

Mr. Whitehead

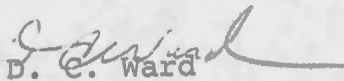
OFFICE OF TELECOMMUNICATIONS POLICY  
WASHINGTON

February 28, 1973

To: All Concerned

Please substitute the attached pages  
for the ones now in your War Emergency  
Readiness Plan.

Note: Section 6 has been replaced in  
its entirety.

  
D. E. Ward

## TABLE OF CONTENTS

<u>Subject</u>	<u>Page</u>
MEMORANDUM	i
TABLE OF CONTENTS	ii
INTRODUCTION	1-1
APPLICABLE REFERENCES	2-1
RELOCATION SITES	3-1
RELOCATION RESPONSIBILITIES	4-1
SUCCESSION PROCEDURES	5-1
WARNING CONDITIONS	6-1
ALERTING PROCEDURES	7-1
MOVEMENT INSTRUCTIONS	8-1
DEPENDENTS INSTRUCTIONS	9-1
VITAL RECORDS	10-1

## SECTION 2

### APPLICABLE REFERENCES

1. Executive Order 11556 of 4 September 1970.
2. Communications Act of 1934, as amended.
3. Executive Order 10705, 17 April 1957, as amended, "Delegating Certain Authority of the President Relating to Radio Stations and Communications."
4. Communications Satellite Act of 1962.
5. Executive Order 11051, 27 September 1962, "Prescribing Responsibilities of the Office of Emergency Planning in the Executive Office of the President."
6. Executive Order 11490, 28 October 1969, "Assigning Emergency Preparedness Functions to Federal Departments and Agencies."
7. Office of Emergency Preparedness, OEP Circular 9410.1C, 19 January 1973, "Federal Civil Readiness Levels and Actions in Response to Official Instructions in an Emergency."
8. "The National Plan for Emergency Preparedness," Office of Emergency Preparedness. (current edition)
9. Memorandum to the Heads of Executive Departments and Agencies, 21 August 1963, "Establishment of the National Communications System."
10. Manual of Regulations and Procedures for Radio Frequency Management.
11. Executive Order 11191, 4 January 1965, "Providing for the Carrying Out of Certain Provisions of the Communications Satellite Act of 1962."
12. OEP Circular 9100.2, April 12, 1972, "Continuity of the Executive Branch of the Federal Government."

## EMERGENCY ASSIGNMENTS

The following OTP personnel will relocate when directed, to Site 1 and 2. The Director and the remainder of OTP personnel will remain at the headquarters.

<u>Site 1</u>	<u>Site 2</u>	
	<u>OTP</u>	<u>IRAC MEMBERS</u>
Deputy Director	Dean	Baker, W. (Int)
Colby	Robinson	Davis, D. (USAF)
Doyle	Lasher	Dodrill, G. (AEC)
Hall, D.	Johnston	Holt, R. (VA)
Chesbrough	Roposh	Horne, C. (FCC)
Polk	Buss	Kessler, S. (USIA)
Enslow	Houston	Landreville, E. (JUS)
Byrum	Jansky	Lemnah, J. (FCC)
White	Hailey	McDonald, J., Jr. (USN)
	Brown	Morton, W. (AGRI)
	Bolen, P.	Myers, R. (TREASURY)
		Owens, W. (FAA)
		Pappas, W. (CG)
		Rasmussen, A. (USAR)
		Torak, W. (FCC)
		Van Winegarden (COMMERCE)

CHART 2



## SECTION 6

### WARNING CONDITIONS

#### PURPOSE

To describe civil readiness levels and actions in response to official instructions in an emergency.

#### POLICY

Defense Readiness Conditions (DEFCONS) will no longer be used to indicate desired changes in civil emergency readiness. Agencies having particular responsibilities keyed to military actions will be notified of DEFCONS by military authorities. The readiness posture of Federal departments and agencies will be tailored to the emergency situation. Special guidance will be issued by the President or the Director of OEP to (1) accelerate or decelerate readiness during a prolonged period of international tension; (2) guide the degree of agency activation of primary and alternate headquarters; and (3) establish further dissemination of readiness requirements to other levels of government and the public.

#### READINESS LEVELS

The following readiness levels are established for civil preparedness actions as indicated:

a. Communications Watch. The normal or near normal preparedness posture of many elements of the Federal Government. This readiness level may be established by the Director, OEP. When notification is received, a capability for monitoring official voice and record communications on a 24-hour basis should be established wherever such a capability is lacking. "Communications watch" readiness level, when directed, will be limited to regular National offices unless specific instructions direct otherwise.

#### OTP Actions

1. Notify key staff members.
2. Review all emergency plans and procedures.

b. Initial Alert. This notification requires establishment of continuous manning of emergency operating centers at regular National offices. This readiness level will be carried out with minimum public disclosure.

#### OTP Actions

1. Upon receipt of initial alert the OTP TIC will be manned on a continuous basis.

2. The Computer Support Section at Site 2 will be alerted for possible around-the-clock operation.

3. Verify, and assure immediate availability of emergency action documents.

c. Advanced Alert. This notification will indicate that the President desires achievement of the highest degree of civil emergency readiness. Primary emergency operating centers of the Federal Government at headquarters, at regions, and at other major field offices will be manned. Actions necessary for the activation of alternate emergency operating centers will be completed.

It is expected that such an instruction would coincide with or be immediately followed by a Presidential statement. Such a statement could contain general guidance on the nature of the deteriorating situation and the appropriate form of public response.

Emergency duties at this time will include continuation of the essential processes of government as well as emergency preparations for the essential functions required if warning of attack should be received.

#### OTP Actions

1. Notify OTP personnel designated to man alternate emergency operating centers to be prepared to relocate upon direction.

2. Be prepared to establish a 24-hour operational watch at the alternate site.

3. Unless otherwise directed IRAC designated personnel will relocate to Site 2.



4. Contact FCC to insure that the common carriers and broadcasting systems have been alerted to the impending critical situation.

5. Contact the Executive Agent, NCS, to insure that all communication readiness measures are being implemented.

Cancellation. The cancellation of any readiness level without a further declaration will indicate agencies should return to normal operations.

Exercise Terms. When used in exercises, readiness levels will be identified as shown below to avoid possible confusion.

<u>Readiness Level</u>	<u>Exercise Term</u>
Communications Watch	Quick Step
Initial Alert	Tight Rein
Advanced Alert	Flood Tide

The Director, OTP will receive notification of these readiness levels directly from the Special Facilities Division.

#### WARNING CONDITIONS

The Defense Civil Preparedness Agency (DCPA) of the Department of Defense has Federal responsibility for making appropriate arrangements for warning the public and for the operation of the Federal portion of the attack warning systems. OTP will receive notification from DCPA via the Special Facilities Division who will assure notification to the Director, OTP, of the attack warning and termination of attack warning.

Attack Warning. This means that an attack against this country has been detected and all feasible Federal/civil agency actions should be directed toward the preservation and continuity of government and measures to preserve life and property.

Termination of Attack Warning. This indicates that the situation warrants the movement of people from shelter and to or from emergency operating facilities, where fallout conditions permit, but the possibility of subsequent attack still exists.

## INDIVIDUAL ALERTING DISSEMINATION ACTIONS

When the telephone alerting system is fully activated, OTP personnel will take the following actions:

After receiving an alerting telephone call, indicating that a Readiness Level change has been declared, the recipient of the call will ensure that he has clearly understood the message transmitted.

The message received will be immediately relayed to those employees whom the recipient of the message is charged with notifying.

Each caller shall identify himself, state the message clearly and succinctly, and, after completing the message, ask the person he is calling to repeat it. The latter to assure that the message has been properly received.

When a called person cannot be contacted immediately, the caller will complete his other calls and then assume responsibility for notifying the persons who would normally be notified by the person whom the caller could not notify.

Except in the case of ATTACK WARNING, telephone alerting messages will be given only to the person called. If the person called is not available, the person answering will be told "this is a call of an emergency nature. Contact Mr. (s) \_\_\_\_\_ immediately and have him return this call as soon as possible." If no one answers the telephone call, the caller should try to complete the call again, conditions permitting. Notice of ATTACK WARNING will be given to any person answering the telephone, and there will be no requirement for returning ATTACK WARNING telephone calls.

## RESPONSIBILITIES

Individual - Each OTP employee will keep the Director's Office informed of his home and office telephone numbers.

Each employee will keep a current copy of this section of the OTP Readiness Plan readily available at his home.



DIRECTOR OF TELECOMMUNICATIONS POLICY  
Secondary Alerting Chart and Group Designation (Non-Duty Hours)

<u>Caller</u>		<u>First Call</u>		<u>Second Call</u>	
1. Jiggetts	323-5954	2. Whitehead	293-3293	3.	
2. Ward	244-4342	4. Dean*	356-7217	5. Joyce	424-5635
3. Joyce		6. Smith, B.	234-6669	7. Daughtrey	261-4060
4. Smith, B.		8. Doyle	765-1608	9. Morton	931-3418
5. Doyle		10. Belo	561-5489	11. Goldberg	525-3878
6. Goldberg		12. Lamb	521-6375	13. Hall, D.	451-6288
7. Hall, D.		14. Lasher	536-4776	15. Johnston	573-4336
8. Lamb		16. Robinson	301-647-7357	17. Beery	569-1622
9. Lasher		18. Toms	871-8984	19. Polk	273-6088
10. Beery		20. Eagle	338-0218		

OEP will call either Ward or Jiggetts. Whoever gets first call will call the other.  
\*Dean will call Frequency Personnel.

## SECTION 8

### MOVEMENT INSTRUCTIONS

#### PURPOSE

To provide guidance for movement to Emergency Relocation Sites.

#### GENERAL

OTP employees scheduled for relocation have been divided into two groups. See Chart 2. All other OTP employees not on these lists will remain at the OTP Office, 1800 G. Street, NW.

Each OTP employee should select at least two possible routes from his office and home locations to his designated relocation site. If possible, each employee should make trial runs to his site so that when relocation is required it can be effected with optimum efficiency. See attached charts pages 8-3 and 8-4.

#### SPECIAL ARRANGEMENTS

By mutual agreement between the FCC and OTP certain FCC personnel will proceed to Site Number 2:

- Upon announcement of ADVANCED ALERT unless otherwise directed.
- Upon order from appropriate authority that relocation should be effected.

#### TRANSPORTATION

Transportation during duty hours for relocation may be provided in accordance with instructions disseminated by the Director, Office of Telecommunications Policy. This fact, however, is not yet certain, for the situation which will exist at a time of possible mass evacuation from Washington is uncertain. Accordingly, employees should take steps to assure transportation under such conditions as are outlined below for non-duty hours.

#### During Non-Duty Hours

Employees should make plans for transportation to sites based upon their own or other office employee's transportation means.

### Contingency

An employee temporarily unable to reach his relocation site should bear in mind that reaching his designated relocation site is his primary mission. However, conditions may arise in which such a temporary situation may last for more than a few hours. In these instances, the employee should contact the nearest community head of civil government, indicate his ultimate destination, and offer his services until conditions permit his travel to his designated relocation site.

### COMMUNICATIONS

An employee unable to reach his designated relocation site should state, if possible, his whereabouts by calling collect to:

301-689-8873

If OTP personnel are not able to make contact by telephone, they should obtain the following forms at any Post Office, complete and mail them immediately:

(1) Civil Service Commission Form 600, Federal Employees Registration Card.

(2) Post Office Department Forms 809 and 810, Emergency Change of Address Card and Safety Notification Card.

