

Subpart O—Administrative Sanctions

§ 159a.97 Individual responsibility.

All personnel, civilian or military, of the Department of Defense are responsible individually for complying with the provisions of this part.

§ 159a.98 Violations subject to sanctions.

(a) DoD Military and civilian personnel are subject to administrative sanctions if they:

(1) Knowingly and willfully classify or continue the classification of information in violation of E.O. 12356, any implementing issuances, or this part.

(2) Knowingly, willfully, or negligently disclose to unauthorized persons information properly classified under E.O. 12356 or prior orders; or

(3) Knowingly and willfully violate any other provision of E.O. 12356, any implementing issuances or this part.

(b) Sanctions include but are not limited to a warning notice, reprimand, termination of classification authority, suspension without pay, forfeiture of pay, removal or discharge, and will be imposed upon any person, regardless of office or level of employment, who is responsible for a violation specified under this paragraph as determined appropriate under applicable law and DoD regulations. Nothing in this part prohibits or limits action under the Uniform Code of Military Justice based upon violations of that Code.

§ 159a.99 Corrective action.

The Secretary of Defense, the Secretaries of the Military Departments, and the heads of other DoD Components shall ensure that appropriate and prompt corrective action is taken whenever a violation under § 159a.98(a) occurs or repeated administrative discrepancies or repeated disregard of requirements of this Regulation occur (see § 159a.100). Commanders and supervisors, in consultation with appropriate legal counsel, shall utilize all appropriate criminal, civil, and administrative enforcement remedies against employees who violate the law and security requirements as set forth in this part and other pertinent DoD issuances.

§ 159a.100 Administrative discrepancies.

Repeated administrative discrepancies in the marking and handling of classified information and material such as failure to show classification authority; failure to apply internal classification markings; failure to adhere to the requirements of this part that pertain to dissemination, storage, accountability, and destruction, and that are determined not to constitute a violation under § 159a.98(a) may be grounds for adverse administrative action including warning, admonition, reprimand or termination of classification authority as determined appropriate under applicable policies and procedures.

§ 159a.101 Reporting violations.

(a) Whenever a violation under § 159a.98(a)(2) occurs, the Director of Counterintelligence and Investigative Programs, ODUSD(P) shall be informed of the date and general nature of the occurrence including the relevant parts of this part, the sanctions imposed, and the corrective action taken. Whenever a violation under § 159a.98(a) (1) or (3) occurs, the Director of Security Plans and Programs, OSUSD(P) shall be provided the same information. Notification of such violations shall be furnished to the Director of the ISOO in accordance with § 5.4(d) of E.O. 12356 by the ODUSD(P).

(b) Any action resulting in unauthorized disclosure of properly classified information that constitutes a violation of the criminal statutes and evidence reflected in classified information of possible violations of Federal criminal law by a DoD employee and of possible violations by any other person of those Federal criminal laws specified in guidelines adopted by the Attorney General shall be the subject of a report processed in accordance with DoD Directive 5210.50 and DoD Instruction 5240.4.

(c) Any action reported under paragraph (b) of this section, shall be reported to the Attorney General by the General Counsel, Department of Defense.

(d) Reports shall be made to appropriate counterintelligence, investigative, and personnel security authorities

concerning any employee who is known year, for appropriate evaluation, including readjudication of the employee's security clearance.

