAL SOURCES

I. GENERAL PROCEDURES

Section 3(e) of Executive Order 10501 requires that defense information of a classified nature furnished to the U.S. by a foreign government or international organization shall be assigned a classification which will assure a degree of protection equivalent to or greater than that required by the government or international organization which furnished the information. The detailed procedures for the protection of information received from international sources are set forth in other directives relating to the specific source of the information concerned.

II. USE OF "CONFIDENTIAL-MODIFIED HANDLING AUTHORIZED"

Information received from NATO, SEATO, or the Bahgdad Pact Organization or friendly foreign nations and classified "Restricted" by them shall be designated Confidential-Modified Handling Authorized in accordance with Part 3 of these Instructions.

Part 6. SECURITY OF CLASSIFIED COMMUNICATIONS INFORMATION

I. GENERAL POLICY

Classified communications information shall be safeguarded in accordance with the provisions of other directives relating to specific measures beyond that required for routine protection of classified material.

II. CRYPTOGRAPHIC SECURITY OF "RESTRICTED-SECURITY INFORMATION"

In order to preserve and maintain cryptographic security as required by Title 18, U.S.C., Section 798, as added by Subsection 24(a) Act of 31 October 1951 (65 Stat. 719).

A. All material directly related to cryptographic systems which was previously classified Restricted-Security Information is upgraded to Confidential. In this regard, where the provisions of Part 3 of these Instructions qualify, the term "Confidential-Modified Handling Authorized" may be used.

B. All messages previously classified Restricted-Security Information are upgraded to Confidential or Confidential-Modified Handling Authorized. Such messages shall be reviewed and, where possible, shall be declassified after appropriate processing.

III. CODE WORDS

A. In order to insure maximum security concerning intentions and to safeguard information pertaining to classified military plans or operations, certain words selected from those listed in JANAP 299 may be given a classified meaning by proper authority.

B. The instructions contained in Appendix (4) regarding the use of code words will be the policy applicable within the Department of Defense.

Part 7. PROTECTION OF RESTRICTED DATA (ATOMIC ENERGY INFORMATION)

I. SAFEGUARDING

The Department of Defense and the Atomic Energy Commission have mutually agreed that:

A. The Department of Defense will assume responsibility for the safeguarding of Restricted Data in accordance with the requirements of E. O. 10501 and the Atomic Energy Act of 1954, as amended, and for further dissemination of it to employees of the Department and its contractor organizations after it has been initially furnished to them.

B. The Department of Defense will assume responsibility for insuring that Restricted Data made available pursuant to regulations implementing the provisions of Section 143, Atomic Energy Act of 1954, as amended, will not be disseminated outside of the Department and its contractor organizations as set forth in the Armed Forces Industrial Security Regulation except to persons cleared by the Atomic Energy Commission, or to any nations or regional defense organizations except pursuant to agreements for cooperation, entered into in accordance with the Atomic Energy Act of 1954.

II. DISSEMINATION OF RESTRICTED DATA BY DEPARTMENT OF DEFENSE

A. The procedures, regulations and eligibility requirements relating to the dissemination of Restricted Data are set forth in reference (p).

B. It should be noted that while classified atomic information may be removed from the Restricted Data category, unless declassified upon removal therefrom, it must still be protected as classified defense information, and specially marked and restricted in its dissemination in accordance with Part 2, Section IV, F, 1, b of these Instructions. Such information relates primarily to the military utilization of atomic weapons and can be identified by reference to current AEC-DOD Classification Guides.

Part 8. CLASSIFICATION OF PHOTOGRAPHY

I. CLASSIFICATION OF AERIAL PHOTOGRAPHY

A. Scope

1. As used herein, aerial photography is divided into three types:

   a. Photography of the United States, its territories and possessions.

   b. Photography of leased bases, U. S. controlled bases, and occupied territory.

   c. Photography of other foreign areas.

2. Photography which is considered to be "intelligence information" will be classified in accordance with the general requirement for protecting such information and the means of acquisition thereof.

B. Policy

1. Except as provided in subparagraph 2 below only those aerial photographs of the type described in A 1 a which reveal classified features of military equipment or any other classified object or item or activities requiring security protection, will be classified. In adopting this policy, consideration has been given to the lack of ability to control aerial photography of areas because of commercial and civilian flying, the requirement by nonmilitary agencies and individuals for much of the photography now classified, and the fact that protection is sought primarily for activities conducted upon or in areas rather than for the areas themselves. Photographs requiring classification under the provisions of this policy will be assigned the least restrictive classification consistent with the proper protection of the information revealed.

2. Aerial photographs of the type described in A 1 a may be classified by the Military Department having

jurisdiction whenever the photography warrants security protection. For this purpose, each Military Department will determine and specify those areas of interest within which it will require security review. Aerial photography made within areas so specified will be submitted to the Service concerned, and will be reviewed and classified according to content as provided for in 1 above. Pending review and final classification by the Service concerned, all photographs taken in the area will bear an interim classification to be assigned by the Department designating the area as one requiring review.

3. Aerial photographs of the type described in A 1 b will be classified by the Department responsible for its procurement, only as indicated below:

   a. As provided for in 1 and 2 above.

   b. When a governmental agreement under which such photography is procured requires security protection of the product thereof.

   c. When it is necessary to protect the source of the photography or to protect the fact that the photography exists and is in the possession of the United States.

4. Aerial photographs of the type described in A 1 c above will be classified as indicated below:

   a. When a governmental agreement under which such photography is procured requires security protection of the product thereof, or

   b. When it is necessary to protect the source of the photography or to protect the fact that the photography exists and is in possession of the United States.

   c. Photography of foreign territory taken during war time shall be considered as intelligence information.

5. The determination of the extent of control necessary to maintain the security sought by the classification of aerial photography within areas, as described in subparagraphs 2 and 3 a above, shall rest with the Department concerned. In making its determination, the Department shall consider the following factors:

   a. The existence of Legislative Acts, Executive Orders or Department of Defense Directives prohibiting photography of the area concerned.

   b. All other means of effecting control over aerial photography of the area, and the desirability of employing such means, including, but not limited to,

      (1) Concealment

      (2) Notice to public regarding prohibited areas

      (3) Coordinated military defense of the area.

   c. The ability of a potential enemy to obtain from other sources the information sought to be protected by the imposition of classification.

6. Whenever classification is imposed on aerial photography within Areas as provided in 2 and 3 a above, the Chief of Staff, U.S. Air Force will be furnished a description of the areas and the interim classification assigned, for inclusion in the consolidated map and list provided for in paragraph F below.

C. Authority to Classify.

Authority to classify aerial photography lies with the Department having primary interest in the information revealed in the photographs, coordinating, as necessary, with any other Department having an interest therein. The authority to classify aerial photography may be delegated, as desired by the Departments. Regrading or declassification may be accomplished only by the U. S. Agency or Military Department responsible for its original classification, or higher authority.

D. Classification

Except for photography classified in accordance with governmental agreements or as prescribed in paragraph A 2 above and in paragraph H below, the degree of classification assigned to any aerial photography requiring security protection will be in accordance with policy prescribed herein and the current Department of Defense definitions of security classification categories.

E. Use of Concealment

It is considered that more effective protection can be afforded activities or material which require protection by means of concealment in addition to the application of security classification as prescribed in this policy. Therefore, Departments concerned will take all steps necessary and practical to insure the maximum concealment from aerial observation of those activities and material which should be protected.

F. Map and List of Classified Areas

1. The Department of the Air Force will maintain a consolidated list and map for the information and guidance of departments and agencies concerned showing approved areas requiring security review of aerial photography furnished in accordance with paragraph B 6 above, and classified areas referred to in paragraph H below.

2. Revision to such consolidated list and map will be published by the Chief of Staff, U.S. Air Force, as changes are made therein.

G. Aerial Photography of Installations or Areas Under the Control of Other U.S. Governmental Agencies

Aerial photography of the installations or areas under the control of other U.S. governmental agencies CLASSIFICATION OF WHICH IS REQUIRED BY THE AGENCY HAVING JURISDICTION, will be classified in accordance with the classification designated by such agency. Downgrading or declassification, as warranted, may be accomplished only after approval of the agency responsible for the installation or area. A list of all such areas or installations, the exact area covered, agency responsible, and, when

appropriate, classification of photography of such areas will be included in the consolidated list provided in paragraph F above.

II. PHOTOGRAPHING OR SKETCHING VITAL INSTALLATIONS OR EQUIPMENT DURING FBI INVESTIGATIONS

A. Background

1. Section 795 of Title 18, United States Code, provides that photographs or sketches of vital military and naval installations or equipment shall not be made except with the express permission of the Commanding Officer or higher authority. Executive Order 10104, issued by the President on 1 February 1950 defines certain vital military and naval installations and equipment as requiring protection against the general dissemination of information relative thereto.

2. It is possible that occasions could arise wherein the urgency or particular factors of an FBI investigation, which urgency or factors could not be previously anticipated, prevents the obtaining of the authority and permission contemplated by Section 795 or Title 18, United States Code.

B. Policy

Where the urgency or particular factors of an FBI investigation, which urgency or factors could not be previously anticipated, prevents the obtaining of the authority and permission contemplated by Section 795 of Title 18, United States Code, such photographs or sketches of vital military and naval installations and equipment as are required for that investigation may be made by the FBI Agents involved in such investigations. Such photographs and sketches must, however, be submitted at the earliest appropriate time to the Commanding Officer or higher authority for review in accordance with Section 795 of Title 18, United States Code.