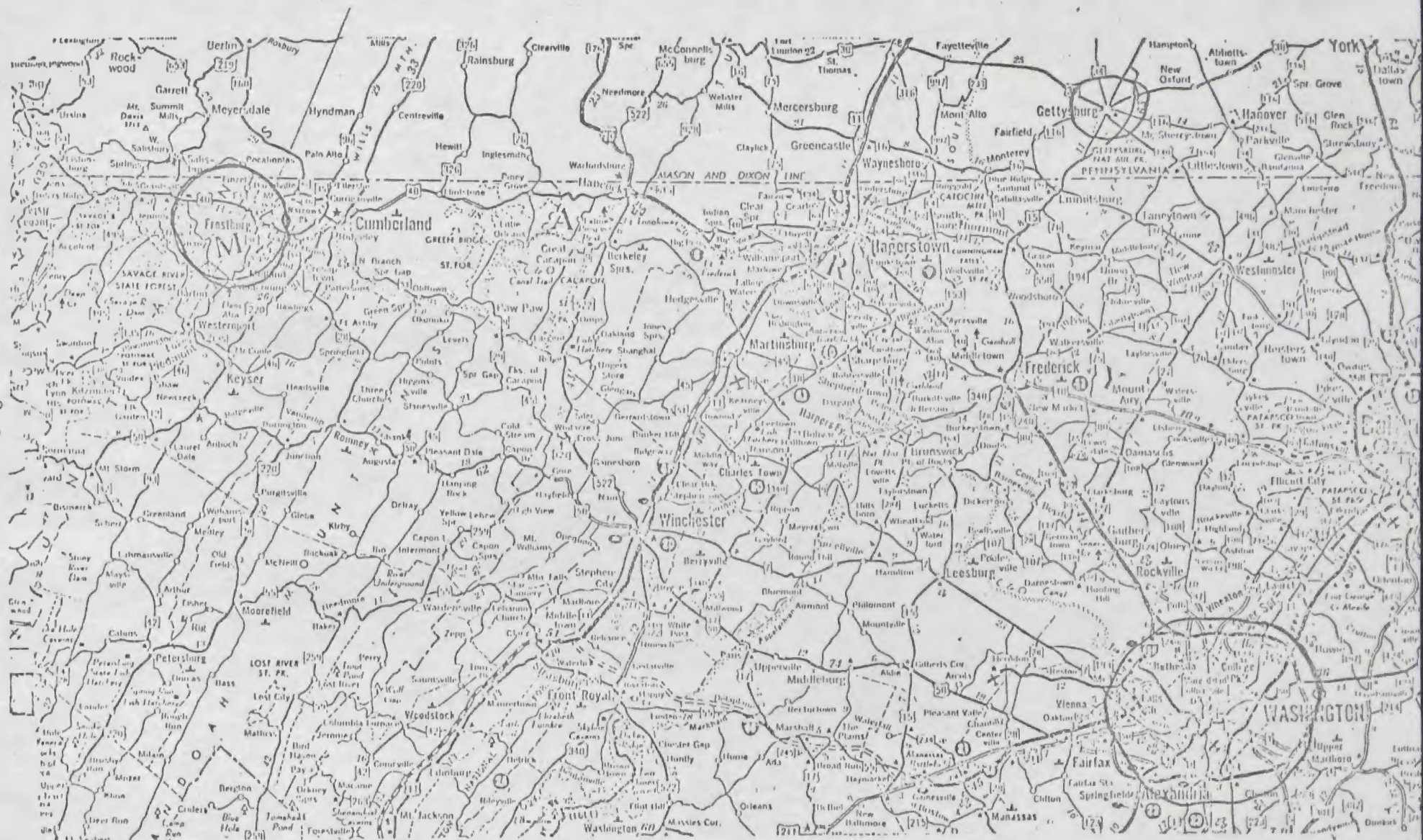
### INDIVIDUAL PRECAUTIONS

Each employee of the OTP should keep the unclassified copy of this document at his home for ready emergency use.

Each Employee should maintain in his office an emergency kit of toilet articles.



# COMPUTER SUPPORT SECTION



8-3



## SECTION 10

### VITAL RECORDS

#### PURPOSE

To prescribe objectives, responsibilities, criteria, and procedures for the protection and availability of OTP vital records.

#### BACKGROUND

Under government continuity policies and objectives established by OEP, the GSA, by Presidential delegation, provides coordination and technical direction to all Federal agencies for the storage and protection of vital records. Within this framework of procedures, OTP must, like all agencies, have a system for storing and protecting those records which are vital to emergency or war operations.

OTP vital records are stored at two locations -- the OTP emergency relocation site and classified OEP site.

#### CRITERIA

Only those records essential to emergency operations or the reconstruction of OTP post-attack operations will be singled out for special storage and protection. Records required to protect the legal rights of individuals are included in this category. Records having peacetime archival, historical, or research value, are not necessarily included.

Overall categories of vital records include: Legislative Acts and Executive Orders; Directives such as DMO's, OEP Circulars, OEP Orders; Presidential Memoranda; Regulations; Emergency Documents such as the National Plan, Emergency Measures Digest, standby authorities, State Plans, etc.; reference materials such as surveys of various resources, critical industrial facilities lists, etc.; Personnel and fiscal records; and some correspondence.

Vital OTP records are those which pertain to: the legal authority for OTP existence and mission; succession of command for appropriate

departments and agencies; delegation of authority within the Executive Branch; authorities to take effect; documents to be administered by OTP, and certain other records as may be approved for inclusion.

To assure the quickest reconstruction and continued operation of OTP, certain administrative records will be provided at each of the three sites.

### RESPONSIBILITIES

The Assistant for Administration to the DTP is responsible for the OTP Vital Records Protection Program and for the selection, processing, and protection of OTP vital records. In addition, he is responsible for affecting all necessary coordination on this subject with the Director of Administration, OEP.

OTP Directors and the Legal Counsel will indicate those records which are recommended for designation as OTP vital records. These recommendations will be forwarded to the Assistant for Administration.

### PROCEDURES

Transmittal - OTP Directors and Legal Counsel will submit to the Assistant for Administration one set of approved vital records for each site at which the records are to be maintained. Any records destined for one of the OEP classified sites must be submitted in three identical sets. In addition, all changes to these documents will be submitted as early as possible after the changes have been approved.

The Assistant for Administration will check the documents received and, if they are approved vital records in proper form and number of copies, forward them for storage. A copy of the correspondence forwarding the records will be maintained on file.

Vital records for storage at the OTP emergency relocation sites will be forwarded directly to the site. Vital records for storage at the classified OEP site will be forwarded to the Management Assistance Branch, OEP.

Storage and Maintenance - Vital records will be categorized as to content and filed simply and uniformly at all relocation sites. In all cases, OTP vital records will be filed together, kept accessible, and maintained current at all times.

Vital records in storage at sites will not be used for day-to-day reference purposes.

Reports - GSA requires semi-annual reports on vital records. Accordingly, the OTP Assistant for Administration will provide a semi-annual statement that OTP vital records at the classified OEP relocation site have been examined and inventoried, and that those files are current and complete. Where deficiencies exist they will be listed, and action will be undertaken by the OTP Assistant for Administration to correct the deficiencies noted. In each instance, the Assistant for Administration will try to determine the reasons for deficiencies noted.

The OTP staff-member-in-charge at the OTP emergency relocation sites will conduct inventories, submit reports, and conduct studies for the vital records at that site. These reports will be forwarded to the Assistant for Administration, OTP.

The reports discussed in the foregoing will be submitted for periods ending June 30 and December 31. They will be submitted as required no later than 15 days after the end of the dates indicated.

#### VITAL RECORDS LISTING

A listing of OTP vital records begins on page 10-6 of this section.



LIST OF  
VITAL RECORDS



SUBJECT: Abbreviations Used in Records Listing

<u>Symbol</u>	<u>Meaning</u>
TEL-1:	Not Used.
TEL-2:	Treaties, Legislation, Executive Orders and Administrative Issuances.
TEL-3:	Mobilization Plans.
TEL-4:	Not Used.
TEL-5:	Not Used.
TEL-6:	Frequency Assignments to Government Radio Stations.
TEL-7:	Memorandums.
TEL-8:	National Communications System
A	Indicates storage at the classified OEP Relocation Site.
B	Indicates storage at the OTP Emergency Relocation Site.
C	Indicates classification of basic document is CONFIDENTIAL.
S	Indicates classification of basic document is SECRET

# VITAL RECORDS LIST

Symbol	Subject and Document	Location	
TEL-1	NOT USED		
TEL-2	<u>Treaties, Legislation, Executive Orders, and Administrative Issuances</u>		
	2.1 <u>International Treaties and Agreements</u>		
	2.1.1 ITU Radio Regulations (current edition)	A	B
	2.1.2 International Telecommunication Convention (current edition)	A	B
	2.2 <u>Legislation</u>		
	2.2.1 The Communications Act of 1934 with Amendments thereto, revised to January 1969	A	B
	2.2.2 Public Law 87-192, 87th Congress, S.2034, August 31, 1961	A	B
	2.2.3 Public Law 87-306, 87th Congress, S.1990, September 26, 1961	A	B
	2.2.4 Public Law 87-439, 87th Congress, S.1371, April 27, 1962	A	B
	2.2.5 Public Law 87-447, 87th Congress, S.205, May 1, 1962	A	B
	2.2.6 Public Law 87-795, 87th Congress, H.R. 11732, October 11, 1962	A	B
	2.3 <u>EXECUTIVE ORDERS</u> -- Nos. 10705; 11007; 11191; 11490; 11556	A	B
	2.4 <u>Administrative Issuances</u>		
	2.4.1 Telecom Circular 3300.4 - "Procedures for the Use and Coordination of the Radio Spectrum During a National Emergency."	A	B

Symbol	Subject and Document	Location	
2.4.2	ODM/BSDA Telecommunications Functions, dated March 12, 1957	A	B
2.4.3	Telecom Circular 3300.5 - "Federal Government Focal Point for EMP Information	A	B
2.4.4	Telecom Circular 3300.6 - "Priority System for the Use and Restoration of Leased Intercity Private Line Services During Emergency Conditions" (36 F.R. 25419, dated December 29, 1971)	A	B
2.4.5	Telecom Circular 3300.2 - "Procedures for Obtaining International Telecommunication Service for Use During a National Emergency" )33 F.R. (33 F.R. 10929, dated August 1, 1968)	A	B
TEL-3	<u>Mobilization Plans</u>		
3.1	Emergency Readiness Plan for Use of the Radio Spectrum	A	B
3.2	Inventory of Non-Government International Radio, Satellite and Cable Circuitry	A	B
3.3	The National Plan for Emergency Preparedness, OEP, dated December 1964	A	B
3.4	Federal Emergency Plan D, dated February 1968 (S)	A	B
3.5	Navy Department Document ONI-60-2, "United States of America Telecommunications Censorship Basic Plan" (C)		B
3.6	Office of Censorship Basic Plan, OCBP-64, dated May 15, 1964 (C)	A	B
3.7	Telecom Annex to Federal Emergency Plan D (S)	A	B



Symbol	Subject and Document	Location	
	3.8 Documents for Contingencies Other Than a Plan D Situation Parts I, II, III, and IV, dated November 1972	A	B
TEL-4	NOT USED		
TEL-5	NOT USED		
TEL-6	<u>Frequency Assignments to Government Radio Stations</u>		
	6.1 . Frequency Assignments to Government Radio Stations - Vol. I (of XX Vols.) Below 2505 KHz (C)	A	B
	6.2 Frequency Assignments to Government Radio Stations - Vol. II (of XX Vols.) 2505 to 4063 KHz (C)	A	B
	6.3 Frequency Assignments to Government Radio Stations - Vol. III (of XX Vols.) 4063 to 5450 KHz (C)	A	B
	6.4 Frequency Assignments to Government Radio Stations - Vol. IV (of XX Vols.) 5450 to 8195 KHz (C)	A	B
	6.5 Frequency Assignments to Government Radio Stations - Vol. V (of XX Vols.) 8195 to 13200 KHz (C)	A	B
	6.6 Frequency Assignments to Government Radio Stations - Vol. VI (of XX Vols.) 13200 to 17700 KHz (C)	A	B
	6.7 Frequency Assignments to Government Radio Stations - Vol. VII (of XX Vols.) 17700 to 24990 KHz (C)	A	B
	6.8 Frequency Assignments to Government Radio Stations - Vol. VIII (of XX Vols.) 24990 KHz to 108 MHz (C)	A	B
	6.9 Frequency Assignments to Government Radio Stations - Vol. IX (of XX Vols.) 108 MHz to 136 MHz (C)	A	B



Symbol	Subject and Document	Location	
6.10	Frequency Assignments to Government Radio Stations - Vol. X (of XX Vols.) 136 MHz to 162 MHz (C)	A	B
6.11	Frequency Assignments to Government Radio Stations - Vol. XI (of XX Vols.) 162 MHz to 166 MHz (C)	A	B
6.12	Frequency Assignments to Government Radio Stations - Vol. XII (of XX Vols.) 166 MHz to 170 MHz (C)	A	B
6.13	Frequency Assignments to Government Radio Stations - Vol. XIII (of XX Vols.) 170 MHz to 174 MHz (C)	A	B
6.14	Frequency Assignments to Government Radio Stations - Vol. XIV (of XX Vols.) 174 to 328.6 MHz (C)	A	B
6.15	Frequency Assignments to Government Radio Stations - Vol. XV (of XX Vols.) 328.6 to 420 MHz (C)	A	B
6.16	Frequency Assignments to Government Radio Stations - Vol. XVI (of XX Vols.) 420 to 1850 MHz (C)	A	B
6.17	Frequency Assignments to Government Radio Stations - Vol. XVII (of XX Vols.) 1850 to 5000 MHz (C)	A	B
6.18	Frequency Assignments to Government Radio Stations - Vol. XVIII (of XX Vols.) 5000 to 7250 MHz (C)	A	B
6.19	Frequency Assignments to Government Radio Stations - Vol. XIX (of XX Vols.) 7250 to 7750 MHz (C)	A	B
6.20	Frequency Assignments to Government Radio Stations - Vol. XX (of XX Vols.) 7750 MHz and above (C)	A	B
6.21	Manual of Regulations and Procedures for Radio Frequency Management - revised current version (C)	A	B