APPENDIX A TO PART 159a—EQUIVALENT FOREIGN AND INTERNATIONAL PACT ORGANIZATION SECURITY CLASSIFICATIONS

Country	Top Secret	Secret	Confidential	
Argentina	Estrictamente Secreto	Secreto	Confidencial	Reservado.
Australia	Top Secret	Secret	Confidential	
Austria	Streng Geheim	Geheim	Verschluss	
Belgium:				
French	Tres Secret	Secret	Confidentiel Restreints	Difusion.
Flemish	Zeer Geheim	Geheim	Vertrouwelijk Verspreiding	Bepertke.
Bolivia	Syoersecreto or Muy Secreto	Secreto	Confidencial	Resedrvado.
Brazil	Ultra Secreto	Secreto	Confidencial	Reservado.
Cambodia	Tres Secret	Secret	Secret/Confidential	
Canada	Top Secret	Secret	Confidential	Restricted.
Chile	Secreto	Secreto	Reservado	Reservado.
Columbia	Ultrasecreto	Secreto	Reservado Restringido	Confidencial.
Costa Rica	Alto Secreto	Secreto	Confidencial	
Denmark	Hojst Himmiligt	Himmiligt	Fortroligt	Til Tjenestebrug.
Ecuador	Secretisimo	Secreto	Confidencial	Reservado.
El Salvador	Ultra Secreto	Secreto	Confidencial	Reservado.
Ethiopia	Yemlaz Birtou Mistir	Kilkil		
Finland	Erittain Salainen	Salainen		
France	Tres Secret	Secret Defense	Confidentiel Defense Restreinte.	Diffusion.
Germany	Streng Geheim	Geheim	Va-Vertraulich	
Greece	Akpre Anopphton	Anopphton	Emilieteytikon Xpheere	Mepinpiemenhe.
Guatemala	Alto Secreto	Secreto	Confidencial	Reservado.
Haiti		Secret	Confidencial	
Honduras	Super Secreto	Secreto	Confidencial	Reservado.
Hong Kong	Top Secret	Secret	Confidential	Restricted.
Hungary	Szigoruan Titkos	Titkos	Bizalmas	
India	Top Secret	Secret	Confidential	Restricted.
Indonesia	Sangat Rahasia	Rahasia	Terbatas	
Iran	Bekoli Serri	Serri	Kheili Mahramaneh	Mahramaneh.
Iraq	(Absolutelyly secret)	(Secret)		(Limited).
Ireland Gaelic	Top Secret An-Sicreideach	Secret Sicreideach.	Confidential Runda	Restricted Srianta.
Israel	Sodi Beyoter	Sodi	Shamur	Mugbal.
Italy	Segretissimo	Segreto	Riservatissimo	Riservato.
Japan	Kimitsu	Gokuhi	Hi Bugaihi	Toriatsukaichui.
Jordan	Maktum Jiddan	Maktum	Sirri	Mahdud.
Korea				
Laos	Tres Secret	Secret	Secret/Confidentiel Restreinte	Difusion.
Lebanon	Tres Secret	Secret	Confidentiel	
Mexico	Alto Secreto	Secreto	Confidencial	Restringido.
Netherlands	Zeer Geheim	Geheim	Confidentieel or Vertrouwelijk	Dienstgeheim.
New Zealand	Top Secret	Secret	Confidential	Dienstgeheim.
Nicaragua	Alto Secreto	Secreto	Confidencial	Reservado.
Norway	Strengt Hemmelig	Hemmelig	Konfideneielt	Begrenset.
Pakistan	Top Secret	Secret	Confidential	Restricted.
Paraguay	Secreto	Secreto	Confidencial	Reservado.
Peru	Estrictamente Secreto	Secreto	Confidencial	Reservado.
Philippines	Top Secret	Secret	Confidential	Restricted.
Portugal	Muito Secreto	Secreto	Confidencial	Reservado.
Spain	Maximo Secreto	Secreto	Confidencial Limitada	Diffussion.
Sweden (Red Borders).	Hemlig	Hemlig	Hemlig	
Switzerland	(¹)	(¹)	(¹)	
French	Secret	Secret	Secret Exclusive Du	Reserve A L'Usage.
German	Streng Geheim	Geheim	Vertraulich Lichen Gebrauch	Nur Fur Dienst-Ad Exclusive Uso.
Italian	Segreto	Segreto	Segreto Di Servizio	Pok Pid.
Thailand	Lup Tisud	Lup Maag	Lup	Hizmete Ozel.
Turkey	Cok Gizli	Gizli	Ozel	
Union of South Africa:				
English	Top Secret	Secret	Confidential	Restricted.
Afrikaana	Uiters Geheim	Geheim	Vertroulik	Reperk.