EXECUTIVE ORDER No. 10501

NOVEMBER 5, 1953

SAFEGUARDING OFFICIAL INFORMATION IN THE INTERESTS OF THE DEFENSE OF THE UNITED STATES

APPENDIX 1

EXECUTIVE ORDER No. 10501
NOVEMBER 5, 1953
SAFEGUARDING OFFICIAL INFORMATION IN THE INTERESTS OF THE DEFENSE OF THE UNITED STATES

WHEREAS it is essential that the citizens of the United States be informed concerning the activities of their government; and

WHEREAS the interests of national defense require the preservation of the ability of the United States to protect and defend itself against all hostile or destructive action by covert or overt means, including espionage as well as military action; and

WHEREAS it is essential that certain official information affecting the national defense be protected uniformly against unauthorized disclosure:

NOW, THEREFORE, by virtue of the authority vested in me by the Constitution and statutes, and as President of the United States, and deeming such action necessary in the best interests of the national security, it is hereby ordered as follows:

Section 1. CLASSIFICATION CATEGORIES

Official information which requires protection in the interests of national defense shall be limited to three categories of classification, which in descending order of importance shall carry one of the following designations: Top Secret, Secret, or Confidential. No other designation shall be used to classify defense information, including military information, as requiring protection in the interests of national defense, except as expressly provided by statute. These categories are defined as follows:

(a) Top Secret: Except as may be expressly provided by statute, the use of the classification Top Secret shall be authorized, by appropriate authority, only for defense information or material which requires the highest degree of protection. The Top Secret classification shall be applied only to that information or material the defense aspect of which is paramount, and the unauthorized disclosure of which could result in exceptionally grave damage to the Nation such as leading to a definite break in diplomatic relations affecting the defense of the United States, an armed attack against the United States or its allies, a war, or the compromise of military or defense plans, or intelligence operations, or scientific or technological developments vital to the national defense.

(b) Secret: Except as may be expressly provided by statute, the use of the classification Secret shall be authorized, by appropriate authority, only for defense information or material the unauthorized disclosure of which could result in serious damage to the Nation, such as by jeopardizing the international relations of the United States, endangering the effectiveness of a program or policy of vital importance to the national defense, or compromising important military or defense plans, scientific or technological developments important to national defense, or information revealing important intelligence operations.

(c) Confidential: Except as may be expressly provided by statute, the use of the classification Confidential shall be authorized, by appropriate authority, only for defense information or material the unauthorized disclosure of which could be prejudicial to the defense interests of the nation.

Section 2. LIMITATION OF AUTHORITY TO CLASSIFY

The authority to classify defense information or material under this order shall be limited in the departments and agencies of the executive branch as hereinafter specified. Departments and agencies subject to the specified limitations shall be designated by the President:

(a) In those departments and agencies having no direct responsibility for national defense there shall be no authority for original classification of information or material under this order.

(b) In those departments and agencies having partial but not primary responsibility for matters pertaining to national defense the authority for original classification of information or material under this order shall be exercised only by the head of the department or agency, without delegation.

(c) In those departments and agencies not affected by the provisions of subsection (a) and (b), above, the authority for original classification of information or material under this order shall be exercised only by responsible officers or employees, who shall be specifically designated for this purpose. Heads of such departments and agencies shall limit the delegation of authority to classify as severely as is consistent with the orderly and expeditious transaction of Government business.

Section 3. CLASSIFICATION

Persons designated to have authority for original classification of information or material which requires protection in the interests of national defense under this order shall be held responsible for its proper classification in accordance with the definitions of the three categories in section 1, hereof. Unnecessary classification and over-classification shall be scrupulously avoided. The following special rules shall be observed in classification of defense information or material:

(a) Documents in General: Documents shall be classified according to their own content and not necessarily according to their relationship to other documents. References to classified material which do not reveal classified defense information shall not be classified.

(b) Physically Connected Documents: The classification of a file or group of physically connected documents shall be at least as high as that of the most highly classified document therein. Documents separated from the file or group shall be handled in accordance with their individual defense classification.

(c) Multiple Classification: A document, product, or substance shall bear a classification at least as high as that of its highest classified component. The document, product, or substance shall bear only one over-all classification, notwithstanding that pages, paragraphs, sections, or components thereof bear different classifications.

(d) Transmittal Letters: A letter transmitting defense information shall be classified at least as high as its highest classified enclosure.

(e) Information Originated by a Foreign Government or Organization: Defense information of a classified nature furnished to the United States by a foreign government or international organization shall be assigned a classification which will assure a degree of protection equivalent to or greater than that required by the government or international organization which furnished the information.

Section 4. DECLASSIFICATION, DOWNGRADING, OR UPGRADING

Heads of departments or agencies originating classified material shall designate persons to be responsible for continuing review of such classified material for the purpose of declassifying or downgrading it whenever national defense considerations permit, and for receiving requests for such review from all sources. Formal procedures shall be established to provide specific means for prompt review of classified material and its declassification or downgrading in order to preserve the effectiveness and integrity of the classification system and to eliminate accumulation of classified material which no longer requires protection in the defense interest. The following special rules shall be observed with respect to changes of classification of defense material:

(a) Automatic Changes: To the fullest extent practicable, the classifying authority shall indicate on the material (except telegrams) at the time of original classification that after a specified event or date, or upon removal of classified enclosures, the material will be downgraded or declassified.

(b) Non-Automatic Changes: The persons designated to receive requests for review of classified material may downgrade or declassify such material when circumstances no longer warrant its retention in its original classification provided the consent of the appropriate classifying authority has been obtained. The downgrading or declassification of extracts from or paraphrases of classified documents shall also require the consent of the appropriate classifying authority unless the agency making such extracts knows positively that they warrant a classification lower than that of the document from which extracted, or that they are not classified.

(c) Material Officially Transferred: In the case of material transferred by or pursuant to statute or Executive order from one department or agency to another for the latter's use and as part of its official files or property, as distinguished from transfers merely for purposes of storage, the receiving department or agency shall be deemed to be the classifying authority for all purposes under this order, including declassification and downgrading.

(d) Material Not Officially Transferred: When any department or agency has in its possession any classified material which has become five years old, and it appears (1) that such material originated in an agency which has since become defunct and whose files and other property have not been officially transferred to another department or agency within the meaning of subsection (c), above, or (2) that it is impossible for the possessing department or agency to identify the originating agency, and (3) a review of the material indicates that it should be downgraded or declassified, the said possessing department or agency shall have power to declassify or downgrade such material. If it appears probable that another department or agency may have a substantial interest in whether the classification of any particular information should be maintained, the possessing department or agency shall not exercise the power conferred upon it by this subsection, except with the consent of the other department or agency, until thirty days after it has notified such other department or agency of the nature of the material and of its intention to declassify or downgrade the same. During such thirty-day period the other department or agency may, if it so desires, express its objections to declassifying or downgrading the particular material, but the power to make the ultimate decision shall reside in the possessing department or agency.

(e) Classified Telegrams: Such telegrams shall not be referred to, extracted from, paraphrased, downgraded, declassified, or disseminated, except in accordance with special regulations issued by the head of the originating department or agency. Classified telegrams transmitted over cryptographic systems shall be handled in accordance with the regulations of the transmitting department or agency.

(f) Downgrading: If the recipient of classified material believes that it has been classified too highly, he may make a request to the reviewing official who may downgrade or declassify the material after obtaining the consent of the appropriate classifying authority.

(g) Upgrading: If the recipient of unclassified material believes that it should be classified, or if the recipient of classified material believes that its classification is not sufficiently protective, it shall be safeguarded in accordance with the classification deemed appropriate and a request made to the reviewing official, who may classify the material or upgrade the classification after obtaining the consent of the appropriate classifying authority.

(h) Notification of Change in Classification: The reviewing official taking action to declassify, downgrade, or upgrade classified material shall notify all addressees to whom the material was originally transmitted.

Section 5. MARKING OF CLASSIFIED MATERIAL

After a determination of the proper defense classification to be assigned has been made in accordance with the provisions of this order, the classified material shall be marked as follows:

(a) Bound Documents: The assigned defense classification on bound documents, such as books or pamphlets, the pages of which are permanently and securely fastened together, shall be conspicuously marked or stamped on the outside of the front cover, on the title page, on the first page, on the back page and on the outside of the back cover. In each case the markings shall be applied to the top and bottom of the page or cover.

(b) Unbound Documents: The assigned defense classification on unbound documents, such as letters, memoranda, reports, telegrams, and other similar documents, the pages of which are not permanently and securely fastened together, shall be conspicuously marked or stamped at the top and bottom of each page, in such manner that the marking will be clearly visible when the pages are clipped or stapled together.

(c) Charts, Maps, and Drawings: Classified charts, maps, and drawings shall carry the defense classification marking under the legend, title block, or scale in such manner that it will be reproduced on all copies made therefrom. Such classification shall also be marked at the top and bottom in each instance.

(d) Photographs, Films and Recordings: Classified photographs, films, and recordings, and their containers, shall be conspicuously and appropriately marked with the assigned defense classification.

(e) Products or Substances: The assigned defense classification shall be conspicuously marked on classified products or substances, if possible, and on their containers, if possible, or, if the article or container cannot be marked, written notification of such classification shall be furnished to recipients of such products or substances.

(f) Reproductions: All copies of reproductions of classified material shall be appropriately marked or stamped in the same manner as the original thereof.

(g) Unclassified Material: Normally, unclassified material shall not be marked or stamped Unclassified unless it is essential to convey to a recipient of such material that it has been examined specifically with a view to imposing a defense classification and has been determined not to require such classification.

(h) Change or Removal of Classification: Whenever classified material is declassified, downgraded, or upgraded, the material shall be marked or stamped in a prominent place to reflect the change in classification, the authority for the action, the date of action, and the identity of the person or unit taking the action. In addition, the old classification marking shall be cancelled and the new classification (if any) substituted therefor. Automatic change in classification shall be indicated by the appropriate classifying authority through marking or stamping in a prominent place to reflect information specified in subsection 4 (a) hereof.

(i) Material Furnished Persons not in the Executive Branch of the Government: When classified material affecting the national defense is furnished authorized persons, in or out of Federal service, other than those in the executive branch, the following notation, in addition to the assigned classification marking, shall whenever practicable be placed on the material, on its container, or on the written notification of its assigned classification:

> "This material contains information affecting the national defense of the United States within the meaning of the espionage laws, Title 18, U.S.C., Secs. 793 and 794, the transmission or revelation of which in any manner to an unauthorized person is prohibited by law."