Symbol	Subject and Document	Location	
TEL-7	<u>Memorandums</u>		
7.1	National Security Action Memorandum No. 166, dated June 25, 1962 (S)	A	B
7.2	National Security Action Memorandum No. 201, dated October 26, 1962 (C)	A	B
7.3	National Security Action Memorandum No. 252, dated July 11, 1963 (C)	A	B
7.4	Presidential Memorandum of August 21, 1963, Subject: "Establishment of the National Communications System"	A	B
TEL-8	<u>National Communications System</u>		
8.1	<u>National Communications System Task 2</u>		
8.1.1	Executive Agent Memorandum to President, dated October 5, 1963, Subject: Establishment of the National Communications System	A	B
8.1.2	SAPT Memorandum to Sec. of Defense, dated October 28, 1963, Subject: Establishment of the National Communications System	A	B
8.2	<u>National Communications System Task 4b</u>		
8.2.1	National Communications System Long Range Plan (S)	A	B
8.2.2	SAPT letter to Executive Agent, dated June 2, 1969	A	B
8.2.3	Letter from ASD (Admin) to SAPT forwarding the Long Range Plan FY 70-74, dated December 20, 1968 (S)	A	B



Symbol	Subject and Document	Location	
8.3	<u>National Communications System Task 8</u>		
8.3.1	Private Line Circuit Restoration Priority & Message Precedence System for the NCS - Report on Task 8, NCS, dated January 17, 1964	A	B
8.3.2	SAPT Memorandum to Sec. of Defense, dated August 27, 1964, Subject: Restoration Priority & Precedence System for the National Communications System	A	B
8.4	<u>National Communications System Circulars</u>		
8.4.1	No. 55-2 -- Subject: Circuit/Trunk Directory & Data Base Format, dated August 10, 1965	A	B
8.4.2	No. 70-1 -- Subject: Operating Procedures for the National Communications System, dated June 22, 1964	A	B
8.4.3	No. 70-2 -- Subject: Technical Control Procedures	A	B
8.4.4	No. 70-3 -- Subject: Performance Objectives for the NCS, dated March 31, 1966	A	B
8.4.5	No. 130-1 -- Subject: Procedures for Processing NCS Telecommunications Circuit Requirements, dated January 24, 1964	A	B
8.4.6	No. 130-2 -- Subject: Interim Procedures for Processing NCS Emergency Telecommunications Circuit Requirements, dated January 24, 1964	A	B



Symbol	Subject and Document	Location
8.5	<u>National Communications System</u> <u>Instructions</u>	
8.5.1	No. 45-1 -- Subject: NCS Operations Center (NCSOC) Organizational Arrangements and Structure, dated July 23, 1965	A B

Whitehead

OFFICE OF TELECOMMUNICATIONS POLICY  
EXECUTIVE OFFICE OF THE PRESIDENT  
WASHINGTON, D.C. 20504

May 31, 1972

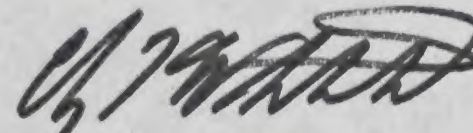
DIRECTOR

MEMORANDUM TO: Employees and Staff of the Office  
of Telecommunications Policy.

SUBJECT : Revised Security Regulations and  
Standards.

The attached order establishes a revised series of security regulations and standards for this Office. This revision is intended to conform existing agency orders and procedures to the policies and guidelines set forth in Executive Order 11652 of March 8, 1972, entitled "Classification and Declassification of National Security Information and Materials." I expect every employee and staff member to conduct himself and discharge his responsibilities in accord with the purposes of this Order.

Any questions or suggestions which you should have with respect to this Order should be referred to me directly.



CLAY T. WHITEHEAD



OFFICE OF TELECOMMUNICATIONS POLICY  
EXECUTIVE OFFICE OF THE PRESIDENT  
WASHINGTON, D.C. 20504

May 31, 1972

To: All Employees and Staff of the Office of Telecommunications Policy

From: Michael J. McCrudden

Subject: Revised Security Regulations

On March 8, 1972, as you know, the President signed an Executive Order establishing a new system of classification and declassification of Government documents relating to the national security. This new system will become effective June 1, 1972. Among its most significant features are these:

The rules for classifying documents are more restrictive.

The number of agencies and people who can originally classify information has been reduced.

Timetables ranging from 6 to 10 years have been set for the automatic declassification of documents. Exceptions will be allowed only for such information as falls within four specifically defined categories.

Sanctions may be imposed upon those who abuse the system.

These are some of the important elements of the new system established by Executive Order 11652:

1. Tighter rules for classification.

Under the new Executive Order, materials can be classified "Top Secret," "Secret," or "Confidential," only if their unauthorized disclosure "could reasonably be expected" to cause, respectively, grave damage, serious damage, or damage to the national security. Heretofore, material could be classified if the originator had any expectation of such damage, however remote. This new test is intended to reduce the amount of protected information. The Executive Order, in addition, explicitly directs that "Top Secret" classification be used with "utmost restraint," while "Secret" shall be used "sparingly."

2. Reduction in classification authority.

Under current rules, 24 Federal departments and agencies outside the Executive Office of the President have broad classification authority, while several others have more restricted powers. Under the new system, only 12 departments and agencies and 11 offices in the Executive Office of the President will have authority to originally classify information "Top Secret." Thirteen others will have authority to classify materials "Secret" and "Confidential."



In the agencies and departments concerned, the number of individuals who may be authorized to classify materials "Top Secret" is drastically reduced from 5,100 to about 1,860. This authority may be exercised only by the heads of agencies and certain high officials within the agency whom the agency head must designate in writing.

You should note that these changes in classification authority do not affect access to classified information. An individual with "Top Secret" clearance, for example, will continue to have access to "Top Secret" materials on a "need-to-know" basis, although he may not be empowered to originally classify materials "Top Secret."

Within OTP, only the Director, Deputy Director, and the Assistant Director for International Communications and Executive Direction have been authorized to originally classify information and materials "Top Secret."

Reductions in classification authority are also being made at the "Secret" and "Confidential" levels. Within OTP, only the following personnel have been authorized to originally classify information and materials "Secret:"

- Assistant Director for Frequency Management
- General Counsel
- Assistant Directors
- Program Managers (GS-16 and above)
- Executive Assistant

Other professional staff GS-13 and above have been authorized to originally classify information and materials "Confidential."

### 3. Precise identification of classified information.

A major source of unnecessary classification under the old system was the practical impossibility of discerning which portions of a classified document actually required classification. Incorporation of any material from a classified paper into another document usually resulted in the classification of the new document, and innocuous portions of neither paper could be released.

To the extent practicable, each classified document under the new system will be marked to show which portions are classified, at what level, and which portions are unclassified.

### 4. Rules for declassifying documents.

The new Executive Order establishes procedures for the downgrading and declassification of documents. Presently, aside from a small number of documents which are subject to declassification after 12 years, the vast majority of documents once classified remain so. The new system significantly changes this.



A. Documents classified after May 31, 1972.

Unless specifically exempted, all documents classified after May 31, 1972, are to be automatically downgraded and declassified. "Top Secret" information is to be downgraded to "Secret" after 2 years, to "Confidential" after 2 more years, and declassified after a total of 10 years. "Secret" information is to be downgraded to "Confidential" after 2 years, and declassified after 8 years. "Confidential" documents are to be declassified after 6 years.

Information may be exempted from this automatic process only by an official with "Top Secret" classification authority, and that official must specify in writing into which of four specific exemption categories the material falls and, where possible, he must also indicate when declassification will in fact occur. The four exemption categories are:

Classified information furnished in confidence by a foreign government or international organization;

Classified information covered by statute, or pertaining to cryptography, or disclosing intelligence sources or methods;

Classified information disclosing a system, plan, installation, project, or specific foreign relations matter, the continued protection of which is essential to the national security;

Classified information which, if disclosed, "would place a person in immediate jeopardy." The jeopardy intended here is physical harm, not personal embarrassment or discomfiture.

Upon request from anyone, including a member of the general public, exempted material is subject to mandatory review by the originating agency after 10 years from the date of origin so long as (a) the request describes the document with sufficient particularity that it may be identified, and; (b) the document can be obtained with a reasonable amount of effort.

B. Documents classified before June 1, 1972.

Essentially these same standards will be applied to materials classified prior to the effective date of Executive Order 11652. In view of their quantity, however, the 6-10 year rule for automatic declassification can only be applied to those documents already subject to a 12-year declassification order under current procedures. All others will be subject to the mandatory review process at any time after 10 years from date of origin, provided the particularity and reasonable effort tests set forth above are met.

5. Sanctions against over-classification.

Under the present system, officials frequently have found it to be in their own best interest to classify all materials of a questionable nature.

Under the new Executive Order, however, classification authority must be used with utmost restraint. In addition, the order explicitly states that information shall never be classified "in order to conceal inefficiency or administrative error . . . or prevent for any other reason the release of information which does not require protection in the interest of national security." Moreover, each agency must provide a means of identifying the classifying authority for each document and each official is to be held personally responsible for the propriety of the classifications attributed to him. Repeated abuse of the process through excessive classification shall be grounds for administrative action.

To implement the changes required by Executive Order 11652, the Director will shortly issue a substantial revision of the existing OTP security regulations. You should all take time to read these revised regulations so that you will fully understand their operations.

If you have any questions regarding these revised regulations, they should be directed to Betty Johnston (x5174) or myself.

OEP 721088



May 31, 1972

OTP Order No. 1  
Revised

## CONTENTS

### CHAPTER ONE -- PHYSICAL SECURITY

- Section 1 - Purpose and objectives.
- Section 2 - Security responsibilities.
- Section 3 - Informational briefings.
- Section 4 - Classification categories.
- Section 5 - Original classifying authority.
- Section 6 - Classification process.
- Section 7 - Identification and marking of classified material.
- Section 8 - Automatic downgrading and declassification process.
- Section 9 - Other declassification processes.
- Section 10 - Reproduction and copying of classified material.
- Section 11 - "Top Secret" material control process.
- Section 12 - Transmission of classified materials.
- Section 13 - Distribution of classified information or materials.
- Section 14 - Facilitating historical research.
- Section 15 - Custody and safekeeping of classified material.
- Section 16 - Disposal and destruction of classified material.
- Section 17 - Publications, public appearances, congressional matters, and related activities.
- Section 18 - Conferences.
- Section 19 - Public discussions and remarks.
- Section 20 - Office area and related controls.
- Section 21 - Security violations infractions.
- Section 22 - Intergovernmental liaison.
- Section 23 - Unauthorized disclosure by Government personnel.

### CHAPTER TWO -- PERSONNEL SECURITY

- Section 1 - Purpose of personnel security.
- Section 2 - Definitions.
- Section 3 - Investigative requirements.
- Section 4 - Responsibility for personnel security programs.
- Section 5 - Security clearance requirements.
- Section 6 - Security standards.
- Section 7 - Suspension and termination.
- Section 8 - Hearing.
- Section 9 - Final action in security hearing cases.
- Section 10 - Reemployment of terminated employees.
- Section 11 - Periodic security reevaluation and review.

## CHAPTER ONE -- PHYSICAL SECURITY.

### Section 1. Purpose and objectives of security.

(a) Physical security is generally concerned with the appropriate safeguarding of official information, the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage ("Top Secret"), serious damage ("Secret"), or damage ("Confidential") to the national security. The classification and safeguarding of information, however, is not for the purpose of concealing bureaucratic mistakes or preventing embarrassments to Government officials and administrations.

The lack of adequate security may result in grave international complications, serious danger to the safety of the United States, or jeopardizing the effectiveness of essential defense programs, plans, or policies. Security is designed to prevent insofar as possible the compromise of such vital information or material to avoid the potentially grave consequences thereof.

Under the previous system of classification it became clear that too many papers could be classified for too long a time. The many abuses of that security system can no longer be tolerated. Fundamental to our way of life is the belief that when information which properly belongs to the public is withheld by those in power, the people soon become ignorant of their own affairs, distrustful of those who manage them, and--eventually--incapable of determining their own destinies.

It is the policy of this Office that no information of any kind shall be unreasonably withheld from public scrutiny except to protect the national security. Accordingly, officials with classification authority are admonished and expected to discharge their responsibilities in this respect with full regard to the policies and procedures set forth in Executive Order 11652, dated March 8, 1972.