APPENDIX A TO PART 159a—EQUIVALENT FOREIGN AND INTERNATIONAL PACT ORGANIZATION
 SECURITY CLASSIFICATIONS—Continued

Country	Top Secret	Secret	Confidential	
United Arab Republic (Egypt).	Top Secret	Very Secret	Secret	Official.

¹ Three languages. TOP SECRET has a registration number to distinguish from SECRET and CONFIDENTIAL.

Country	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
United Kingdom	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Uruguay	ULTRA SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
USSR	СОВЕРШЕННО СЕКРЕТНО	СЕКРЕТНО	НЕ ПОДЛЕЖИТ ОПУБЛИКОВАНИЮ	ДЛЯ СЛУЖЕБНОГО ПОЛЬЗОВАНИЯ
Viet Nam French	TRES SECRET	SECRET DEFENSE	CONFIDENTIEL DEFENSE	DIFFUSION RESTREINTE
Vietnamese	TOP SECRET	SECRET	KIN	TU MAT
INTERNATIONAL ORGANIZATION	TOP SECRET	SECRET	CONFIDENTIAL	(SEE CHAPTER XI)
NATO	COSMIC TOP SECRET	NATO SECRET	NATO CONFIDENTIAL	NATO RESTRICTED

NOTES:

In all instances foreign security classification systems are not exactly parallel to the U.S. system and exact equivalent classifications cannot be stated. The classifications given above represent the nearest comparable designations that are used to signify degrees of protection and control similar to those prescribed for the equivalent U.S. classifications.

"ATOMAL" information is an exclusive designation used by NATO to identify "Restricted Data" or "Formerly Restricted Data" information released by the U.S. Government to NATO.

[54 FR 26959, June 27, 1989, as amended at 54 FR 31334, July 28, 1989]

Office of the Secretary of Defense

Pt. 159a, App. C

APPENDIX B TO PART 159a—GENERAL ACCOUNTING OFFICE OFFICIALS AUTHORIZED TO CERTIFY SECURITY CLEARANCES (SEE §159a.53(b)(3))

The Comptroller General, Deputy Comptroller General and Assistant Comptroller General and Assistants to the Comptroller General

The General Counsel and Deputy General Counsel

The Director and Deputy Director, Personnel; the Security Officer

The Director and Deputy Director, Office of Internal Review

The Director and Assistants to the Director of the Office of Program Planning and the Office of Policy

The Director and Deputy Directors of the Community and Economic Development Division

The Director, and Deputy Directors, Associate Directors, Deputy Associate Directors, Senior Group Directors, and the Assistant to the Director for Planning and Administration of the Energy and Minerals Division

The Director, Deputy Directors, Associate Directors and Division Personnel Security Officer of the Human Resources Division

The Directors, Deputy Directors, and Associate Directors, of the following Divisions:

- Claims
- Field Operations
- Financial and General Management Studies
- General Government
- International
- Logistics and Communications
- Procurement and Systems Acquisition
- Program Analysis Division

Directors and Managers of International Division Overseas Offices as follows:

Director European Branch, Frankfurt, Germany

Director Far East Branch, Honolulu, Hawaii
Manager, Sub Office, Bangkok, Thailand

Regional Managers and Assistsant Regional Managers of the Field Operations Division's Regional Offices as follows:

- Atlanta, Georgia
- Boston, Massachusetts
- Chicago, Illinois
- Cincinnati, Ohio
- Dallas, Texas
- Denver, Colorado
- Detroit, Michigan
- Kansas City, Missouri
- Los Angeles, California
- New York, New York
- Norfolk, Virginia
- Philadelphia, Pennsylvania
- San Francisco, California
- Seattle, Washington
- Washington, D.C.