Use of alternative marking concerning "Restricted Data" as defined by the Atomic Energy Act is authorized when appropriate.

Section 6. CUSTODY AND SAFEKEEPING

The possession or use of classified defense information or material shall be limited to locations where facilities for secure storage or protection thereof are available by means of which unauthorized persons are prevented from gaining access thereto. Whenever such information or material is not under the personal supervision of its custodian, whether during or outside of working hours, the following physical or mechanical means shall be taken to protect it:

(a) Storage of Top Secret Material: Top Secret defense material shall be protected in storage by the most secure facilities possible. Normally it will be stored in a safe or a safe-type steel file container having a three-position, dial-type, combination lock, and being of such weight, size, construction, or installation as to minimize the possibility of surreptitious entry, physical theft, damage by fire, or tampering. The head of a department or agency may approve other storage facilities for this material which offer comparable or better protection, such as an alarmed area, a vault, a secure vault-type room, or an area under close surveillance of an armed guard.

(b) Secret and Confidential Material: These categories of defense material may be stored in a manner authorized for Top Secret material, or in metal file cabinets equipped with steel lockbar and an approved three combination dial-type padlock from which the manufacturer's identification numbers have been obliterated, or in comparably secure facilities approved by the head of the department or agency.

(c) Other Classified Material: Heads of departments and agencies shall prescribe such protective facilities as may be necessary in their departments or agencies for material originating under statutory provisions requiring protection of certain information.

(d) Changes of Lock Combinations: Combinations on locks of safekeeping equipment shall be changed, only by persons having appropriate security clearance, whenever such equipment is placed in use after procurement from the manufacturer or other sources, whenever a person knowing the combination is transferred from the office to which the equipment is assigned, or

whenever the combination has been subjected to compromise, and at least once every year. Knowledge of combinations shall be limited to the minimum number of persons necessary for operating purposes. Records of combinations shall be classified no lower than the highest category of classified defense material authorized for storage in the safekeeping equipment concerned.

(e) Custodian's Responsibilities: Custodians of classified defense material shall be responsible for providing the best possible protection and accountability for such material at all times and particularly for securely locking classified material in approved safekeeping equipment whenever it is not in use or under direct supervision of authorized employees. Custodians shall follow procedures which insure that unauthorized persons do not gain access to classified defense information or material by sight or sound, and classified information shall not be discussed with or in the presence of unauthorized persons.

(f) Telephone Conversations: Defense information classified in the three categories under the provisions of this order shall not be revealed in telephone conversations, except as may be authorized under section 8 hereof with respect to the transmission of Secret and Confidential material over certain military communications circuits.

(g) Loss or Subjection to Compromise: Any person in the executive branch who has knowledge of the loss or possible subjection to compromise of classified defense information shall promptly report the circumstances to a designated official of his agency, and the latter shall take appropriate action forthwith, including advice to the originating department or agency.

Section 7. ACCOUNTABILITY AND DISSEMINATION

Knowledge or possession of classified defense information shall be permitted only to persons whose official duties require such access in the interest of promoting national defense and only if they have been determined to be trustworthy. Proper control of dissemination of classified defense information shall be maintained at all times, including good accountability records of classified defense information documents, and severe limitation on the number of such documents originated as well as the number of copies thereof reproduced. The number of copies of classified defense information documents shall be kept to a minimum to decrease the risk of compromise of the information contained in such documents and the financial burden on the Government in protecting such documents. The following special rules shall be observed in connection with accountability for and dissemination of defense information or material:

(a) Accountability Procedures: Heads of departments and agencies shall prescribe such accountability procedures as are necessary to control effectively the dissemination of classified defense information, with particularly severe control on material classified Top Secret under this order. Top Secret Control Officers shall be designated, as required, to receive, maintain accountability registers of, and dispatch Top Secret material.

(b) Dissemination Outside the Executive Branch: Classified defense information shall not be disseminated outside the executive branch except under conditions and through channels authorized by the head of the disseminating department or agency, even though the person or agency to which dissemination of such information is proposed to be made may have been solely or partly responsible for its production.

(c) Information Originating in Another Department or Agency: Except as otherwise provided by section 102 of the National Security Act of July 26, 1947, c. 343, 61 Stat. 498, as amended, 50 U.S.C. sec. 403, classified defense information originating in another department or agency shall not be disseminated

outside the receiving department or agency without the consent of the originating department or agency. Documents and material containing defense information which are classified Top Secret or Secret shall not be reproduced without the consent of the originating department or agency.

Section 8. TRANSMISSION

For transmission outside of a department or agency, classified defense material of the three categories originated under the provisions of this order shall be prepared and transmitted as follows:

(a) Preparation for Transmission: Such material shall be enclosed in opaque inner and outer covers. The inner cover shall be a sealed wrapper or envelope plainly marked with the assigned classification and address. The outer cover shall be sealed and addressed with no indication of the classification of its contents. A receipt form shall be attached to or enclosed in the inner cover, except that Confidential material shall require a receipt only if the sender deems it necessary. The receipt form shall identify the addressor, addressee, and the document, but shall contain no classified information. It shall be signed by the proper recipient and returned to the sender.

(b) Transmitting Top Secret Material: The transmission of Top Secret material shall be effected preferably by direct contact of officials concerned, or, alternatively, by specifically designated personnel, by State Department diplomatic pouch, by a messenger-courier system especially created for that purpose, or by electric means in encrypted form; or in the case of information transmitted by the Federal Bureau of Investigation, such means of transmission may be used as are currently approved by the Director, Federal Bureau of Investigation, unless express reservation to the contrary is made in exceptional cases by the originating agency.

(c) Transmitting Secret Material: Secret material shall be transmitted within the continental United States by one of the means established for Top Secret material, by an authorized courier, by United States registered mail, or by protected commercial express, air or surface. Secret material may be transmitted outside the continental limits of the United States by one of the means established for Top Secret material, by commanders or masters of vessels of United States registry, or by United States Post Office registered mail through Army, Navy, or Air Force postal facilities, provided that the material does not at any time pass out of United States Government control and does not pass through a foreign postal system. Secret material may, however, be transmitted between United States Government and/or Canadian Government installations in continental United States, Canada, and Alaska by United States and Canadian registered mail with registered mail receipt. In an emergency, Secret material may also be transmitted over military communications circuits in accordance with regulations promulgated for such purpose by the Secretary of Defense.

(d) Transmitting Confidential Material: Confidential defense material shall be transmitted within the United States by one of the means established for higher classifications, by registered mail, or by express or freight under such specific conditions as may be prescribed by the head of the department or agency concerned. Outside the continental United States, Confidential defense material shall be transmitted in the same manner as authorized for higher classifications.

(e) Within an Agency: Preparation of classified defense material for transmission, and transmission of it, within a department or agency shall be governed by regulations, issued by the head of the department or agency, insuring a degree of security equivalent to that outlined above for transmission outside a department or agency.

Section 9. DISPOSAL AND DESTRUCTION

Documentary record material made or received by a department or agency in connection with transaction of public business and preserved as evidence of the organization, functions, policies, operations, decisions, procedures or other activities of any department or agency of the Government, or because of the informational value of the data contained therein, may be destroyed only in accordance with the act of July 7, 1943, c. 192, 57 Stat. 380, as amended, 44 U.S.C. 366-380. Non-record classified material, consisting of extra copies and duplicates including shorthand notes, preliminary drafts, used carbon paper, and other material of similar temporary nature, may be destroyed, under procedures established by the head of the department or agency which meet the following requirements, as soon as it has served its purpose:

(a) Methods of Destruction: Classified defense material shall be destroyed by burning in the presence of an appropriate official or by other methods authorized by the head of an agency provided the resulting destruction is equally complete.

(b) Records of Destruction: Appropriate accountability records maintained in the department or agency shall reflect the destruction of classified defense material.

Section 10. ORIENTATION AND INSPECTION

To promote the basic purposes of this order, heads of those departments and agencies originating or handling classified defense information shall designate experienced persons to coordinate and supervise the activities applicable to their departments or agencies under this order. Persons so designated shall maintain active training and orientation programs for employees concerned with classified defense information to impress each such employee with his individual responsibility for exercising vigilance and care in complying with the provisions of this order. Such persons shall be authorized on behalf of the heads of the departments and agencies to establish adequate and active inspection programs to the end that the provisions of this order are administered effectively.

Section 11. INTERPRETATION OF REGULATIONS BY THE ATTORNEY GENERAL

The Attorney General, upon request of the head of a department or agency or his duly designated representative, shall personnally or through authorized representatives of the Department of Justice render an interpretation of these regulations in connection with any problems arising out of their administration.

Section 12. STATUTORY REQUIREMENTS

Nothing in this order shall be construed to authorize the dissemination, handling or transmission of classified information contrary to the provisions of any statute.

Section 13. "RESTRICTED DATA" AS DEFINED IN THE ATOMIC ENERGY ACT

Nothing in this order shall supersede any requirements made by or under the Atomic Energy Act of August 1, 1946, as amended. "Restricted Data" as defined by the said act shall be handled, protected, classified, downgraded, and declassified in conformity with the provisions of the Atomic Energy Act of 1946, as amended, and the regulations of the Atomic Energy Commission.

Section 14. COMBAT OPERATIONS

The provisions of this order with regard to dissemination, transmission, or safekeeping of classified defense information or material may be so modified in

connection with combat or combat-related operations as the Secretary of Defense may by regulations prescribe.

Section 15. EXCEPTIONAL CASES

When, in an exceptional case, a person or agency not authorized to classify defense information originates information which is believed to require classification, such person or agency shall protect that information in the manner prescribed by this order for that category of classified defense information into which it is believed to fall, and shall transmit the information forthwith, under appropriate safeguards, to the department, agency, or person having both the authority to classify information and a direct official interest in the information (preferably, that department, agency, or person to which the information would be transmitted in the ordinary course of business), with a request that such department, agency, or person classify the information.