(b) An important objective of the OTP physical security program is to ensure that all persons associated with this Office know what to do to safeguard classified material, and to foster the development of responsible practices in that regard. Another objective is to assure public confidence in the ability of this Office to follow responsible information policies. A third is to ensure that OTP practices are generally in accord with Government-wide policies and practices respecting classified information handling.



These regulations provide information regarding the original classification of information and materials, the safekeeping of classified materials, the review of classified materials to assure necessary downgrading or declassification processes, document control procedures, and related matters.

Section 2. Security responsibility.

- (a) Each person employed by or serving in an official capacity with this Office is individually responsible for exercising vigilance and care in the use, handling, and safekeeping of classified information and material. Each person is responsible for providing adequate protection for classified information and materials regardless of the means by which such information is obtained.
- (b) All individuals in supervisory positions are responsible for the adequate protection of classified information and material within their areas of responsibility, and for insuring compliance with these regulations by their subordinates.
- (c) Each individual having original classification authority is personally responsible for the propriety of the classifications attributable to him. Repeated abuse of the process through excessive classification shall be grounds for administrative action.
- (d) The Security Officer of this Office is responsible for the development, installation, maintenance, inspection, and advise to the Director, on facilities, procedures, and controls for safeguarding classified information and material originating in, received by, transiting through, or in the custody of the Office. He shall maintain active training and orientation programs for employees with respect to the handling and care of classified information and materials to impress upon each employee his individual responsibility under these regulations. He will make, or cause to be made, such inspections as are necessary to insure that these regulations are administered effectively. This will include a continuing review of the implementation of these regulations to assure that no information is withheld from the public on the basis of an improper or unnecessary security classification, and that classified information is properly safeguarded.

Section 3. Informational briefings.

- (a) Each new employee upon the commencement of his or her employment shall be notified by the Personnel Office to report



to the Security Officer for an informational briefing prior to commencing his duties. At this time the employee will be given a copy of these Security Regulations, and other appropriate materials, and at this time will read and execute Form OTP 4, "Secrecy Agreement," in the presence of a representative of the Security Office. All new employees will be issued an OTP identification card.

(b) Upon termination of employment with the Office, an employee will be given an exit interview to impress upon him or her, his or her obligations with regard to maintaining the security of any classified information obtained during his service with the Office, and any applicable statutory requirements in this connection. Employees shall also be required to read and execute Form OTP 5, "Security Termination Statement," in the presence of a representative of the Security Office, and to surrender his or her OTP and all other special identification cards and account for any controlled classified material in his possession or custody.

#### Section 4. Classification categories.

(a) "Classified information and material" as used in these regulations means official information or material which requires protection against unauthorized disclosure in the interest of the national defense or foreign relations of the United States (hereinafter referred to collectively as "national security") and which is classified in one of three categories, namely, "Top Secret," "Secret," or "Confidential" depending upon the degree of its significance to national security. No other categories shall be used to identify official information or material as requiring protection in the interest of national security, except as otherwise expressly provided by statute. These classification categories are defined as follows:

- (1) TOP SECRET. "Top Secret" refers to that national security information or material which requires the highest degree of protection. The test for assigning "Top Secret" classification shall be whether its unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security. Examples of "exceptionally grave damage" include armed hostilities against the United States or its allies; disruption of foreign relations vitally affecting the national security; the compromise of vital national defense plans or complex cryptologic and communications intelligence systems; the revelation of sensitive intelligence operations, and; the disclosure of scientific and technological developments vital to



national security. This classification shall be used with the utmost restraint.

- (2) SECRET. "Secret" refers to that national security information or material which requires a substantial degree of protection. The test for assigning "Secret" classification shall be whether its unauthorized disclosure could reasonably be expected to cause serious damage to the national security. Examples of "serious damage" include disruption of foreign relations significantly affecting the national security; significant impairment of a program or policy directly related to the national security; revelation of significant military plans on intelligence, operations, and; compromise of significant scientific or technological developments relating to national security. The classification "Secret" shall be sparingly used.
- (3) CONFIDENTIAL. "Confidential" refers to that national security information or material which requires protection. The test for assigning "Confidential" classification shall be whether its unauthorized disclosure could reasonably be expected to cause damage to the national security.

(b) "Restricted Data" is a term used in connection with atomic energy matters. Section 11.r. of the Atomic Energy Act of 1954 defines "restricted data as follows:

The term "RESTRICTED DATA" means all data concerning:

- (1) Design, manufacture, or utilization of atomic weapons;
- (2) The production of special nuclear material;
- (3) The use of special nuclear material in the production of energy; but shall not include data declassified or removed from the RESTRICTED DATA category pursuant to section 142 of the Act.

"Restricted Data" may be classified "Top Secret," "Secret," or "Confidential." However, before any person may be permitted to have access to "restricted data," he or she must have a "Q" clearance from, or the special permission of, the Atomic Energy Commission. Nothing in these regulations shall be construed as superseding any requirements of the Atomic Energy Act of 1954.

"Restricted Data" shall be handled, protected, classified, downgraded in accordance with the provisions of the Atomic Energy Act and the security regulations of the Atomic Energy Commission.



Section 5. Original classification authority.

(a) The authority to originally classify information or material under these regulations shall be exercised only by the Director and such senior principal deputies and assistants as he may designate in writing.

(b) The authority to originally classify information or material under these regulations as "Secret" shall be exercised only by:

- (1) Officials who have "Top Secret" classification authority under section 5(a), above, and;
- (2) Such subordinates as the Director may designate in writing.

(c) The authority to originally classify information or material under these regulations as "Confidential" may be exercised by officials who have "Top Secret" or "Secret" classification authority, and such other subordinates as the Director may designate in writing.

(d) Original classification authority for the assignment of "Top Secret," "Secret," and "Confidential" classifications as the Director may delegate may not be redelegated.

(e) After an authorized person has decided upon the proper classification for a given document, it shall be marked in accordance with the provisions of sections 7 and 8 of these regulations.

Section 6. Classification process.

(a) Each person possessing classification authority in this Office shall be held accountable for the propriety of the classifications attributed to him. Accordingly each such person should thoroughly familiarize himself with the categories of classifications set forth in section 4, above. Both unnecessary classification and over-classification shall be avoided. Classification shall be solely on the basis of national security considerations. In no case shall information be classified in order to conceal inefficiency or administrative error, to prevent embarrassment of a person or this Office, to restrain competition or independent initiative, or to prevent for any other reason the release of information which does not require protection in the interest of national security.

(b) Cases of over-classification of OTP documents or documents originating elsewhere shall be reported to the Security Officer. If the Security Officer believes that there is unnecessary classification, that the assigned classification is improper, or that the document is subject to declassification under Executive



Order 11652, he shall so inform the originator. Repeated abuse of the process through excessive classification on the part of an employee of this Office shall be grounds for administrative action by the Director.

(c) The following rules shall be followed with respect to classification of information under this order:

- (1) Each document shall be carefully examined and classified according to its own content and not necessarily according to its relationship to other documents. Material containing references to classified materials, which references do not reveal classified information, shall not be classified.
- (2) The classification of a file or group of physically connected documents will, to the extent practicable, be marked to show which portions are classified, at what level, and which portions are unclassified. The inclusion of innocuous portions of a file under an overall "blanket" classification should be avoided insofar as practicable.
- (3) A letter of transmittal, covering memorandum, routing slip, and the like, forwarding classified documents, shall be classified only insofar as it may contain classified information and material.
- (4) Classified information or material furnished to the United States by a foreign government or international organization shall either retain its original classification or be assigned a United States classification. In either case, the classification shall assure a degree of protection equivalent to that required by the government or international organization which furnished the information or material.
- (5) In an exceptional case when a person not authorized to classify information originates information which is believed to require classification, he or she shall protect that information in the manner prescribed in these regulations, and shall transmit the information forthwith, under appropriate safeguards, to the person in this Office having both the authority to classify and a direct official interest in the subject matter with a request that a determination be made as to classification.

Section 7. Identification and marking of classified material.

(a) Each classified document shall show on its face its classification and whether it is subject to or exempt from the General Declassification Schedule, as set forth in section 8 herein. It



shall also show this Office as place of origin, the date of its preparation, and its classification, and to the extent practicable, be so marked as to indicate which portions are not classified in order to facilitate excerpting and other use.

(b) Material classified under these regulations shall indicate on its face the identity of the highest authority authorizing its classification. Where the individual who signs or otherwise authenticates a document has also authorized the classification, no further annotation as to his identity is required.

(c) Exemptions from the General Declassification Schedule may be made only by officials of this Office having "Top Secret" classification authority. In each case, such official shall specify in writing on the face of the material the exemption category set forth in section 5(B) of Executive Order 11652 being claimed and, unless impossible, a date or event for automatic declassification. The use of this exemption authority shall be kept to the absolute minimum consistent with national security requirements and shall be restricted to the following categories:

- (1) Classified information or material furnished by foreign governments or international organizations and held by the United States on the understanding that it be kept in confidence.
- (2) Classified information or material specifically covered by statute or pertaining to cryptography, or disclosing intelligence sources or methods.
- (3) Classified information or material disclosing a system, plan, installation, project, or specific foreign relation matter the continuing protection of which is essential to the national security.
- (4) Classified information or material the disclosure of which would place a person in immediate jeopardy. (The jeopardy intended here is physical harm, not personal embarrassment or discomfiture.)

(d) After a determination of the proper classification, if any, of information or materials has been made, and the requirements of subsections (a) through (c) met, where applicable, the classified items shall be marked, preferably in red, as follows:

- (1) Bound documents. The assigned classification of 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.

- (2) Unbound documents. The assigned 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 or when the document is turned face down.
- (3) Charts, maps and drawings. On classified charts, maps, and drawing, the classification shall be inserted under the legend, title block, or scale in such a manner that it will be reproduced on all copies made therefrom. The classification shall also appear at the top and bottom of the back on each chart, map, or drawing. Any required special markings shall also be applied conspicuously.
- (4) Photographs, slides, films, and recordings. Classified photographs and photographic negatives, films, and recordings and their containers shall be conspicuously and appropriately marked with the assigned classification. Clasified films and sound recordings shall contain an opening and closing statement indicating their classification.
- (5) Reproductions. All copies or reproductions of classified material shall be appropriately marked or stamped in red in the same. Reproductions of NATO, CENTO, and SEATO classified documents shall, in addition to classification be marked "Reproduced in OTP."
- (6) Unclassified material. 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 with a view towards classification and has been determined not to require such classification.
- (7) 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, and the old classification marking cancelled and the new classification, if any, substituted therefor.



- (8) Material furnished persons not in the executive branch of the Government. When classified material 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 be placed on the front cover or first page of the material, on its container, or on the written notification of its assigned classification:

NATIONAL SECURITY INFORMATION

Unauthorized disclosure subject to criminal sanctions.

- (9) Restricted Data. Any material containing "Restricted Data" will in addition to assigned classification markings, also be stamped near the marking of the classification on the front cover and title page in the following manner:

RESTRICTED DATA

This document contains RESTRICTED DATA as defined by the Atomic Energy Act of 1954. Its transmittal or the disclosure of its contents to an unauthorized person is prohibited.

or

RESTRICTED DATA  
ATOMIC ENERGY ACT--1954

- (10) Whenever originators or recipients of classified documents determine that information is contained therein which should be withheld from foreign nationals, such documents shall, in addition to the assigned classification, be stamped or marked as follows:

SPECIAL HANDLING REQUIRED, NOT RELEASEABLE  
TO FOREIGN NATIONALS.

Section 8. Automatic downgrading and declassification process.

- (a) Information and material classified pursuant to Executive Order 11652 and these regulations, unless declassified earlier by the original classifying authority shall be declassified

and downgraded after May 31, 1972 in accordance with the following rules:

(1) General Declassification Schedule.

- (A) "Top Secret." Information and material originally classified "Top Secret" shall become automatically downgraded to "Secret" at the end of the second full calendar year following the year in which it was originated, downgraded to "Confidential" at the end of the fourth full calendar year following the year in which it was originated, and declassified at the end of the tenth full calendar year following the year in which it was originated. Such documents shall be marked:

Downgraded to SECRET after \_\_\_\_\_ (date) \_\_\_\_\_

Downgraded to CONFIDENTIAL after \_\_\_\_\_ (date) \_\_\_\_\_

Declassified after \_\_\_\_\_ (date) \_\_\_\_\_.

These markings shall be in addition to any other markings required herein.