APPENDIX C TO PART 159a—INSTRUCTIONS GOVERNING USE OF CODE WORDS, NICKNAMES, AND EXERCISE TERMS (SEE §159a.54(j))

1. Definitions

a. *Using Component.* The DoD Component to which a code word is allocated for use, and which assigns to the word a classified meaning, or which originates nicknames and exercise terms using the procedure established by the Joint Chiefs of Staff.

b. *Code Word.* A single word selected from those listed in Joint Army-Navy-Air Force Publication (JANAP) 299 and later volumes, and assigned a classified meaning by appropriate authority to insure proper security concerning intentions, and to safeguard information pertaining to actual military plans or operations classified as Confidential or higher. A code word shall not be assigned to test, drill or exercise activities. A code word is placed in one of three categories:

(1) *Available.* Allocated to the using component. Available code words *individually* will be unclassified until placed in the active category.

(2) *Active.* Assigned a classified meaning and current.

(3) *Canceled.* Formerly active, but discontinued due to compromise, suspected compromise, cessation, or completion of the operation to which the code word pertained. Canceled code words *individually* will be unclassified and remain so until returned to the active category.

c. *Nickname.* A combination of two separate unclassified words which is assigned an unclassified meaning and is employed only for unclassified administrative, morale, or public information purposes.

d. *Exercise Term.* A combination of two separate unclassified words, normally unclassified, used exclusively to designate a test, drill, or exercise. An exercise term is employed to preclude the possibility of confusing exercise directions with actual operations directives.

2. Policy and Procedure

a. *Code Words.* The Joint Chiefs of Staff are responsible for allocating words or blocks of code words from JANAP 299 to DoD Components. DoD Components may request allocation of such code words as required and may reallocate available code words within their organizations, in accordance with individual policies and procedure, subject to applicable rules set forth herein.

(1) A permanent record of all code words shall be maintained by the Joint Chiefs of Staff.

(2) The using Component shall account for available code words and maintain a record of each active code word. Upon being canceled, the using component shall maintain

the record for 2 years; thence the record of each code word may be disposed of in accordance with current practices, and the code word returned to the available inventory.

b. Nicknames

(1) Nicknames may be assigned to actual events, projects, movement of forces, or other nonexercise activities involving elements of information of any classification category, but the nickname, the description or meaning it represents, and the relationship of the nickname and its meaning must be unclassified. A nickname is not designed to achieve a security objective.

(2) Nicknames, improperly selected, can be counterproductive. A nickname must be chosen with sufficient care to ensure that it does not:

(a) Express a degree of bellicosity inconsistent with traditional American ideals or current foreign policy;

(b) Convey connotations offensive to good taste or derogatory to a particular group, sect, or creed; or,

(c) Convey connotations offensive to our allies or other Free World nations.

(3) The following shall not be used as nicknames:

(a) Any two-word combination voice call sign found in JANAP 119 or ACP 110. (However, single words in JANAP 119 or ACP 110 may be used as part of a nickname if the first word of the nickname does not appear in JANAP 299 and later volumes.)

(b) Combination of words including word "project," "exercise," or "operation." (The word "project" often is used as the first or second word with an unclassified nickname originating outside the Department of Defense.)

(c) Words that may be used correctly either as a single word or as two words, such as "moonlight."

(d) Exotic words, trite expressions, or well-known commercial trademarks.

(4) The Joint Chiefs of Staff shall:

(a) Establish a procedure by which nicknames may be authorized for use by DoD Components.

(b) Prescribe a method for the using Components to report nicknames used.

(5) The heads of DoD Components shall:

(a) Establish controls within their Components for the assignment of nicknames authorized under subparagraph 2.b.(4)(a), above.