Section 16. REVIEW TO INSURE THAT INFORMATION IS NOT IMPROPERLY WITHHELD HEREUNDER

The President shall designate a member of his staff who shall receive, consider, and take action upon, suggestions or complaints from non-Governmental sources relating to the operation of this order.

Section 17. REVIEW TO INSURE SAFEGUARDING OF CLASSIFIED DEFENSE INFORMATION

The National Security Council shall conduct a continuing review of the implementation of this order to insure that classified defense information is properly safeguarded, in conformity herewith.

Section 18. REVIEW WITHIN DEPARTMENTS AND AGENCIES

The head of each department and agency shall designate a member or members of his staff who shall conduct a continuing review of the implementation of this order within the department or agency concerned to insure that no information is withheld hereunder which the people of the United States have a right to know, and to insure that classified defense information is properly safeguarded in conformity herewith.

Section 19. REVOCATION OF EXECUTIVE ORDER NO. 10290

Executive Order No. 10290 of September 24, 1951 is revoked as of the effective date of this order.

Section 20. EFFECTIVE DATE

This order shall become effective on December 15, 1953.

DWIGHT D. EISENHOWER

THE WHITE HOUSE,

November 5, 1953.

EXECUTIVE ORDER NO. 10816

May 7, 1959

AMENDMENT OF EXECUTIVE ORDER NO. 10501 of NOVEMBER 5, 1953, RELATING TO SAFEGUARDING OFFICIAL INFORMATION IN THE INTERESTS OF THE DEFENSE OF THE UNITED STATES

By virtue of the authority vested in me by the Constitution and statutes of the United States, and as President of the United States, and deeming such action necessary in the best interests of the national security, it is hereby ordered as follows:

Executive Order No. 10501 of November 5, 1953, relating to safeguarding official information in the interests of the defense of the United States, is hereby amended as follows:

1. Section 4 is amended by adding a new subparagraph at the end thereof, as follows:

"(i) Departments and agencies which do not have authority for original classification. The provisions of this section relating to the declassification of defense material shall apply to departments or agencies which do not, under the terms of this order, have authority for original classification of material, but which have formerly classified material pursuant to Executive Order No. 10290 of September 24, 1951."

2. Section 15 is amended by adding a new subparagraph at the end thereof, as follows:

"Historical Research. As an exception to the standard of access prescribed in the first sentence of section 7, but subject to all other provisions of this order, the head of an agency may permit persons outside the executive branch performing functions in connection with historical research projects to have access to classified defense information originated within his agency if he determines that: (a) access to the information will be clearly consistent with the interests of national defense, and (b) the person to be granted access is trustworthy: Provided, that the head of the agency shall take appropriate steps to assure that classified information is not published or otherwise compromised."

3. The first sentence of subparagraph (d) of section 8 is amended to read as follows:

"Confidential defense material shall be transmitted within the continental United States by one of the means established for higher classifications, by registered, certified or first-class mail, or by express or freight under such conditions as may be prescribed by the head of the department or agency concerned."

THE WHITE HOUSE
May 7, 1959

DWIGHT D. EISENHOWER

DEPARTMENT OF DEFENSE - GOVERNMENT PRINTING OFFICE

AGREEMENT

This Agreement between the Department of Defense and the Government Printing Office govems the security measures employed by the Government Printing Office, including all facilities therof, for insuring the safeguarding of classified information released to it by Department of Defense activities for reproduction.

It is essential that certain security measures be taken by the Public Printer to assure the Department of Defense that classified information released to the Government Printing Office by the Department of Defense and its activities is being safeguarded in accordance with the provisions of Executive Order 10501, "Safeguarding Official Information in the Interests of the Defense of the United States" and Executive Order 10450, "Security Requirements for Government Employment." Accordingly, the following employment practices and operating procedures for handling such classified information by the Public Printer are hereby agreed to:

SECTION I

GENERAL REQUIREMENTS

The Public Printer shall:

a. Be responsible for safeguarding all Department of Defense classified information released to him and shall determine which of his employees require possession of, or access to, the information, and shall not supply or disclose such information to any unauthorized person. No classified information shall be disseminated outside the Government Printing Office without authority of the Department of Defense activity whose information is involved;

b. Determine the trustworthiness of employees in accordance with Executive Order 10450 as amended and issue appropriate clearances prior to permitting access to classified information. Further, such employees will have access to material on a "need-to-know" basis and only to the extent of their clearances. He shall maintain a current record of all employees who have access to classified information, indicating the degree of clearance and the date clearance was granted;

c. Provide suitable physical protective measures for safeguarding classified information in accordance with Executive Order 10501. These physical security controls shall include but not be limited to receiving, handling, transmission, storage, area controls and visitor control procedures;

d. Not contract with industry for the reprodcution of Department of Defense classified information except as specifically approved by the activity whose classified information is involved; and

e. Distribute and transmit Department of Defense classified information in accordance with specific instructions provided by the activity whose information is involved.

SECTION II

INSPECTIONS

The Department of Defense, upon appropriate coordination with the Public Printer shall have the right to inspect at reasonable intervals the procedures, methods, and facilities utilized in complying with the requirements of the provisions of this Agreement.

SECTION III

PRIOR AGREEMENTS

This Agreement supersedes all other agreements, understandings and representations with respect to the safeguarding of classified information, entered into between the Public Printer and the Department of Defense (including the three military departments). This shall not include agreements, understanding and representation contained in contracts for the furnishing of supplies and services to the Department of Defense heretofore entered into between the Public Printer and activities of the Department of Defense.

SECTION IV

SECURITY COSTS

This Agreement does not obligate the Department of Defense funds, and the Department of Defense shall not be liable for any costs or claims of the Government Printing Office arising out of this Agreement or instructions issued hereunder.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement as of June 26, 1956 .

The United States of America

See notations A and B below.

BY /s/ Frederick W. Baumann, Jr.
Government Printing Office

BY /s/ Jerome D. Fenton
Department of Defense

This agreement is executed with the understanding that:

A. The first paragraph does not include our GPO-Department of State Service Office, which is under the control securitywise of the Atomic Energy Commission and the Central Intelligence Agency;

B. Section IV, "Security Costs", does not release the Department of Defense from obligations of surchages placed against each job for the special handling required of security work.

/s/ F.W.B.
June 26, 1956

LIST OF GENERAL ACCOUNTING OFFICE OFFICIALS AUTHORIZED TO CERTIFY SECURITY CLEARANCES

Accounting and Auditing Organizations

Directors
Deputy Directors
Associate Directors
Assistant Directors
Regional Managers
- Boston, Mass.
- New York, N. Y.
- Philadelphia, Pa.
- Richmond, Va.
- Atlanta, Ga.
- Detroit, Mich.
- Cleveland, Ohio
- Cincinnati, Ohio
- Chicago, Ill.
- St. Louis, Mo.
- New Orleans, La.
- St. Paul, Minn.
- Kansas City, Mo.
- Dallas, Texas
- Denver, Colo.
- Seattle, Wash.
- Portland, Ore.
- San Francisco, Calif.
- Los Angeles, Calif.

Director, European Branch
Director, Far East Branch

Other GAO Organizations

Director, Claims Division
Director, Division of Personnel (or the Acting Director in the absence of the Director)
Director, Transportation Division

#Revised Jul 9, 58

POLICY AND PROCEDURE GOVERNING USE OF CODE WORDS

1. Purpose

The purpose of these instructions is to prescribe policy and procedure concerning the use of code words within the Department of Defense.

2. Definitions

a. Code Words - A "code word" is a word selected from those listed in JANAP 299 and assigned a classified meaning by proper authority to insure maximum security concerning intentions and to safeguard information pertaining to military plans or operations classified as Confidential or higher.

b. Inactive Code Word - An "inactive code word" is a classified code word which has been placed in use but which is subsequently replaced by another code word having the same meaning.

c. Obsolete Code Word - A classified word assigned to a plan or operation which has been discontinued, or completed, and not replaced by a similar plan or operation, whenever the meaning for security reasons cannot be declassified.

d. Cancelled Code Word - A declassified code word assigned to a plan or operation which has been discontinued or completed and which no longer requires a minimum security classification of Confidential.

e. Nickname - A name consisting of two separate words, neither of which appear in JANAP 299 and neither of which will be a word similar to such words as project, exercise, operation, etc., used to designate an unclassified meaning and employed for administrative convenience, for morale or public relations purposes.

f. Using Agency - The agency to which a code word is allocated for use and which assigns to the word a classified meaning.

3. Allocation of Code Words

a. The Secretary, ~~Joint Intelligence Group,~~ * Intelligence Directorate, the Joint Staff is responsible for the allocation of code words or blocks of code words from JANAP 299 to agencies of the Department of Defense.

APPENDIX (4)

b. Agencies of the Department of Defense will request from the Secretary, ~~Joint Intelligence Group~~ Intelligence Directorate, The Joint Staff, such allocation of code words as they require. Recipient agencies may reissue code words within their organization in accordance with agency policies and procedures, subject to applicable rules set forth herein.