- (B) "Secret". Information and material originally classified "Secret" shall become automatically downgraded to "Confidential" at the end of the second full calendar year following the year in which it was originated, and declassified at the end of the eighth full calendar year following the year in which it was originated. Such documents shall be marked:

Downgraded to CONFIDENTIAL after \_\_\_\_\_ (date) \_\_\_\_\_.

Declassified after \_\_\_\_\_ (date) \_\_\_\_\_.

These markings shall be in addition to any other markings required herein.

- (C) "Confidential". Information and material originally classified "Confidential" shall become automatically declassified at the end of the sixth full calendar year following the year in which it was issued. Such documents shall be marked:

Declassified after \_\_\_\_\_ (date) \_\_\_\_\_.



This marking shall be in addition to any other markings required herein.

- (2) Exemptions from the General Declassification Schedule. Certain classified information or material may warrant some degree of protection for a period exceeding that provided in the General Declassification Schedule. An official of this Office authorized to originally classify information or material "Top Secret" may exempt from the Schedule any level of classified information or material originated by him or under his supervision if it falls within one of the categories set forth in section 7(c), above. Such documents shall be marked in addition to any other markings required herein as follows:

EXEMPTED FROM GENERAL DECLASSIFICATION SCHEDULE.

BY (name and position of exempting authority).

FOR (set forth in full provision of regulation on which exemption claim is based).

Declassified after (set forth date and/or event if possible).

All exempted material shall be subject to a mandatory classification review by this Office after the expiration of 10 years from date of origin provided:

- (A) A department or agency or member of the public requests a review;
- (B) The request describes the record with sufficient particularity to enable its identification, and;
- (C) The record can be obtained with only a reasonable amount of effort.

Information or material which no longer qualifies for exemption shall be declassified. Information or material determined to continue to qualify for exemption shall be so marked and, unless impossible, a date for automatic declassification shall be set.

(b) Applicability of the General Declassification Schedule to Previously Classified Material.

- (1) Information and material classified before June 1, 1972, and assigned to Group 4 under Executive Order 10501, as amended by Executive Order 10964, shall be subject to the General Declassification Schedule set forth in section 8(a)(1) above. Group 4 documents are those

documents which are marked:

Group 4  
Downgraded at 3-year intervals.  
Declassified 12 years after date  
of origin.

All such documents shall be promptly reviewed and shall be downgraded or declassified in accordance with the Schedule. For the purpose of such downgrading or declassification the date of origin of such document and not the date of issuance of these regulations shall be considered.

- (2) Information or material classified before June 1, 1972, whether or not assigned to Groups 1, 2, or 3, of Executive Order 10501, shall not be subject to the General Declassification Schedule. However, at any time after the expiration of ten years from the date of origin of any such record it shall be subject to a mandatory classification review and disposition under the same conditions and criteria that apply to information or material classified after May 31, 1972, as set forth in section 8(a)(2) above.

(c) Authority to downgrade and declassify.

- (1) Information or material originated in this Office and classified after May 31, 1972, may be downgraded or declassified at a time earlier than would be required under the General Declassification Schedule only by an official of this Office with authority to originally classify information "Top Secret." Requests for such action shall be submitted to an authorized official of this Office on Form OEP 195, "Request for Adjustment of Classification," with explicit reasons for the desired change. If an adjustment of classification or declassification is approved, the authorized official shall make such change and instruct the requesting office to notify all custodians of the documents to adjust the classification by stamping all copies on the cover or first page as follows:

CLASSIFICATION CHANGED

TO \_\_\_\_\_.

BY \_\_\_\_\_.

DATE \_\_\_\_\_.



- (2) Information or material originated in this Office or predecessor agencies and classified into Group 4 prior to June 30, 1972, may be downgraded or declassified at a time earlier than would be required under the General Declassification Schedule as made applicable to such documents by section 8(b), above, by action of the Security Officer upon appropriate request. Any such actions shall be noted by stamping on the cover or first page of such document as follows:

CLASSIFICATION CHANGED

TO \_\_\_\_\_.

BY AUTHORITY OF \_\_\_\_\_.

BY \_\_\_\_\_.

DATE \_\_\_\_\_.

- (3) Information or material originated in this Office or predecessor agencies and classified whether into Groups 1, 2, or 3, prior to June 30, 1972, may be downgraded or declassified at a time earlier than otherwise required by an official of this Office authorized to originally classify documents "Top Secret."
- (4) "Restricted Data" and material designated as "Formerly Restricted Data," shall be handled, protected, downgraded, and declassified in conformity with the provisions of the Atomic Energy Act of 1954, as amended, and the regulations of the Atomic Energy Commission.

Section 9. Other declassification processes.

(a) Declassification of classified information or material after 30 years. All classified matter which is 30 years old or more, whether originating before or after May 31, 1972, shall be declassified under the following conditions:

- (1) All information and material classified after June 1, 1972, shall whether or not declassification has been requested, become automatically declassified at the end of 30 full calendar years after the date of its original classification except for such specially identified information and material which the Director of this Office personally determines at that time to require continued protection because such continued protection is essential to the national security or disclosure would place a person in immediate jeopardy. In such a case, the Director shall also specify the period of continued classification.



- (2) All information and material classified before June 1, 1972, and more than 30 years old shall be transmitted to the Archivist of the United States, who will keep protected only such information as the Director of this Office shall specifically identify in accordance with section 9(a)(1), above.

(b) The Security Officer of this Office is authorized to declassify or downgrade any classified material in the possession of this Office which is more than 5 years old, and it appears:

- (1) that such material originated in a now defunct organization whose files and other property have not been officially transferred by statute or executive order, or;
- (2) that identification of the originating agency is impossible, and;
- (3) a review of such material indicates that the classification should be adjusted.

The Security Officer shall not exercise this authority without the concurrence of any agency or department which has, within 30 days of notice, expressed a substantial interest in the information and considerable objection to downgrading or declassifying the particular matter. In his discretion, the Security Officer may transmit such material to any nonconcurring agency or department for retention.

(c) Information or material transmitted by electrical means may be downgraded or declassified in accordance with the procedures described above unless specifically prohibited by the originating agency. Unclassified information or material which is transmitted in encrypted form shall be safeguarded and handled in accordance with the regulations of the originating agency.

#### Section 10. Reproduction and copying of classified material.

(a) Reproduction of documents includes copying in whole or in part by writing, typing, printing, mimeographing, photographing, or through thermofax, hectograph, multilith, ozalid, microfilm, photostat, xerox, or other processes.

(b) Reproduction of "Top Secret" or "Secret" information or material originating in other departments and agencies must be approved in writing in each instance by the originator or other individual in the agency having authority to approve such reproduction. The necessary approval for the reproduction of "Top Secret" information shall be obtained by the Security Officer. The requesting office will be responsible for obtaining approval for the reproduction of "Secret" material.



(c) "Top Secret" or "Secret" documents originating in this Office will be reproduced only with the approval of the classifying authority. Reproduction of "Top Secret" documents shall be processed through the Security Officer in accordance with procedures for the control of "Top Secret" documents established by these regulations.

(d) It is essential that the number of copies of classified material prepared or reproduced be kept to a minimum, since the risk of unauthorized disclosure increases in proportion with the number of copies in existence.

(e) The concurrence of the Security Officer shall be obtained when the quantity to be reproduced is 25 copies or more for "Secret" material and 75 copies or more for "Confidential" material.

Section 11. "Top Secret" material control process.

(a) The Security Officer shall be the "Top Secret" Control Officer for this Office, and he may designate Alternate "Top Secret" Control Officers.

(b) The control of all "Top Secret" documents originating in this Office and coming from other departments and agencies shall be centralized with the Security Officer. All "Top Secret" documents shall be processed through this central accountability point prior to distribution to other agencies. It is the responsibility of every custodian of "Top Secret" matter to ascertain that any individual to whom it is proposed to transmit such matter has the appropriate security clearance.

(c) The following procedures apply for the control of "Top Secret" documents within this Office:

(1) Documents originating in OTP:

(A) Upon completion of the preparation of a document and its classification as "Top Secret" by an authorized official, the originating office will contact the Security Officer and furnish the following information:

(i) Originator of the document and classifying authority;

(ii) Number of copies prepared, and;

(iii) Subject matter (unclassified).

The Security Officer will in turn assign a "Top Secret" control number for each copy of the document.

(B) Upon receipt of the control numbers, the originating office will:

- (i) Prepare and attach to each copy of the document a "Top Secret" Cover Sheet (Form OEP 73) which reflects the signature of each individual receiving the document, the date and time of receipt, and the release of the document;
- (ii) Enter the "Top Secret" control number in the right hand corner of the document and the cover sheet;
- (iii) Prepare a classified document receipt (Form OEP 162) in triplicate for each copy of the document to be transmitted to an addressee;
- (iv) One copy of the receipt will be retained by the addressee; one copy by the originator, and one copy (the hard back) will be forwarded to the Security Officer.

(C) "Top Secret" documents originating in OTP for transmittal to another agency do not require a cover sheet. The Security Officer will make any necessary inquiries to determine the security clearance of the addressee.

(D) Any subsequent transmission of any copy of the document will follow these procedures, except that a new "Top Secret" cover sheet will not be prepared. A continuous chain of signatures must be maintained on all "Top Secret" Cover Sheets.

(2) Documents originating outside OTP.

(A) All "Top Secret" documents forwarded to this Office by other departments and agencies will be received in the Security Office. The Security Officer will prepare any necessary forms and transmit the document to the addressee.

(B) If a "Top Secret" document originating in another agency is delivered to an OTP office, the receiving office will then notify the Security Officer and control the document as outlined above.



(d) The control of all material containing "Restricted Data" originating in or received by this Office is the responsibility of the Security Officer. The procedures to be followed for the control of all "Restricted Data" material will be the same as those with respect to "Top Secret" material except.

- (1) A different series of control numbers will be used to distinguish "Restricted Data" from "Top Secret" material;
- (2) All material will contain "Restricted Data" markings in addition to the usual classification markings and a "Restricted Data" Cover Sheet (Form OEP 97) will be placed on top.
- (3) In the event that "Restricted Data" material originating in this Office is directly related to the work of the Atomic Energy Commission, or was prepared as a result of "Restricted Data" material furnished to this Office by the AEC, notification of the origination of such material will be furnished to the AEC in writing by the Security Officer.

(e) All inquiries with respect to the above procedures and handling of "Top Secret" and "Restricted Data" materials will be referred to the Security Officer.

#### Section 12. Transmission of classified material.

(a) Outside OTP. Information and material classified "Top Secret," "Secret," or "Confidential" which is to be transmitted to an authorized individual outside this Office shall be double-wrapped in inner and outer opaque covers. The inner cover shall be a sealed wrapper or envelope clearly stamped at center, top, and bottom with the assigned classification of its contents, and shall be fully addressed to the authorized recipient. The outer cover shall be a sealed wrapper or envelope and shall be fully addressed including the sender's return address, but shall not be marked with a classification. All "Top Secret," "Secret," and "Confidential" information and material transmitted shall be covered by a receipt (Form OEP 162) which shall contain no classified information but shall identify the sender, addressee, and the document. This receipt shall be enclosed in or attached to the inner cover. The following regulations shall be followed in addition:

- (1) "Top Secret" information or material shall be transmitted to an authorized person outside this Office only by its custodian, a responsible member of his staff, or the Security Officer. "Top Secret" material shall never be transmitted by postal facilities, even



as registered mail. The transmittal of all "Top Secret" information and material shall be coordinated with the Security Officer.

- (2) Information and material classified "Secret" or "Confidential," when not hand-carried by the custodian or a member of his staff may be transmitted to an authorized person outside this Office by special messenger or registered mail (return receipt requested) in the 48 contiguous States, the District of Columbia, Alaska, Hawaii, Canada, the Commonwealth of Puerto Rico, or a U.S. possession. "Secret" and "Confidential" information and material may be transmitted to authorized recipients outside of these areas only by the courier mail of other Federal departments and agencies.
  - (3) "Restricted Data" information and material regardless of classification shall be transmitted only to an individual with a "Q" clearance, and in compliance with these regulations:
    - (A) "Top Secret Restricted Data" information and materials shall be prepared and transmitted outside this Office in the same manner as "Top Secret" information and material. The hardback receipt must be forwarded to the Security Officer in all cases.
    - (B) "Secret" and "Confidential" "Restricted Data" information and material shall be prepared and transmitted outside this Office in the same manner as "Secret" and "Confidential" information and material. The hardback receipt must be forwarded in all cases to the Security Officer.
  - (4) NATO, CENTO, and SEATO "Secret" and "Confidential" information and material shall be prepared and transmitted outside this Office in the same manner as U.S. "Secret" and "Confidential" information and material.
- (b) Within OTP.
- (1) "Top Secret" information and material shall be placed in a single opaque envelope and hand-carried by the custodian thereof, or a responsible member of his staff, having a "Top Secret" security clearance. In the course of such transmittal, a receipt for the "Top Secret" document is required and the transfer shall be coordinated with the Security Officer.