(b) Under the procedures established, advise the Joint Chiefs of Staff of nicknames as they are assigned.

c. Exercise Term

(1) Unclassified exercise terms may be assigned only to tests, drills, or exercises for the purpose of emphasizing that the event is a test, drill, or exercise and not an actual operation. However, the description or meaning it represents, and the relationship of the exercise term and its meaning can be classified

or unclassified. A classified exercise term is not authorized.

(2) Selection of exercise terms will follow the same guidance as contained in subparagraphs 2.b.(2) and (3), above.

(3) The Joint Chiefs of Staff shall:

(a) Establish a procedure by which exercise terms may be authorized for use by DoD Components.

(b) Prescribe a method for using Components to report exercise terms used.

(4) The heads of DoD Components shall:

(a) Establish controls within their Component for the assignment of exercise terms authorized under subparagraph 2.c.(3), above.

(b) Under the procedures established, advise the Joint Chiefs of Staff of exercise terms as they are assigned.

3. Assignment of Classified Meanings to Code Words

a. The DoD Component responsible for the development of a plan or the execution of an operation shall be responsible for determining whether to assign a code word.

b. Code words shall be activated for the following purposes only:

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

(2) To designate classified geographic locations in conjunction with plans or operations referred to in subparagraph 3.b.(1), above; or,

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

c. The using Component shall assign to a code word a specific meaning classified Secret or Confidential. Code words shall not be used to cover unclassified meanings. The assigned meaning need not in all cases be classified as high as the overall classification assigned to the plan or operation. Top Secret code words may be issued only with DUSD(P) or DoD Component head approval.

d. Code words shall be selected by each using Component in such manner that the word used does not suggest the nature of its meaning.

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

f. Each DoD Component shall establish policies and procedures for the control and assignment of classified meanings to code words, subject to applicable rules set forth herein.

4. Notice of Assignment, Dissemination, and Cancellation of Code Words and Meanings

a. The using Component shall promptly notify the Joint Chiefs of Staff when a code

word is made active, indicating the word, and its classification. Similar notice shall be made when any changes occur, such as the substitution of a new word for one previously placed in use.

b. The using Component is responsible for further dissemination of active code words and meanings to all concerned activities, to include classification of each.

c. The using Component is responsible for notifying the Joint Chiefs of Staff of canceled code words. This cancellation report is considered final action, and no further reporting or accounting of the status of the canceled code word will be required.

5. Classification and Downgrading Instructions

a. During the development of a plan, or the planning of an operation by the headquarters of the using Component, the code word and its meaning shall have the same classification. When dissemination of the plan to other DoD Components or to subordinate echelons of the using Component is required, the using Component may downgrade the code words assigned below the classification assigned to their meanings in order to facilitate additional planning implementation, and execution by such other Components or echelons, but code words shall, at a minimum, be classified Confidential.

b. A code word which is replaced by another code word due to a compromise or suspected compromise, or for any other reason, shall be canceled, and classified Confidential for a period of 2 years, after which the code word will become unclassified.

c. When a plan or operation is discontinued or completed, and is not replaced by a similar plan or operation but the meaning cannot be declassified, the code word assigned thereto shall be canceled and classified Confidential for a period of 2 years, or until the meaning is declassified, whichever is sooner, after which the code word will become unclassified.

d. In every case, whenever a code word is referred to in documents, the security classification of the code word shall be placed in parentheses immediately following the code word, for example, "Label (C)."

e. When the meaning of a code word no longer requires a classification, the using Component shall declassify the meaning and the code word and return the code word to the available inventory.

6. Security Practices

a. The meaning of a code word may be used in a message or other document, together with the code word, only when it is essential to do so. Active code words may be used in correspondence or other documents forwarded to addresses who may or may not have knowledge of the meaning. If the context of a document contains detailed instruc-

tions or similar information which indicates the purpose or nature of the related meaning, the active code word shall not be used.

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

c. Code words shall not be used for addresses, return addresses, shipping designators, file indicators, call signs, identification signals, or for other similar purposes.