4. Assignment of Classified Meanings to Code Words

a. All code words placed in use within the Department of Defense will be selected from JANAP 299.

b. The agency responsible for the development of a plan or execution of an operation will be responsible for determining whether to assign a code word and a classified meaning in connection therewith.

c. Agencies contemplating making use of code words are cautioned against employing such words except to provide for maximum security on a continuing basis. Code words will be placed in use for the following purposes only:

(1) To designate a classified military plan or operation;

(2) To designate geographic locations in conjunction with plans or operations referred to in (1) above; and

(3) To conceal intentions in discussions and messages or other documents pertaining to plans, operations, or geographic locations referred to in (1) and (2) above.

d. The agency placing a code word in use will assign to that word a specific meaning classified Top Secret, Secret or Confidential, commensurate with military security requirements. Code words will not be used to cover unclassified meanings.

e. The classified meaning of a code word will be limited to information indicating the nature of a specified plan or operation or the relationship thereto of geographic locations. The assigned meaning need not in all cases be classified as high as the classification assigned to the plan or operation as a whole.

f. Code words should be selected by each using agency in such manner that the word used does not suggest the nature of its meaning.

g. A code word should not be used repeatedly for similar purposes; i.e. if the initial phase of an operation is designated "Meaning", succeeding phases should not be designated "Meaning II" and "Meaning III", but should have different code words.

h. Each agency will establish its own policies and procedures for the control and initial assignment of classified meanings to code words subject to applicable rules set forth herein.

5. Notification of Assignment and Dissemination of Code Words and Meanings

a. Upon assignment of a classified meaning to a code word, the using agency will promptly notify the Secretary, ~~Joint Intelligence Group~~ Intelligence Directorate, The Joint Staff, of the fact of assignment, indicating the word and its classification, and the dissemination required when appropriate. Similar notification will be made when any changes occur, such as the substitution of a new word for one previously placed in use. Dissemination of the code word and its meaning to other agencies of the Department of Defense will be made by the Secretary, Joint Intelligence Group, at the request of the using agency.

b. The using agency is responsible for the dissemination to activities within its jurisdiction of code words and their meanings. It is also responsible for determining the dissemination to be made to other agencies, but such dissemination will be made through the Secretary, ~~Joint Intelligence Group~~, whenever time permits. Using agencies will promptly advise the Secretary ~~Joint Intelligence Group~~, of the fact whenever it discloses directly to an organization or office of another agency a code word and the meaning thereof.

c. Each agency having a planning, administrative or operational responsibility to fulfill in connection with a classified meaning received from another agency will be responsible for disseminating the classified meaning and the related code word to activities under its jurisdiction as it deems essential, commensurate with security requirements, but will not initially furnish the meaning to any other agency without the approval of the original using agency.

d. An agency receiving a classified meaning and its related code word from another agency for information and record purposes and having no responsibility for action in connection therewith will make no internal dissemination of the meaning outside the office responsible for maintaining records of code words for the receiving agency unless authorized by the original using agency.

e. When a meaning has not been furnished an agency for a code word contained in documents or messages received, and the agency considers that it requires knowledge of the meaning, this information may be requested from the office maintaining records of code words within the agency, submitting reasons therefor.

f. When a word which has been assigned a special meaning is furnished by a governmental agency outside the Department of Defense for use and dissemination within the Department of

Defense, recipients will be advised that the word originated outside the Department of Defense and is not subject to Department of Defense policy regarding the use of code words. However, such a word shall be safeguarded in accordance with the classification assigned thereto by the originating agency.

6. Classification, Downgrading and Declassification

a. During the development of a plan or the planning of an operation by the headquarters of the using agency, the code word and its meaning will have the same classification. When dissemination of the plan to other agencies or to subordinate echelons of the using agency is required, the using agency may downgrade the primary code word and such code words as are assigned to geographic locations in conjunction therewith below the classification assigned to their meanings in order to facilitate additional planning, implementation and execution by such other agencies or echelons. Code words in use or obsolete code words will not be downgraded below Confidential, will retain their classification and be safeguarded accordingly until the classification of their related meanings is cancelled.

b. A code word which is replaced by another code word due to the compromise or suspected compromise of the security of information connecting it with its assigned meaning, or for any other reason, will be carried as an "inactive code word" on the records of all agencies concerned and will retain its classification until its original related meaning has been declassified.

c. When a plan or operation is discontinued or completed, and is not replaced by a similar plan or operation but the meaning cannot for security reasons be declassified, the code word assigned thereto will be declared obsolete.

d. In every case whenever a code word in current use is employed, or an inactive or obsolete code word is referred to in written documents, the security classification of the code word will be placed in parentheses immediately following the code word, i.e., "Label (Confidential)".

e. When the meaning of a code word no longer requires a classification, the using agency will cancel the classification of both the meaning and the code word, including inactive and obsolete code words.

f. Immediately upon changing the classification of the code word or its meaning or cancelling the classification of a code word and its meaning, the using agency will notify the Secretary, Joint Intelligence Group, and all activities concerned within its own jurisdiction. The Secretary, ~~Joint Intelligence Group~~ Intelligence Directorate, the Joint Staff, will inform all other agencies concerned of the action taken.

7. Security Practices

a. Each agency will take positive action to insure that personnel

under its jurisdiction who receive knowledge of code words or the meanings of code words are informed of security measures necessary for their protection.

b. During discussions involving details of a classified plan or operation which reveal a classified meaning, the use of the related code word will be avoided unless all personnel present or within hearing also require knowledge of the code word. Likewise, whenever a code word is used during discussions, disclosure of information indicating the related meaning will be avoided unless all personnel present or within hearing also require knowledge of the meaning.

c. The meaning of a code word will be used in a message or other document together with the code word only when it is absolutely essential to do so. Code words may be used in correspondence or other documents forwarded to addressees who may or may not have knowledge of the meaning, but in all cases the code word will be employed in a document for purposes of concealment only. If the context of a document contains, for example, detailed instructions or similar information which indicates the purpose or nature of the related meaning, the assigned code word should not be used.

d. In handling correspondence pertaining to code words and their meanings, care should be used to avoid bringing the code words and their meanings together. They should be handled in separate card files, catalogs, indexes, or lists, enveloped separately and dispatched at different times so that they do not travel through mail or courier channels together.

e. A document containing a code word in use will be classified Confidential or higher in accordance with the highest classification assigned to information contained therein on the same basis as any other document which requires security protection. In no event, however, will the classification of the document be lower than the classification of the code word.

f. In view of the classification assigned thereto, code words will not be used for addresses, return addresses, shipping designators, file indicators, call signs, identification signals, or for other similar purposes.

g. The use of an inactive or obsolete code word for the purpose of referring to the classified meaning originally assigned to it is prohibited. Documents, including correspondence, containing a code word need not be revised or amended, but after receiving notice that the status of a code word has been changed to "inactive" or "obsolete", offices will promptly discontinue use of the word. Correspondence between offices concerned with the substitution of new words for old code words will be specific as to the inactive status of the old word.

h. The use of a declassified code word, standing alone, to represent or to substitute for its original meaning is prohibited. After declassification of a code word, reference to such word may be made in documents pertaining to the related plan or operation provided the text shows clearly that the word is no longer in use to represent a classified meaning.

i. A permanent record of all code words placed in use will be maintained by the Secretary, ~~Joint Intelligence Group.~~ * A code word which has been placed in use and subsequently declassified will be reallocated to a using agency only at the discretion of the Secretary, Joint Intelligence Group, at such time as he may consider that such reallocation and the assignment of a new meaning will not result in administrative confusion or loss of security concerning the new meaning.

* Intelligence Directorate, the Joint Staff

8. Compromise

a. Whenever the security of information connecting a code word in use with its classified meaning is compromised, the using agency will substitute a new code word for the old one immediately and change the status of the old word to "inactive".

b. Using agencies may also substitute new code words for code words in use, changing the status of the latter to "inactive", at their discretion whenever compromise of the security of information connecting the current code word with its meaning is suspected or anticipated due to excessive dissemination or for any other reason.

c. Reports submitted to the Secretary, ~~Joint Intelligence Group~~, showing the substitution of new code words for old code words will contain a statement explaining the reason for the substitution. For this purpose, the following terms may be used, whichever may be appropriate: "compromised", "compromise suspected", "excessive dissemination".

d. The agency having knowledge of the compromise or suspected compromise of classified information pertaining to code words by personnel under its jurisdiction, or having reason to believe that its personnel were involved in connection therewith, will make an investigation of the circumstances, fix responsibility for the compromise and take such corrective action as may be necessary.

F

20 August 1954
NUMBER 5200.8

Department of Defense Directive

SUBJECT Authority of Military Commanders under the Internal Security Act of 1950 to Issue Security Orders and Regulations for the Protection of Property or Places under Their Command

Reference: (a) Secretary of Defense Memorandum, dated 11 May 1951, Subject: "Authority of Military Commanders Under the Internal Security Act of 1950 to Issue Security Orders and Regulations for the Protection of Property or Places Under Their Command"

I. PURPOSE

The purpose of this Directive is:

A. To designate military commanders to promulgate regulations for the protection of property or places under their command, pursuant to the provisions of Section 21 of the Internal Security Act of 1950 (Public Law 831, 81st Congress).

B. To reissue in directive form the provisions of Reference (a) in order to comply with Section VI of Department of Defense Directive 5025.1, dated 2 February 1954, subject: "Department of Defense Directives System".

II. CANCELLATION

Reference (a) is cancelled and superseded by this Directive.

III. BACKGROUND

A. Section 21 of the Internal Security Act of 1950 states:

"797. Security regulations and orders; penalty for violation

(a) Whoever willfully shall violate any such regulation or order as, pursuant to lawful authority, shall be or has been promulgated or approved by the Secretary of Defense, or by any military commander designated by the

Secretary of Defense, or by the Director of the National Advisory Committee for Aeronautics, for the protection or security of military or naval aircraft, airports, airport facilities, vessels, harbors, ports, piers, water-front facilities, bases, forts, posts, laboratories, stations, vehicles, equipment, explosives, or other property or places subject to the jurisdiction, administration, or in the custody of the Department of Defense, any Department or agency of which said Department consists, or any officer or employee of said Department or agency, or of the National Advisory Committee for Aeronautics or any officer or employee thereof, relating to fire hazards, fire protection, lighting, machinery, guard service, disrepair, disuse or other unsatisfactory conditions thereon, or the ingress thereto or egress or removal of persons therefrom, or otherwise providing for safeguarding the same against destruction, loss, or injury by accident or by enemy action, sabotage or other subversive actions, shall be guilty of a misdemeanor and upon conviction thereof shall be liable to a fine of not to exceed $5,000 or to imprisonment for not more than one year, or both.