- (2) "Secret" and "Confidential" information may be transmitted by the custodian, a member of his staff, or an authorized Office messenger. Material shall be placed in a single opaque envelope. The use of a classified receipt is optional with the sender.
- (3) Information and material containing "Restricted Data" shall be hand-carried in an opaque envelope by an authorized person who has been granted Class "Q" clearance, and shall be transmitted only to an individual with Class "Q" clearance, A receipt is required for all "Restricted Data" material.
- (4) A receipt (Form OEP 162) is required for all transmissions within this Office of information and material classified NATO, CENTO, and SEATO "Secret".
- (c) "Dispatch Instructions" (Form OEP 92) shall be used as an instruction to the messengers and mail room in the handling of "Secret" and "Confidential" material. This form is to be used only when classified mail is being transmitted. It is not a receipt and should not be used in lieu of a receipt. The form is to be stapled or securely affixed to the outer envelope in which classified mail has been placed.

Section 13. Distribution of classified information or materials.

- (a) A person is entitled to have knowledge or possession of classified information or material only when his or her official duties require such knowledge or possession. An individual is not authorized to gain classified information or material merely by virtue of his position or degree of security clearance. It is imperative that classified information or material receive absolute minimum distribution and that such information and material be given only to those employees who deal directly with the subject matter of the classified material involved. The "need-to-know" doctrine shall be enforced at all times in the interest of good security. No employee of this Office shall release any classified information or material to any person outside this agency without establishing the "need-to-know", and determining the extent to which that person is cleared to receive classified material.
- (b) The distribution and accounting of all "Top Secret" documents shall be in accord with the "Top Secret" Control Procedures set forth above.
- (c) An inventory of all "Top Secret" and "Restricted Data" documents shall be submitted to the Security Officer on the last working day in March of each year, current as of the



close of business of that date. Documents shall be listed by the OTP control number and separate lists prepared for each staff member having custody of such documents.

- (d) Each office shall be responsible for the complete accountability of incoming and outgoing documents classified "Secret". For this purpose, all custodians of classified material shall maintain a document control log which will be inspected periodically to determine that records are being properly maintained.
- (e) Classified information and material originating in this Office shall not be sent to other Federal Agencies or employees thereof except by a signed letter of transmittal, and in compliance with these regulations.
- (f) Classified information and material originated in another agency and in the custody of this Office shall not be disseminated or distributed to a third agency or any employees thereof without the consent of the originating agency.
- (g) Requests from State or municipal agencies, private firms and corporations, educational institutions, private individuals or other non-Government persons for classified information shall be referred to the Security Officer. Such requests shall meet the following requirements and be processed the following manner:
  - (1) The request shall describe in writing the classified document with sufficient particularity to enable this Office to identify it and to obtain or otherwise retrieve it with only a reasonable amount of effort.
  - (2) Requests for classified documents made at any time after the expiration of ten years from date of origin of such documents shall be deemed a request for a mandatory classification review pursuant to section 5(C) of Executive Order 11652 and these regulations. The Security Officer shall promptly take such steps and initiate such action as may be necessary to accomplish such a classification review.
  - (3) Documents which, as a result of such review are determined to no longer warrant classification shall be promptly declassified in accordance with these regulations and transmitted to the requesting person forthwith.
  - (4) Documents which are determined to warrant continued classification, and other documents to which mandatory



classification review procedures are not applicable, shall be released to non-Government persons only upon the following determinations by the Security Officer:

- (A) That the classified document or information will be accessible only to persons having the proper degree of security clearance;
  - (B) That adequate facilities will be available for the proper safeguarding of the classified material;
  - (C) That the requesting person has a "need-to-know" such classified information and that access thereto would not be inconsistent with national security interests.
- (5) Classified information and material, whose dissemination or distribution has been approved shall be prepared and stamped prior to distribution in the manner prescribed in these regulations.

Section 14. Facilitating historical research.

Notwithstanding the provisions of section 13, above, access to classified information or material may be granted to persons outside the executive branch who are engaged in historical research projects or who have previously occupied policy making position in Government to which they were appointed by the President; provided, however, that in each case the Director of this Office shall:

- (a) determine that access is clearly consistent with the interests of national security, and;
- (b) take appropriate steps to assure that classified information is not published or otherwise compromised.

Access granted a person by reason of his having previously occupied a policy-making position shall be limited to those papers which the former official originated, reviewed, signed, or received while in public office.

This section shall have no application to "Restricted Data" or "Formerly Restricted Data" insofar as access to such materials may be granted only by the Atomic Energy Commission.

Section 15. Custody and safekeeping of classified material.

- (a) These regulations impose upon the employees of this Office the responsibility for the proper protection and safekeeping

of classified information and material in their custody. When an official entrusts the custody of classified matter to a subordinate he shall not consider himself relieved of responsibility to insure that the material is properly safeguarded. The safeguarding of classified information and material refers to the physical or mechanical security measures taken to protect such material both during and outside working hours.

- (b) All work on classified information and material must be performed in offices where facilities for secure storage and protection are available. Persons having custody of classified documents shall not remove them from the areas of this Office except for the purpose of attending official meetings or transmittal to authorized persons in accord with these regulations. Under no circumstances shall any classified material be removed to living quarters without the express prior permission of the Director.
- (c) The storage of classified material shall be as follows:
  - (1) "Top Secret" and "Secret" material shall be protected by storage in the most secure facilities possible. Normally such classified material will be stored in a safe or 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 any possibility of surreptitious entry, physical theft, damage by fire, or tampering.
  - (2) "Confidential" material may be stored in the manner required for "Top Secret" and "Secret" material, above, or in a steel file cabinet, equipped with a lockbar and an approved three-position, dial-type combination padlock.
  - (3) "Restricted Data" shall be stored in the manner proscribed for "Top Secret" and "Secret," above.
  - (4) When an office is in possession of classified material of such size, quantity, or bulk that the material cannot be adequately stored, the matter shall be referred immediately to the Security Officer. Such material to be stored must be properly labeled in order to prevent accumulation of material and to insure return to the proper individual or office.



(d) Requests for proper safekeeping equipment shall be coordinated with the Security Officer. The Security Officer will survey and evaluate the security requirements of a requesting office and authorize the issuance of safekeeping equipment as required.

(e) Defects or malfunctioning of safekeeping equipment or locking devices shall be reported immediately to the Security Officer and any necessary repairs or replacements made promptly.

(f) Combinations to safekeeping equipment shall be changed under the following circumstances but in any event no less frequently than once a year:

- (1) Whenever such equipment is placed in use after procurement from the manufacturer or other sources, or;
- (2) Whenever any person knowing the combination to such equipment severs his connection with the office in which the safe is located, or;
- (3) Whenever there is reason to believe that the combination to such equipment has been compromised, or;
- (4) For any other reason necessitating the changing of a combination in the interest of good security.

(g) Records of combinations shall never be classified lower than "Secret," and shall be classified "Top Secret" when material of that category is contained in a safe. Combinations to safekeeping equipment containing classified material shall never be discussed over the telephone except in an extreme emergency, after which the circumstances shall be reported to the Security Officer, and the combination to such equipment shall be changed immediately. Combinations must be committed to memory and no written record thereof kept without the express permission of the Security Officer. The Security Officer shall maintain a master record of combinations for all safekeeping equipment in this Office.

(h) The number of individuals having knowledge of the combination to safekeeping equipment shall be limited to the minimum consistent with operating efficiency and in any event should not normally exceed three persons.

(i) An appropriate sign marked "Open" and provided by the Security Officer shall be displayed on every piece of safekeeping equipment containing classified material when unlocked. When such equipment is locked the sign should be reversed to show "Locked." The utilization of these signs provides a very effective visual warning and reminder to responsible employees to assure that safes are locked and secured at the close of each day, or during unguarded periods.



(j) Security inspectors will make inspections periodically after working hours, on weekends, and holidays, to ascertain and assure that all regulations for the safekeeping of all classified materials are properly observed. The following procedures shall apply:

- (1) If a safe or file cabinet containing classified material is found unlocked, a violation card will be placed immediately on the safe or cabinet, the equipment shall be secured, and the Security Officer notified.
- (2) Classified information or material found outside safekeeping equipment by security inspectors will be locked in the safe provided for such material in the Security Office. A violation report shall be filed, and will reflect that the classified matter involved has been placed in that safe.
- (3) If a safe is found unlocked by a security inspector, and such safe contains "Top Secret" material, an inventory of all "Top Secret" and "Restricted Data" documents in that office must be submitted to Security Officer by the close of business the following working day.
- (4) A written report with respect to security violations of this nature, and the details of the action taken shall be made to the Security Officer for appropriate action.

Section 16. Disposal and destruction of classified material.

(a) Documents and other record materials originated or received by this Office in connection with the transaction of public business and preserved as evidence of the organization function, policies, operations, decisions, or activities of this Office or 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 44 U.S.C. §§3301-314. These provisions generally require congressional authorization for such destruction through the Archivist of the United States. All proposals for the destruction of such records and materials shall be submitted to the Security Officer.

(b) Nonrecord classified material, consisting of extra copies and duplicates may be destroyed in the manner prescribed below, providing that appropriate accountability records are maintained:



- (1) "Top Secret" material to be disposed of shall be returned by the custodian to the Security Officer with a letter or memorandum in duplicate requesting destruction. The letter or memorandum shall include:  
(a) control numbers of the documents; (b) title or subject matter; (c) justification for destruction. The accountability records of the Security Officer will reflect the destruction of each "Top Secret" document.
- (2) "Secret" and "Confidential" documents shall be destroyed by the custodian thereof. A report of destruction covering each "Secret" document shall be maintained in the custodian's files for a period of 3 years. The disposition column of the classified log shall reflect the destruction for record purposes and must be initialed by the person making the entry.
- (3) All "Secret" NATO, CENTO, SEATO, and "Restricted Data" documents will be returned to the Security Officer for destruction with a signed request for disposal listing control numbers, titles, and document dates. "Confidential" NATO, CENTO, and SEATO documents will be returned to the Security Officer but no listing thereof need be made.
- (4) All classified material to be destroyed shall be torn into small pieces and placed in "Burn" bags (obtainable from the supply room). "Burn" bags awaiting destruction or partially-filled "Burn" bags shall be stored in a manner affording protection commensurate with the classification of information and material contained therein.
- (5) Filled "Burn" bags shall be sealed by stapling and will be collected periodically by authorized personnel designated by the Administrative Office. "Burn" bags will then be destroyed by incineration under the supervision of the Security Officer.
- (6) Records of destruction are not required for classified work sheets, carbon paper, stenographer's notes, stencils, unshaved cylinders, typewriter ribbons, dictabelts and other sound recordings, but such materials shall be appropriately safeguarded until their destruction.



Section 17. Publications, public appearances, congressional hearings, and outside activities.

(a) No employee of this Office shall publicly make a speech, write for publication, or give a public course of instruction dealing with, or closely related to classified information available to him in the course of his employment, except upon the prior authorization of the Director. A written request for such authorization should be addressed to the Security Officer stating the time and place of the proposed activity. The request should include, as applicable, a copy of the actual text of the address or publication or a brief outline of the proposed course of instruction. When it has been determined that there will be no unauthorized disclosure of classified information, the authorization will be granted. The final responsibility that classified information and material will not be revealed to any unauthorized person, however, rests with the employee concerned.

(b) Any employee of this Office who is requested to appear before any congressional committee or subcommittee, or to testify in any judicial or quasi-judicial tribunal, shall notify the Director in writing of the circumstances surrounding the request prior to making any such appearance or giving such testimony. Whenever such appearance or testimony may involve the disclosure of any classified information or material, the notification will also include, insofar as possible, the nature of such information. A copy of this notification shall be forwarded to the Security Officer. In such cases, the Director or his delegate will request that any testimony involving classified information or material be taken in executive session and not appear in the record of hearings or other publicly available documents.

(c) The Attorney General has issued a list of foreign and domestic organizations, associations, movements, and groups or combinations of persons which have been designated as totalitarian, fascist, communist, or otherwise subversive. In order to avoid criticism or embarrassment, employees of this Office should consult the Security Officer whenever there is any doubt as to the true character of any organization by which they are approached for speaking engagements, membership, endorsement, contributions, or for any other reason.

Section 18. Conferences.

(a) In conducting conferences with employees of this Office, or other departments, agencies, or organizations, in which classified information or material may be involved, every precaution shall be observed to insure that all participants are entitled to receive information of the level of classification involved. All participants at such meetings must have appropriate security classifications whether they are Government employees or nongovernment employees.