7. Former Words

All code words formerly categorized as "inactive" or "obsolete" shall be placed in the current canceled category and classified Confidential. Unless otherwise restricted, all code words formerly categorized as "canceled" or "available" shall be individually declassified. All records associated with such code words may be disposed of in accordance with current practices, provided such records have been retained at least 2 years after the code words were placed in the former categories of "inactive," "obsolete," or "canceled."

8. Non-DoD Words

Nicknames or code words originating outside of the Department of Defense that are jointly used by the originating organization and the Department of Defense shall be registered with the DUSD(P) to prevent confusion with DoD-originated words.

APPENDIX D TO PART 159a—FEDERAL AVIATION ADMINISTRATION AIR TRANSPORTATION, SECURITY FIELD OFFICES (SEE § 159a.59(c)(1)(i))

City	State
Anchorage	Alaska
Atlanta	Georgia
Baltimore	Maryland
Boston	Massachusetts
Chicago (O'Hare)	Illinois
Cleveland	Ohio
Dallas	Texas
Denver	Colorado
Detroit	Michigan
Honolulu	Hawaii
Houston	Texas
Kansas City	Missouri
Las Vegas	Nevada
Los Angeles	California
Miami	Florida
Minneapolis	Minnesota
Newark	New Jersey
New Orleans	Louisiana
New York (John F. Kennedy)	New York
New York (La Guardia)	New York
Philadelphia	Pennsylvania
Pittsburgh	Pennsylvania
Portland	Oregon

<i>City</i>	<i>State</i>
St. Louis	Missouri
San Antonio	Texas
San Diego	California
San Francisco	California
San Juan	Puerto Rico
Seattle	Washington
Tampa	Florida
Tucson	Arizona
Washington (Dulles)	Washington, DC
Washington (National)	Washington, DC

APPENDIX E TO PART 159a—TRANSPORTATION PLAN (SEE § 159a.57(e))

The provisions of § 159a.57(e) of this part require that transmission instructions or a separate transportation plan be included with any contract, agreement or other arrangement involving the release of classified material to foreign entities. The transportation plan is to be submitted to and approved by applicable DoD authorities. As a minimum, the transportation plan shall include the following provisions:

a. A description of the classified material together with a brief narrative as to where and under what circumstances transfer of custody will occur;

b. Identification, by name or title, of the designated representative of the foreign recipient government or international organization who will receipt for and assume security responsibility for the U.S. classified material (person(s) so identified must be cleared for access to the level of the classified material to be shipped);

c. Identification and specific location of delivery points and any transfer points;

d. Identification of commercial carriers and freight forwarders or transportation agents who will be involved in the shipping process, the extent of their involvement, and their security clearance status;

e. Identification of any storage or processing facilities to be used and, relative thereto,

certification that such facilities are authorized by competent government authority to receive, store, or process the level of classified material to be shipped;

f. When applicable, the identification, by name or title, of couriers and escorts to be used and details as to their responsibilities and security clearance status;

g. Description of shipping methods to be used as authorized by the provisions of subpart I, together with the identification of carriers (foreign and domestic);

h. In those cases when it is anticipated that the U.S. classified material or parts thereof may be returned to the United States for repair, service, modification, or other reasons, the plan must require that shipment shall be via a carrier of U.S. or recipient government registry, handled only by authorized personnel, and that the applicable Military Department (for foreign military sales (FMS)) or Defense Investigative Service (for commercial sales) will be given advance notification of estimated time and place of arrival and will be consulted concerning inland shipment;

i. The plan shall require the recipient government or international organization to examine shipping documents upon receipt of the classified material in its own territory and advise the responsible Military Department in the case of FMS, or Defense Investigative Service in the case of commercial sales, if the material has been transferred enroute to any carrier not authorized by the transportation plan; and

j. The recipient government or international organization also will be required to inform the responsible Military Department or the Defense Investigative Service promptly and fully of any known or suspected compromise of U.S. classified material while such material is in its custody or under its cognizance during shipment.