"(b) Every such regulation or order shall be posted in conspicuous and appropriate places. Sept. 23, 1950, c. 1024, Title I, Par. 21, 64 Stat. 1005."

IV. DESIGNATION OF AUTHORITY

The following military commanders are hereby designated as having the authority to promulgate the necessary regulations pursuant to paragraph III above.

A. Commanding officers of all military reservations, posts, camps, stations, or installations subject to the jurisdiction, administration, or in the custody of the Department of the Army.

B. Commanding officers of all naval ships, stations, activities and installations; and commanding officers of all Marine Corps posts, stations, and supply activities, subject to the jurisdiction, administration, or in the custody of the Department of the Navy.

C. Commanders of major air commands, numbered air forces, air divisions, wings, groups and installations, subject to the jurisdiction, administration, or in the custody of the Department of the Air Force.

V. PROMULGATION OF REGULATIONS

A. Regulations promulgated by military commanders designated hereby shall be in accordance with policies and procedures relative thereto established by the Secretary of the Military Department concerned.

B. Regulations issued pursuant hereto shall be posted in a conspicuous and appropriate place, and shall make appropriate citation of this designation and the Public Law under which the designation is made.

VI. EFFECTIVE DATE

This Directive is effective immediately.

C. E. Wilson

Secretary of Defense

G

AGENCY STRENGTH BY CATEGORY AS OF 30 SEPTEMBER 1961

	CIVILIAN	MILITARY	TOTAL
PROFESSIONAL EMPLOYEES:			
Scientific & Engineering Occupations			
Cryptologic Occupations			
Data Systems Occupations			
Other Occupations			
SUB TOTAL			
SUB-PROFESSIONAL SUPPORTING EMPLOYEES:			
Engineering Technicians			
Cryptologic Technicians			
Data Systems Technicians & Operators			
Other Support Occupations			
SUB TOTAL			
CLERICAL EMPLOYEES:			
WAGE BOARD (BLUE COLLAR) EMPLOYEES:			
TOTAL			

SECRET

AGENCY STRENGTH
AS OF
30 SEPTEMBER 1961

ORGANIZATION	CIVILIAN Authorized Man Years	CIVILIAN On Board	MILITARY Authorized Billets	MILITARY On Board	TOTAL Civilian Man Years & Military Billets	TOTAL On Board
Director, Deputy Director & Special Assistant (D & DI)						
Inspector General (D2)						
National Cryptologic Staff (D3)						
Production Organization (P)						
Production Group A (A)						
Production Group B (B)						
Production Group C (C)						
TOTAL PROD						
SUSLO's & Field Activities (F)						
Communications Security Organization (S)						
Management Services Organization (M)						
TOTAL O/M						
R/D Operations Organization (R)						
TOTAL NSA						

*Based on current PROD planning distributions.

SECRET

SECRET

NATIONAL SECURITY AGENCY
MANAGEMENT SERVICES ORGANIZATION
(M)

ASSISTANT DIRECTOR, NSA, FOR MANAGEMENT SERVICES

DEPUTY ASSISTANT DIRECTOR, NSA, FOR MANAGEMENT SERVICES

TECHNICAL DIRECTOR | **EXECUTIVE**

- PLANS AND PROGRAMS STAFF — M01
- LEGAL ADVISOR — M02

- OFFICE OF FINANCIAL SERVICES — M1
  - BUDGET DIVISION — M11
  - FINANCE AND ACCOUNTING DIVISION — M12
  - INTERNAL REVIEW DIVISION — M13
- OFFICE OF LOGISTIC SERVICES — M2
  - SUPPLY DIVISION — M21
  - EQUIPMENT DIVISION — M22
  - FACILITIES SERVICES DIVISION — M23
  - REQUIREMENTS DIVISION — M24
- OFFICE OF PERSONNEL SERVICES — M3
  - MEDICAL DIVISION — M31
  - MILITARY PERSONNEL DIVISION — M32
  - SERVICES AND SUPPORT DIVISION — M33
  - SELECTION AND EVALUATION DIVISION — M34
  - PERSONNEL OPERATIONS DIVISION — M35
- OFFICE OF TRAINING SERVICES — M4
  - NSA SCHOOL — M41
  - CRYPTOLOGIC LITERATURE DIVISION — M42
  - LANGUAGE RESEARCH DIVISION — M43
  - TRAINING SUPPORT DIVISION — M44
- OFFICE OF SECURITY SERVICES — M5
  - PHYSICAL AND INDUSTRIAL SECURITY DIVISION — M51
  - CLEARANCE DIVISION — M52
  - PERSONNEL INTERVIEW DIVISION — M53
  - SPECIAL OPERATIONS DIVISION — M54
  - SECURITY EDUCATION DIVISION — M55
- OFFICE OF ADMINISTRATIVE SERVICES — M6
  - MAIL TRAFFIC DIVISION — M61
  - OPERATIONS DIVISION — M62
  - MESSAGE CONTROL DIVISION — M63
  - CENTRAL REPRODUCTION SERVICES DIVISION — M64
- OFFICE OF RESOURCES ANALYSIS — M7
  - MANAGEMENT ENGINEERING DIVISION — M71
  - STATISTICAL SERVICES DIVISION — M72
  - RESOURCES ANALYSIS AND RESEARCH DIVISION — M73

CONFIDENTIAL

3 January 1962
Office of Resources Analysis
Management Engineering Division

J

MANAGEMENT SERVICES ORGANIZATION
OFFICE OF PERSONNEL SERVICES
(M3)

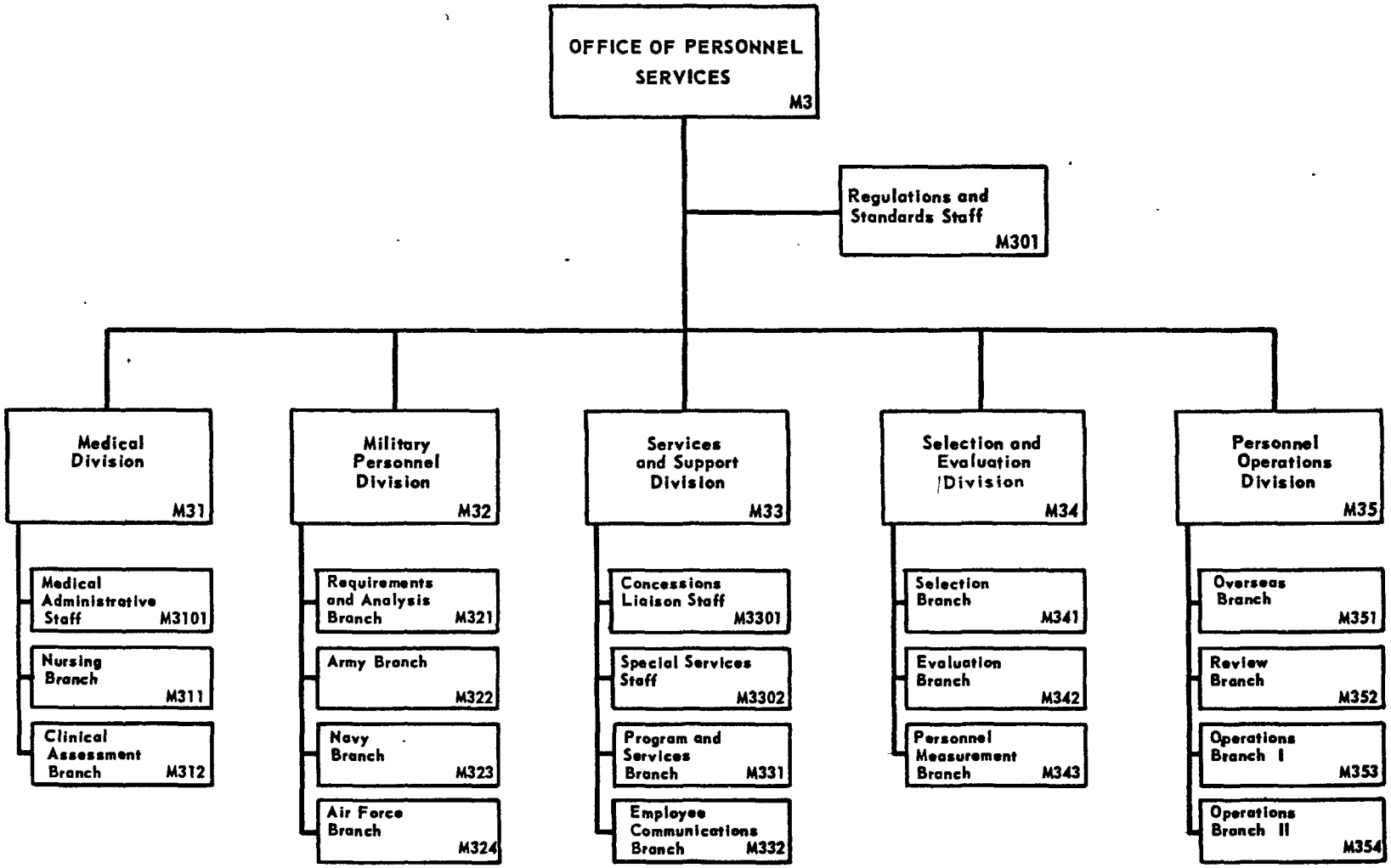


CHART NO. 4 – OFFICE OF PERSONNEL SERVICES
M3
(Page 1 of 2 Pages)

MANAGEMENT SERVICES ORGANIZATION
ORGANIZATION MANUAL

M3 - OFFICE OF PERSONNEL SERVICES

The Chief, Office of Personnel Services, is responsible for:

1. Advising the Assistant Director, NSA, for Management Services on personnel matters.

2. Formulating and establishing policies and regulations concerning personnel management and directing the related programs and organizations.