(b) As early as possible in advance of a meeting in which classified information or material may be involved, a complete list of participants and alternates will be compiled and forwarded to the Security Officer, together with the classification of the subject matter to be discussed. The Security Officer will determine in advance of the meeting whether the proposed participants are authorized to receive information of the classification level indicated and notify those in charge of the meeting of his determinations. It is the responsibility of the office sponsoring the meeting to verify that clearances have been received before the conference or meeting convenes.

(c) During the course of the conference or meeting, distribution of any classified documents shall be kept to the minimum consistent with good security. Whenever possible, classified documents shall be collected prior to adjournment. If it is believed desirable for participants to retain any classified documents, a record will be kept listing the identity of the documents, the number of copies, and the names of the persons permitted to retain them. A copy of such list shall be maintained by the employee of this Office responsible for the custody of the documents. Prior to distribution for retention, it should be determined that the recipient has proper storage facilities available. Verification of a facility clearance is required prior to the release or transmission of any classified information or material to representatives of private industry in attendance at conferences or meetings.

(d) Before adjournment of any conference or meeting, agreement shall be reached on the proper classification of the minutes and individual notes of the meeting. Participants will be reminded regarding their responsibility for the proper safeguarding of classified information or material.

(e) Following adjournment, it shall be the responsibility of the office sponsoring the conference or meeting to see that all notes and other papers left as waste are collected and placed in a "Burn" bag for destruction.

(f) All employees of this Office scheduled to visit another facility, Government agency, international organization, or foreign government for the purpose of classified briefings or meetings which require clearance certification, must notify the Security Officer as far in advance of such meeting as possible. This notice will include: (1) the name and address of the facility, Government agency, international organization, or foreign government; (2) the date or dates of the visit; (3) the purpose of the visit; (4) the person or persons to be visited, and; (5) the security clearance required.



Section 19. Public discussions and remarks.

(a) Classified information or material shall not be discussed with, or within the hearing of, unauthorized persons, or persons with no need to know such information. Discussions of classified information in homes, with relatives or friends, in public places, or in public conveyances is strictly prohibited.

(b) Regular telephones shall not be used for the purpose of discussing any classified information or material. The presumption is that conversations over ordinary telephones, mobile telephones, or interoffice communications equipment will be overheard by unauthorized persons. The use of telecopiers or facsimile devices, telex, or TWX machines for the transmission of classified information or materials being similarly amenable to unauthorized interception is strictly prohibited.

The transmission of classified information or materials over telephone circuits is permitted only over the secure telephone equipment maintained in the Office's Telecommunications Information Center. Information and authorization respecting the use of this secure equipment may be obtained from the Security Officer.

(c) The initiation of a conversation involving classified information or material by a party on the other end of a telephone conversation does not relieve the recipient of responsibility in a prohibited conversation unless he immediately warns the talker of the infraction and terminates the conversation if the infraction persists.

Section 20. Office area and related controls.

(a) Effective security is largely a matter of proper habits. Daily operations should be performed in a manner which will encourage good security practices to become routine. These procedures shall be followed:

- (1) Offices in which classified documents are in use shall never be left unattended at any time during the working day unless classified information and material has first been locked in proper safekeeping equipment.
- (2) The custodians of classified information or materials must follow procedures that prevent access by sight or sound to such information by unauthorized persons. When an employee is working on classified information or materials and a visitor enters, care will be exercised not to leave classified documents exposed to observation. At such time, classified documents shall be turned face down on the desk, or placed in proper safekeeping



equipment. The visitor shall not be left alone even for a brief interval where classified documents are unprotected. Similar precautions will be observed when repairmen, maintenance, or other service personnel enter an office.

- (3) "Burn" bags shall be used only for classified waste, and waste baskets used only for unclassified waste. Partially filled "Burn" bags shall be stored overnight in safes or locked files which will afford proper protection as prescribed earlier. Stenographic notebooks, used carbons, paper or carbon typewriter ribbons, stencils, dictabelts and similar dictating machine recordings and tapes, individual notes, drafts, and outlines utilized in the preparation or use of classified information or material shall be stored and safeguarded at the end of the work day in the same manner as the finished classified products or the classified information from which they derive.
- (4) Each office shall institute a system of security checks to be made in each organizational unit at the close of each working day. The person conducting the security check shall see that all classified material has been properly secured, that safes and file cabinets are securely locked, and that desks, table tops, "In" and "Out" trays and the tops of filing equipment are free of classified information or material. Employees who work on weekends or holidays will be responsible for the security of the office area at that particular time.
- (5) When classified information or material is found not properly safeguarded, or when repositories are found not to have been secured, the person making the inspection shall transmit a memorandum the following day to the Security Officer, stating the nature and scope of the violation, the person or persons apparently responsible, and any other pertinent information. The person performing the after-hours security check shall be held accountable for any violation discovered after his or her check. Loose classified material found unsecured as a result of a security check will be deposited in a safe until turned over to the Security Officer.

(b) All employees of this Office are required to present identification passes to building guards, and to sign a register when entering or leaving the building outside normal working hours, on weekends, or on holidays. In the event an identification card is lost, a memorandum shall be submitted immediately to the Security Officer, detailing the circumstances of such loss, and any efforts made towards recovery.



(c) Fire is an ever-present security hazard for classified information or material. In case of fire, employees shall observe the following precautions:

- (1) Upon discovery of fire, an alarm shall be sounded except when the fire can be extinguished without assistance.
- (2) If the building fire alarm rings, employees will immediately store classified information or material in proper safekeeping equipment and secure all safes and file cabinets. Compliance with evacuation procedures as specified in the "Facilities Self-Protection Plan" will be expected.

Section 21. Security violations and infractions.

(a) All reports of security violations shall be promptly directed to the attention of the Security Officer. It is the responsibility of each employee having knowledge of any type of security violation to immediately report such facts. Experience has shown that the results of corrective action are more effective when violations are reported immediately. In any instance where there is a possibility of the compromise of classified information or material as a result of the violation it is imperative that this be reported immediately in order that appropriate remedial action may be taken. Violations of security regulations may result in disciplinary action against employees, depending upon the nature and number of violations. Such adverse actions may include:

- (1) Letter of reprimand;
- (2) Suspension without pay;
- (3) Dismissal.

In the case of a serious violation, an employee may be subject to immediate suspension or dismissal even though no previous security violation has been reported. It should be borne in mind that repeated security violations, even though not serious enough to result in formal disciplinary action, may have a significant effect upon an individual's promotion and reassignment opportunities.

(b) The unnecessary classification and over-classification of information or materials by an officer or employee of this Office with classification authority may also be grounds for adverse administrative action. Repeated abuse of the classification process shall be grounds for an administrative reprimand. If in any case the Security Officer should find unnecessary classification or over-classification has occurred, he will make a report to the Director in order that corrective steps may be taken.



Section 22. Intergovernmental liaison.

(a) All liaison functions pertaining to security matters or having security implications will be the responsibility of the Security Officer. Such liaison includes liaison with other Federal Government departments, agencies, and establishments, and with State, local, or municipal investigative or law enforcement organizations. All certifications of security clearances with respect to employees or staff of this Office will be made by the Security Officer or his designated representatives.

(b) Employees of other agencies seeking to discuss security matters, or individuals offering information of security significance will be referred promptly to the Security Officer.

(c) The Security Officer will be consulted regarding the interpretation of security regulations, personnel security problems, physical security of office areas, and any other security matters which may arise.

Section 23. Unauthorized disclosure by Government personnel.

The Director of this Office is directed by section 13(B) of Executive Order 11652, to take prompt and stringent administrative action against any officer or employee of this Office, at any level of employment, determined to have been responsible for any release or disclosure of national security information or material in a manner not authorized by or under Executive Order 11652 and these regulations, or a directive of the President issued through the National Security Council. Where a violation of criminal statutes may be involved, the Director will refer any such case promptly to the Department of Justice.

## CHAPTER TWO -- PERSONNEL SECURITY REGULATIONS.

### Section 1. Purpose of personnel security.

Personnel security is generally concerned with insuring that all persons privileged to be employed by or officially associated with this Office are reliable and trustworthy, of good conduct and character, of complete loyalty to the United States, and that, accordingly classified national security information or material may be entrusted to them without risk.

### Section 2. Definitions.

For the purposes of this chapter, unless the context otherwise requires--

(a) "Sensitive position" means any position in this Office the occupant of which could bring about a material adverse effect on the national defense or foreign relations of the United States (hereinafter collectively termed "national security") because of the nature of his or her position.

(b) Sensitive positions shall be divided into two categories:

(1) "Critical-sensitive positions" are those positions designated by authority of the Director which involve:

- (A) Access to "Top Secret" national security information or material, or;
- (B) Development or approval of war plans, plans or particulars of future or major or special operations of war, or critical and extremely important items of war, or;
- (C) Development or approval of plans, policies, or programs which affect the overall operation of this Office (policy-making or policy-determining positions) or;
- (D) Investigative duties including the issuance of personnel security clearances, or duty on personnel security boards, or;
- (E) Fiduciary, public contact, or other duties, demanding the highest degree of public trust.

(2) "Noncritical-sensitive positions" are those positions designated by authority of the Director which would require access to "Secret" or "Confidential" classified information or material and which do not meet the criteria set forth in (1) above.



Section 3. Investigative requirements.

(a) Critical-sensitive positions. A full field investigation shall be conducted on all persons being considered for such positions. The background investigation shall be conducted and based upon a favorable determination, a "Top Secret" clearance will be granted by the Security Officer of this Office prior to appointment. However, when not feasible in case of an emergency, the requirement for a full field investigation prior to appointment may be waived as provided by section 3(b) of Executive Order 10450, as amended. In the event that such a waiver has been approved by the Director, it shall be made a matter of record in the individual's security and personnel file, and the background investigation shall be initiated within 3 working days after the individual's entrance on duty. Such an appointment will be limited to 90 days pending satisfactory completion of the investigation.

(b) Noncritical-sensitive positions. A National Agency Check and Inquiry (NACI) shall be completed on all persons prior to their appointment to a noncritical-sensitive position in this Office. This NACI, however, should not be construed to preclude the Director from initiating a full field investigation on any applicant or employee when he may consider such action appropriate.

Section 4. Responsibility for personnel security programs.

The Security Officer will be responsible to the Director for the effective administration of the personnel security program prescribed herein, and will provide staff assistance and perform such other functions as may be required to implement these regulations.

Section 5. Security clearance requirements.

The Director has prescribed that a security clearance is a prerequisite to employment in this Office or for access to classified information or material. The specific requirements are as follows:

(a) No person shall be employed, or retained as an official or employee of this Office unless the employment or retention of such an individual is clearly consistent with national security interests.

(b) No position in this Office will be filled or occupied unless the person to fill or occupy the position has been the subject of an NACI or a full field investigation. When not feasible in case of an emergency, the requirement for a full field investigation prior to appointment may be waived as provided by section 3(b) of Executive Order 10450, as amended. In the event that such waiver is approved, a background investigation



will be initiated no later than 3 working days after the individual's entrance on duty. Such an appointment will be limited to 90 days pending satisfactory completion of an investigation. No waiver or exception to a preappointment security clearance will be made without specific authorization of the Director. In such a case, the waiver action will be made a part of the personnel and security file of the person concerned. No definite commitment shall be made by any other official or employee of this Office to any applicant for any position before the appropriate security clearance has been obtained.

(c) If a full field investigation of an employee, applicant, or individual officially associated with this Office results in a favorable determination with respect to the loyalty, integrity, and general suitability of the person, the Security officer will grant a security clearance to such person, permitting access to security information classified "Confidential," "Secret, and "Top Secret" on a need-to-know basis.

(d) Atomic Energy "Q" clearance is an additional security clearance obtained from the Atomic Energy Commission for those employees whose duties require access to "Restricted Data" as defined by the Atomic Energy Act of 1954. All such cases will be handled by the Security Officer, who will furnish the AEC with a justification setting forth the reasons why an employee's duties require access to "Restricted Data."

(e) NATO, SEATO, CENTO, and "Cryptographic" access clearances may be issued by the Security Officer to those employees whose duties require access to such classified information or material.

(f) Members of certain advisory committees and other groups advisory to this Office are required to have appropriate security clearances in accordance with the provisions of these regulations and Executive Order 10450, as amended.

(g) When an employee of a contractor to this Office, or a special Government employee, requires access to classified information or material, the Security Officer shall make a security evaluation. If his security evaluation conflicts with a comparable security evaluation made by another Government agency, the Security Officer shall meet within 15 days with appropriate representatives of such agency or agencies in order to resolve the conflict. The results of this interagency consultation shall be effective when approved by the Director in writing, and will be recorded in the Security Office files.