3. Providing guidance and assistance on personnel management in consonance with established policy and regulations.

4. Administering the Agency's delegated appointing and classification authorities.

5. Ascertaining personnel requirements within established manpower allocations and developing recruitment programs.

6. Procuring, appointing and placing employees and maintaining an effective workforce in consonance with the Agency's needs.

7. Conducting a complete job classification program; developing occupational standards; and maintaining the NSA Cryptologic Career Occuptational Structure.

8. Providing employee counseling guidance, recognition and incentive programs.

9. Providing a complete medical and health program.

10. Providing employee welfare activities and related employee services.

11. Planning and supervising all concession facilities in the NSA Operations Building.

12. Formulating, consolidating, and recommending the NSA Personal Services Budget and executing the approved funding program.

13. Providing liaison with Department of Defense, U. S. Civil Service Commission, and other Federal Agencies with respect to personnel matters.

Functional responsibilities delegated to the chiefs of the divisions and staffs of the Office of Personnel Services are as follows:

M301 - REGULATIONS AND STANDARDS STAFF

1. Conducting liaison with the U. S. Civil Service Commission, various Federal Departments and other public and private agencies to obtain information pertaining to personnel management.

2. Defining and publishing the basic and special programs, policies and procedures governing civilian and military personnel, within the framework of regulations, and legal and administrative authorities.

3. Publishing and disseminating manuals for the management of civilian and military personnel.

4. Issuing new or revised regulations, personnel policies, and instructions.

5. Maintaining reference material comprising personnel programs, policies, regulations and procedures issued by the Office of Personnel Services as well as those issued by the U. S. Civil Service Commission, Department of Defense, Departments of the Army, Navy, and Air Force; the Comptroller General's decisions; and other publications pertaining to civilian and military personnel administration.

6. Studying Agency jobs for the development, issuance and maintenance of occupational standards.

7. Conducting investigations and collecting information on Federal, private, and locality pay systems and pay fixing practices.

8. Maintaining and interpreting the NSA Cryptologic Career Occupational Structure, and the Cryptologic Career Occupational Handbook.

9. Maintaining and interpreting the NSA Job Evaluation Handbook.

10. Developing and recommending salary and wage administration plans, policies, and pay schedules for use in conjunction with the NSA Cryptologic Career Occupational Structure.

11. Determining the effect of Department of Defense and other directives, regulations, or issuances on the personnel program and recommending necessary action.

12. Providing for continuing analysis and evaluation of programs, organization, methods and procedures of the Office of Personnel Services in the implementation of policies and regulations, and assisting in resolving special problems, and conducting special studies and investigations, as required.

M31 - MEDICAL DIVISION

1. Establishing and maintaining an Agency medical program designed to: produce an accurate assessment of Agency working conditions as they affect employee health; assure proper assessment of employee capability to perform work in a specified Agency environment; afford professional diagnosis and recommendation regarding improvement of Agency working environment(s) and employee health problems. In fulfillment of these responsibilities, implementing such programs as:

a. The establishment, periodic review and validation of medical standards for Agency employment, which specify physical and psychological minimal acceptance criteria.

b. The conduct of pre-employment medical examination and periodic medical re-assessment to assure maintenance of employee health at minimum acceptable health levels in accordance with specified Agency health standards.

c. The provision of medical services for the treatment of on-the-job illnesses requiring emergency attention and for the treatment of injuries and illnesses due to occupational causes as authorized by the Federal Employees' Compensation Act of September 7, 1916, as amended.

d. The provision of diagnostic service (including psychological and psychiatric services) in determining the fitness of employees for duty.

e. The planned education of the work force toward health conservation and disease prevention.

2. Providing medical advice to Agency management and to the Office of Personnel Services in matters pertaining to mental hygiene, occupational health problems, safety practices and working environment.

3. Conducting medical research into specific areas relating to occupational disease prevention and reduction in absenteeism.

4. Maintaining liaison with the U. S. Public Health Service, the Civil Service Commission and other Federal agencies, professional medical societies and community health groups on programs and functions which relate to health service programs.

M32 - MILITARY PERSONNEL DIVISION

1. Developing and implementing military manpower programming; including programs for procurement, assignment and reassignment; utilization of military personnel, and effective military personnel management and administration.

2. Providing guidance and assistance to appropriate Agency operating officials in interpreting the philosophy, policies, procedures, and current rating practices and trends of the military services.

3. Providing personnel background information and assistance, as needed, in support of the military job classification and the military awards and decorations programs, and in the promulgation of regulations, standards, and procedures affecting military personnel administration in the Agency.

4. Providing information and requirements needed by other Agency elements in preparing, maintaining, and distributing accurate and timely strength data in support of programming and procurement actions, assignment and reassignment actions, military grade and skill distribution controls, and military billet change actions in meeting military manning requirements; also, in preparing the Agency Military Personnel Manning Document and the Classification and Assignment (C&A) Roster.

5. Rendering advice to Agency employees concerning military service obligations, including those encountered under the U. S. Armed Forces Reserve Program. Determining Agency requirements for military utilization of Agency employees having military status, in the event of partial or total mobilization.

6. Developing and implementing military personnel administration programs to provide for timely and accurate processing of personnel action requirements incident to military administration, such as disciplinary, training, classification and reclassification, and other related actions; maintaining the official Agency military personnel records.

7. Providing official representation needed on behalf of the Agency with the respective military services in discharging functions relating to the procurement, utilization and administration of military personnel.

M33 - SERVICES AND SUPPORT DIVISION

1. Providing employee services to meet needs of the Agency.

2. Maintaining liaison with the Fort Meade Post, with Federal employee groups, and with community service organizations on personnel services matters affecting employee relations.

3. Providing employee welfare activities.

4. Providing employee recognition and incentives programs.

5. Providing personnel management communications through such media as the NSA Newsletter and the Agency Public Address System.

6. Arranging for, supervising and coordinating private enterprise concession services in the NSA Operations Building, including Agency liaison with the banking facility in the NSA Operations Building.

7. Providing employee services for NSA personnel at NSA, Washington and NSA Vint Hill Farms Station, Virginia, either directly or through coordination with station employee associations.

8. Implementing certain Agency plans as they apply to the Office of Personnel Services; for example, the NSA General Operating Plan, War Emergency Plan, Alert Cadre and Local Emergency Plan.

M34 - SELECTION AND EVALUATION DIVISION

1. Procuring and placing applicants to meet Agency needs.

2. Developing and exploiting all available recruitment sources, and executing and effecting a public relations program through participation at annual college placement conferences.

3. Insuring the timely procurement of qualified civilian personnel to maintain the Agency at authorized strength.

4. Developing and conducting the Agency's induction and orientation program for civilian employees.

5. Administering the Agency's Registry for Consultants in coordination with other elements of the Office of Personnel Services.

6. Developing and applying evaluative criteria to determine the initial and continuing suitability of applicants and employees for employment with NSA.

7. Providing liaison with the Office of Security Services and appropriate elements of the Office of Personnel Services with respect to suitability matters.

8. Administering the Agency's psychological measurement program for the selection, placement and reassignment of personnel in certain occupational specialties.

M35 - PERSONNEL OPERATIONS DIVISION

1. Maintaining an effective work force in accordance with the Agency needs, including field and overseas stations.

2. Providing guidance and assistance in personnel management, including implementation of appropriate policy regulations to insure uniform administration.

3. Executing a complete position classification program implementing appropriate occupational standards.

4. Providing personnel assistance to management on matters relating to career development, in-service placement, promotions, reduction in force, performance ratings, separations, counseling of employees in matters of employment and morale.

5. Administering personnel actions (in-service placement, separations, suspensions, terminations) in accordance with the provisions of current applicable statutory and regulatory requirements.

6. Establishing and maintaining appropriate employee records and file systems in accordance with approved standards.

7. Executing supplemental and related programs; for example:

   a. Determining military personnel position requirements.

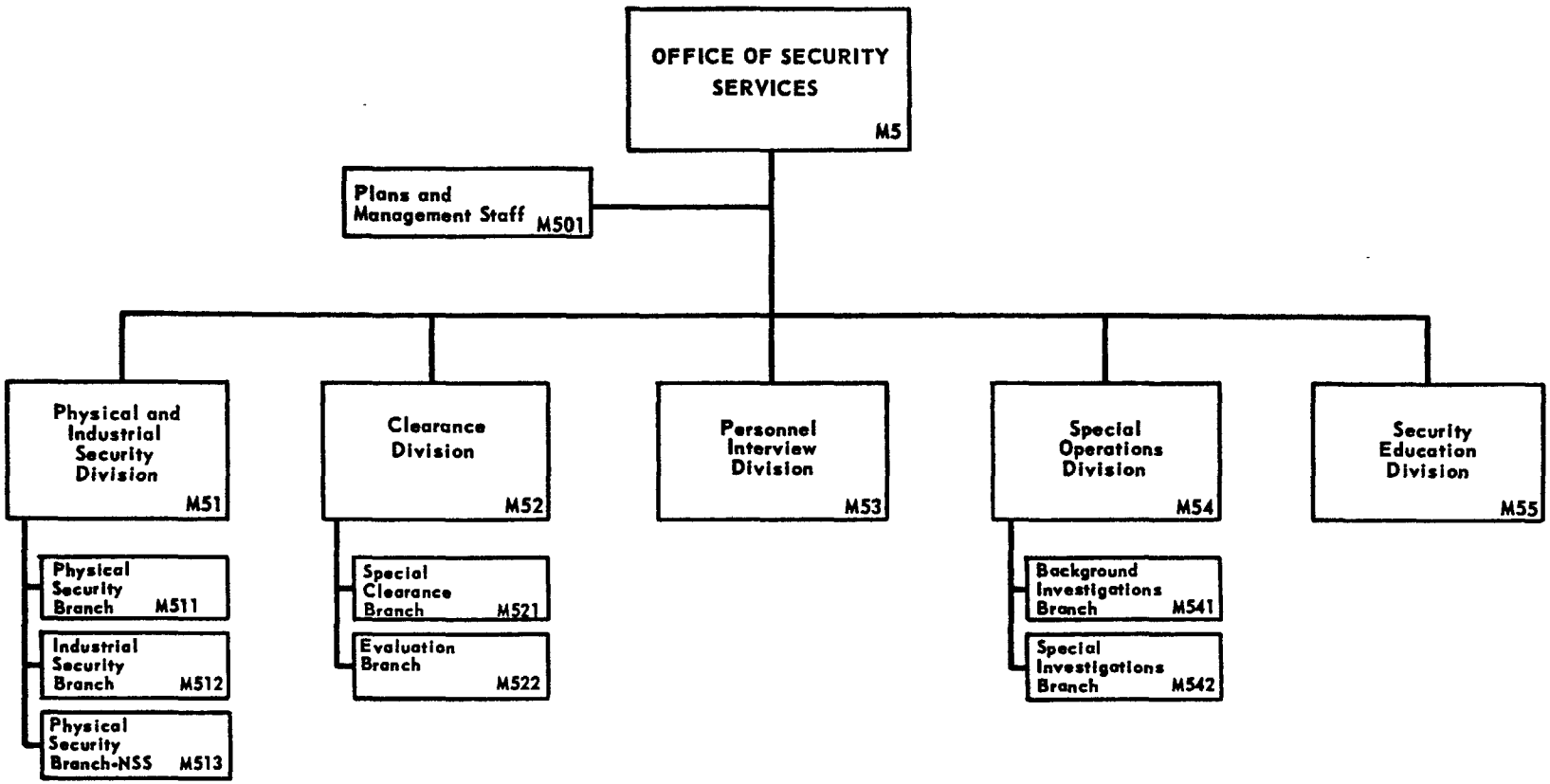
   b. Conducting utilization audits, as required.

8. Maintaining pertinent data concerning military obligation status of Agency employees for use in determining Agency retention or deferment action in the event of partial or total mobilization. Providing required evaluation of Agency retention needs of civilian employees having military service obligations.

K

CHART NO. 6 – OFFICE OF SCURITY SERVICES
M5
(Page 1 of 2 Pages)

MANAGEMENT SERVICES ORGANIZATION
OFFICE OF SECURITY SERVICES
(M5)



M5 - OFFICE OF SECURITY SERVICES

The Chief of the Office of Security Services is responsible for:

1. Developing security plans, policies, and procedures (except for communications security).

2. Assuring that all persons requiring access to NSA material meet Agency security standards including provision of the requisite indoctrination and orientation.

3. Conducting the Agency Security Education Program.

4. Ensuring physical security standards necessary to protect adequately NSA classified matter (except communications security material) by inspection, use of security devices, use of those guard forces assigned to the Office of Security Services, and coordination of the guard activities of the Marine Barracks, Fort Meade, Maryland.

5. Assisting and advising the Director in his counter-intelligence, investigative and other security responsibilities (except communications security).

6. Controlling the destruction of non-cryptographic classified waste.

Functional responsibilities delegated to the chiefs of the divisions and staffs of the Office of Security Services are as follows:

M501 - PLANS AND MANAGEMENT STAFF

1. Assisting the Chief, Office of Security Services, in developing, augmenting, and implementing security plans, policies, standards, and programs, including advisory participation in Agency planning or operational conferences and review of directives of the Department of Defense and other higher authority to determine applicability to security activities.

2. Assuring that the management responsibilities with respect to established plans, policies, and programs are properly accomplished by the elements within the Office of Security Services.

3. Providing staffing for unique security problems, and conducting those special studies necessary for the effective administration and direction of security operations.

4. Processing, maintaining and recalling, as required, all operational and administrative files of the Office of Security Services.

5. Providing processing services for all clearance actions involving NSA civilian applicants, employees, military personnel, employees of industrial facilities working on industrial contracts, consultants, advisors, concessionaire personnel, and GSA personnel assigned to NSA.

6. Recording and maintaining records of clearance actions, and, when required, forwarding the clearance status of Agency employees to other interested Governmental activities and industrial facilities where NSA personnel are to visit for official purposes.

7. Preparing, justifying, and executing the Operating Budget for the Office of Security Services.

8. Providing internal administrative and management services, including maintenance of a work measurement system.

M51 - PHYSICAL AND INDUSTRIAL SECURITY DIVISION

1. Developing, promulgating, and evaluating the necessary standards and practices for physical and industrial security to insure that unauthorized individuals do not gain access to classified information and materials of the Agency.

2. Developing, implementing, and monitoring control systems to insure that Agency operations are conducted in accordance with the prescribed standards, procedures, and practices for physically safeguarding the sensitivity of Agency space, operations, information and materials.

3. Providing operational servicing of or monitoring the application of regulatory controls for procedures or practices such as the storage, handling, transmission, and destruction of classified matter, as required, to insure its protection from unauthorized persons.

4. Conducting physical security surveys in order to properly establish security requirements for sensitive operations and insure compliance with recommendations based upon such surveys through the conduct of physical security inspections.

5. Investigating security violations occurring within Agency installations and evaluating reports of possible COMINT compromises which occur in NSA and the Service Cryptologic Agencies.

6. Assuming complete cognizance for all security requirements on COMINT procurements, including personnel clearance, facility clearances, surveys, inspections, visitor control, and security guidance, to insure that classified NSA material in the possession of commercial contractors is properly safeguarded.

7. Conducting surveys and inspections, as required, for the purpose of establishing requirements and rendering security guidance to all contractors, consultants, and advisors engaged in classified operations, other than COMINT, on behalf of the Agency to insure that all NSA classified material is adequately safeguarded.

8. Performing internal and external liaison on physical security matters and required operational liaison on industrial security matters.

9. Conducting necessary liaison with appropriate military authorities to coordinate matters pertaining to the operation and utilization of a Marine Guard Force for the protection of Agency spaces and information.

MANAGEMENT SERVICES ORGANIZATION
ORGANIZATION MANUAL

M52 - CLEARANCE DIVISION

1. Reviewing and evaluating personnel information collected during the processing of applicants for employment by NSA to insure that the Office of Personnel Services is aware, prior to the completion of hiring action, of any instance in which the applicant may not meet security standards for clearance.

2. Determining the eligibility of applicants for access to classified information at the SECRET level, during the period pending completion of investigative action necessary before a determination of eligibility for full clearance can be made.

3. Conducting evaluations of all personnel and investigative data collected regarding new employees and determining eligibility in each case for TOP SECRET and Cryptographic clearance and indoctrination for COMINT.

4. Conducting evaluations of non-employees' cases to determine eligibility of the individuals involved for full or limited access to Agency spaces and/or classified information.

5. Conducting evaluations of all data developed during reinvestigations of employees and non-employees who require access to NSA's sensitive materials or information, and determining eligibility in each case for continued TOP SECRET and cryptographic clearance and access to COMINT.

6. Reviewing security files of employees and non-employees to determine eligibility for special access, PCS, TDY, or for such other purposes as may be required.

7. Conducting such other activities relating to clearances as may be required, including review of incident reports, interview of employees, preparation of case summaries, the initiation of requests for special investigations and preparation of pertinent informantion for dissemination to other investigative agencies.

MANAGEMENT SERVICES ORGANIZATION
ORGANIZATION MANUAL

M53 - PERSONNEL INTERVIEW DIVISION

1. Conducting personnel security interviews with the aid of the polygraph of applicants, contractor and consultant personnel working on NSA classified information, and other persons directly affiliated with NSA activities for the purpose of obtaining information which will be useful in reaching a determination of eligibility for access to NSA spaces or classified information.

2. Conducting interviews with the aid of the polygraph of NSA employees, when required, in connection with cases involving eligibility for continued clearance.

MANAGEMENT SERVICES ORGANIZATION
ORGANIZATION MANUAL

M54 - SPECIAL OPERATIONS DIVISION

1. Conducting limited numbers of complete investigations into the backgrounds of applicants for employment with the National Security Agency for the purpose of collecting information germane to a clearance determination.

2. Engaging in the collection of background data and other pertinent facts concerning selected employees, contractors, consultants, and advisors to permit an expeditious evaluation of the individual's eligibility for access to NSA classified information.

3. Conducting necessary investigative activity to satisfactorily resolve complaints, allegations, and incidents involving NSA civilian personnel.

4. Conducting such other investigations as may be required from time to time, including, but not limited to, priority re-investigations, missing employees, supplements to service investigations, inquiries on behalf of the Directorate, special investigations in support of clearance programs and investigation of incidents and possible criminal activity.

5. Developing, implementing, and supervising a counterintelligence program designed to prevent or detect any attempt by a foreign intelligence activity to penetrate NSA operations.

6. Establishing and maintaining liaison with local law enforcement and Governmental agencies to develop and co-ordinate matters of material interest and insure prompt notification of matters of interest to NSA and the Office of Security Services.

MANAGEMENT SERVICES ORGANIZATION
ORGANIZATION MANUAL

M55 - SECURITY EDUCATION DIVISION

1. Administering an education program designed to instruct all employees of the Agency of their individual security responsibilities and to remind them on a periodic basis of the necessity for protecting classified information. These programs include the Security Lecture Program, the Security Education Officer Program, and addresses to groups or organizations upon request.

2. Conducting security orientation, limited access briefings, and providing COMINT indoctrinations and debriefings.

3. Providing guidance for security education material to industrial concerns engaged in classified procurements on behalf of the National Security Agency in order to insure the adequate development of a security education program to assist in the safeguarding of NSA material.

4. Designing, developing, and issuing security education materials, reminders, and other visual aids as part of a program to engender security consciousness on the part of all persons having access to NSA material, information, or space.

5. Providing security guidance on an individual basis including special briefings to personnel scheduled for temporary or permanent assignment overseas, spouses of such persons, and personnel traveling to foreign countries on annual leave.

~~TOP SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~