(h) In general, positions to which Executive Reservists are assigned shall be considered as "critical-sensitive" positions. Designations of Executive Reservists shall not be approved until a "Top Secret" security clearance has been processed and granted in conformance with these regulations.



Section 6. Security standards.

(a) Information regarding an applicant for employment, or an employee of OTP, which may preclude a finding that his or her employment or retention in employment is clearly consistent with national security interests shall relate, but not be limited to the following:

- (1) Depending upon the relationship of the Government 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 omissions of material facts;
  - (C) Any criminal, infamous, dishonest, immoral, or notoriously disgraceful conduct, habitual use of intoxicants to excess, drug addition, sexual perversion, or financial irresponsibility;
  - (D) An adjudication of insanity, or treatment for serious mental or neurological disorder without satisfactory evidence of cure;
  - (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 national security.
- (2) Commission of any act of sabotage, espionage, treason, or sedition, or attempts thereat, 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 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 alteration of the form of government of the United States by unlawful means.
- (4) Advocacy of use of force or violence to overthrow the Government of the United States, or of alteration of the form of government 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 classified information disclosure of which is prohibited by law, or willful violation or disregard of security regulations.
- (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.

(b) Whenever in the course of an investigation of an employee or job applicant of this Office information is developed relating to any of the matters set forth in subparagraphs (2) through (7), above, or information indicates that an employee has been subject to coercion; influence, or pressure to act contrary to the best interests of national security, such information shall be referred to the Department of Justice for full investigation.

(c) All information indicating that the retention in employment of an employee of this office may not be clearly consistent with national security interests shall be referred promptly to the Security Officer.

(d) All reports of investigation shall be evaluated by the Security Officer, who will make such inquiries of the employee concerned or others as he deems necessary to determine whether to recommend to the Director the suspension or retention of the employee.

#### Section 7. Suspension and termination.

(a) The Director of this Office is authorized by Executive Order 10450, and 5 U.S.C. §§7531-32 to suspend employees of this agency when deemed necessary in the interests of national security.

(b) Upon receipt of an investigative report containing derogatory information relating but not limited to any of the matters set forth in section 6, above, the Security Officer will promptly evaluate such report from the standpoint of Office security. After consultation with the General Counsel, the Security Officer shall report his findings, conclusions, and recommendations to the Director.



(c) Upon receipt of the report of the Security Officer, the Director will make a determination as to the need for suspension of the employee in the interests of national security. If the Director determines that suspension is necessary, the employee shall be suspended immediately and shall be so notified in writing as promptly as possible. To the extent that the Director determines that the interests of national security permit, the suspended employee shall be notified of the reasons for his suspension.

If the Director determines that suspension is not necessary, a written determination to that effect shall be made a part of the investigative file of the individual concerned.

(d) Factors to be taken into consideration in making the determination required by (c), above, shall include but shall not be limited to:

- (1) the seriousness of the derogatory information involved;
- (2) the possible access, both authorized and unauthorized of the employee to classified information or material, and;
- (3) the opportunity by reason of the nature of his or her position for the employee to commit acts adversely affecting the interests of national security.

#### Section 8. Hearing.

(a) Procedure with respect to a person entitled to a hearing. Any employee suspended pursuant to 5 U.S.C. §7532 and section 7, above, who

- has a permanent or indefinite appointment;
- has completed his probationary or trial period, and;
- is a citizen of the United States;

is entitled, after suspension and before removal to:

- (1) A written suspension notice advising him or her--
  - (A) that within 30 days after receipt of the suspension notice he or she is entitled to submit to the Security Officer statements or affidavits to show why he should be restored to duty;
  - (B) that within 30 days after the actual date of his or her suspension he shall be furnished a statement of the charges against him stated as specifically as security considerations permit;



- (C) that the statement of charges may be subject to amendment within 30 days of its date;
  - (D) that at any time within 30 days after he or she receives the statement of charges, or at any time within 30 days after he or she receives any amendment to the statement of charges he or she has the right to submit to the Security Officer for consideration any statements in writing or affidavits he may care to execute, or any statements in writing or affidavits of other persons, or any documents which refute or explain any or all of the charges against him.
- (2) a hearing at his or her request made within the time specified above for the submission of statements, affidavits, and documents, before a Security Hearing Board, unless he has been reinstated;
  - (3) a review of his case by the Director of this Office or his designee before a decision adverse to the employee is made final, and;
  - (4) a written statement of the decision by the Director of this Office.
- (b)
- (1) Prior to the issuance of any statement of charges, the General Counsel, after consultation with the Security Officer, shall consult with the Department of Justice concerning the legal aspects of the proposed statement of charges and the procedures to be followed subsequent to the issuance of that statement.
  - (2) Upon receipt of an employee's statements, affidavits, or documents filed pursuant to (a), above, the Security Officer and the General Counsel shall consider them, and make a joint recommendation to the Director. If the General Counsel and the Director are in disagreement they shall make their recommendations separately.
  - (3) On the basis of the recommendation or recommendations of the General Counsel and the Security Officer, the Director, upon review may--
    - (A) order reinstatement: If he finds that reinstatement of the suspended employee to the position from which he or she has been suspended is clearly consistent with the interests of national security, the Director may restore the employee to duty and provide that he or she be compensated for the period of suspension. In any such case, a written determination to that effect shall be made a part of the employee's security file.



- (B) direct that a hearing be held: If he finds that reinstatement of the suspended employee would not be consistent with the interests of national security, and that a request for a hearing has been timely filed, the Director may order such hearing held.
- (C) order reinstatement pending the results of a hearing: If the Director finds that reinstatement pursuant to (A) may be warranted and that a hearing pursuant to (B) is necessary, he may order reinstatement pending result of such a hearing, provided, however only when extraordinary conditions may make such action necessary.

(c) Procedures with respect to a person not entitled to a hearing. Any employee suspended pursuant to 5 U.S.C. §7532 and section 7, above, who

- is an alien;
- a temporary or probationary appointee, or;
- in a trial period status;

is entitled to:

(1) a written suspension notice:

- (A) stating the specific reasons for his suspension, to the extent that the Director determines the interests of national security permit, and;
- (B) advising him that within 30 days after his receipt of this written notice he has the right to submit to the Security Officer for consideration any statements in writing or affidavits he may care to execute, or any statements or affidavits of other persons, or any documents which refute or explain any or all the reasons for suspension given the employee in the notice or otherwise show why he should be restored to duty.

(d) (1) Such statements, affidavits, or documents as the employee may submit, together with the employee's investigative file, shall be considered by the Security Officer and General Counsel, who shall make a recommendation to the Director. If the Security Officer and General Counsel disagree, they shall make individual recommendations.

(2) On the basis of the recommendations or recommendations of the Security Officer and the General Counsel the Director will determine:

- (A) If reinstatement of the suspended employee in the position from which he has been suspended is clearly consistent with the interests of national security, in which case he shall be restored to duty and compensated from the period of suspension, or;
- (B) If reinstatement of the suspended employee to his prior position is not clearly consistent with the interests of national security, in which case the employment of the employee shall be terminated, he or she shall be given a written notice of termination, and the Civil Service Commission notified thereof. Such determination by the Director shall be final.

(e) Security Hearing Boards.

- (1) The Security Hearing Board, in any case involving an employee entitled to a hearing, shall be composed of not less than 3 civilian employees of the Federal Government selected by the Director from rosters maintained for that purpose by the Civil Service Commission. The General Counsel of this Office shall not act as prosecutor but shall aid the Board in its procedural determinations and will participate where necessary in the examination of cross-examination of witnesses.

The employee shall have the right to be represented by counsel of his or her own choosing. In the event that the employee does not retain outside counsel, the General Counsel will appoint a qualified member of his staff to advise the employee of his rights before the board and to assist him in his defense.

- (2) Proceedings before the Security Hearing Board shall be conducted in an orderly manner, and in a serious, business-like atmosphere of dignity and decorum. Proceedings shall be expedited to the extent consistent with the rights of the employee and the ends of justice.
- (3) Proceedings of the Board shall be private except as the Director may direct upon the request of the employee. No persons except members of the Board, a stenographer, the employee and his counsel, if any, the General Counsel and his designee, if any, shall be present. Witnesses shall be present at the hearing only when actually giving testimony.



- (4) Testimony before the Board shall be given under oath or affirmation, administered by an official authorized to administer oaths.
- (5) The Board shall conduct and control its proceedings in such a manner as will fully protect any information relating to the national security from unauthorized disclosure. In questions regarding the disclosure of classified information or materials, the Board will consult with the Security Officer and comply with his determinations.
- (6) The Board will take whatever actions it determines necessary to insure the employee full and fair consideration of his case, and to that end the Board will inform him or her of his or her rights including the right:
  - (A) to participate in the hearing;
  - (B) to be represented by counsel of his own choice;
  - (C) to present witnesses and to offer other evidence on his behalf, and in refutation of all or any part of the charges brought against him;
  - (D) to control the sequence of witnesses that may be called by him;
  - (E) to cross-examine any of the witnesses offered in support of the charges;
  - (F) to a copy of the transcript of the hearing without charge upon request.
- (7) The Security Hearing Board, in its discretion, may invite any person to appear and testify if it believes such person can materially assist the Board in reaching a fair and just determination. The Board shall not be bound by such testimony by reason of having called any person, and shall have the right fully to cross-examine such person.
- (8) Hearings shall be opened by the reading of the statement of charges against an employee, and unless waived, statements, affidavits, and other documents which the employee may have submitted. Both the employee and this Office may introduce such evidence as either party may deem proper. Formal evidentiary rules shall not be binding on the Board, but reasonable restrictions shall



be imposed to assure the relevance, materiality, and competency of any matters submitted for consideration. Due consideration shall also be given to documentary evidence developed by investigation. The fact that such evidence has been introduced for consideration shall be made a part of the transcript of the hearing.

- (9) Following the conclusion of the hearing, the Board shall make and render its decision in writing. That decision shall be based upon the entire record in the case.
- (10) The decision of the Security Hearing Board shall be by a majority vote, in writing, dated and signed by all its members. This decision shall be a recommendation to the Director of this Office and shall be advisory only. Any member of the Board who dissents from the decision of the majority will indicate before his signature the phrase "I dissent." A statement setting forth the reasons or basis for such dissent may be included as an attachment to the majority opinion. The decision shall be prepared in such form to protect fully from unauthorized disclosure any information which might adversely affect the interests of national security. The decision of the Board together with the complete record of the case shall be forwarded to the Security Officer.

#### Section 9. Final action in security hearing cases.

(a) The Security Officer will forward to the Director of this Office the recommendation of the Security Hearing Board and the complete record of the case.

(b) On the basis of the recommendation of the Board, and his review of the complete record of the case the Director will:

- (1) Restore the employee to duty and direct that he be compensated for any period of suspension, if he finds that the reinstatement of the employee to his former position is clearly consistent with the interests of national security, or;
- (2) Terminate the employment of the suspended employee, if he finds that reinstatement of the employee is not clearly consistent with the interests of national security.

The employee shall immediately be notified in writing of the action and decision of the Director.

(c) Notices of suspension, reinstatement, or termination ordered in all security cases shall be promptly supplied by the Security Officer to the Civil Service Commission.



(d) Any person whose employment has been suspended or terminated in the interests of national security and who is subsequently restored or reinstated to duty by the Director shall be compensated for the period of such suspension or termination, in an amount not to exceed the difference between the amount such person would normally have earned during the period of such removal, at the rate at which he was compensated on the date of his removal, and the interim net earnings, if any, of such person.

Section 10. Reemployment of terminated employees.

No person whose employment has been terminated by this Office or by any department, agency, or establishment pursuant to 5 U.S.C. 7531-32 or Executive Order 10450, as amended, or any other security or loyalty program, shall thereafter be employed in this Office unless the Director, after consultation with the Security Officer, finds and determines that such employment is clearly consistent with the interests of national security, and unless the Civil Service Commission determines that such person is eligible for such employment. The findings and determination of the Director and the determination of the Civil Service Commission shall be made a part of the security file of the person concerned.

Section 11. Periodic security reevaluation and review.

(a) Each employee of this Office is required 5 years after his appointment and at least once each succeeding 5 years to submit an update personnel security questionnaire (Standard Form 86) to the Security Officer. The questionnaire will be reviewed by the Security Officer and a determination made regarding what further action, if any, is appropriate. Such action may include the following: check of local police and credit records, a national agency check, and an updated full field investigation.

(b) An investigation of an employee may also be initiated in the following circumstances:

- (1) Access to more highly classified material is required than an employee's existing clearance will permit;
- (2) Information is received subsequent to a previous clearance which makes a reevaluation of the basis for such clearance appropriate.