# CHAPTER 1

# POLICY AND PROGRAM MANAGEMENT

## Section 1

## Policy

### 1-100 Purpose and Scope

a. This Regulation implements Executive Order 12958, Classified National Security Information, and associated OMB directives within the Department of Defense. It applies to all Components of the Department of Defense. It establishes the Department of Defense Information Security Program to promote proper and effective classification, protection and downgrading of official information requiring protection in the interest of the national security. It also promotes the declassification of information no longer requiring such protection.

b. There is information, other than classified information, that has been determined to require some type of protection or control. This information is generally known as "controlled unclassified information." Guidance concerning the protection or controls required for such information may be found in a number of DoD Directives, Regulations and Instructions. However, since classified information and controlled unclassified information often exist side-by-side in the work environment, often in the same document, the essence of available guidance pertaining to controlled unclassified information has been captured in Appendix C of this Regulation. The purpose of the Appendix is to provide the user, to the extent possible, a single source document for guidance concerning both classified and controlled unclassified information.

### 1-101 Policies

a. All personnel of the Department of Defense are personally and individually responsible for providing proper protection to classified information under their custody and control. All officials within the Department of Defense who hold command, management, or supervisory positions have specific, nondelegable responsibility for the quality of implementation and management of the Information Security Program within their areas of responsibility. Management of classified information shall be included as a critical element or item to be evaluated in the rating of original classification authorities, security managers or specialists, and other personnel whose duties primarily involve the creation or handling of classified information.

b. Except for information subject to the Atomic Energy Act of 1954 (as amended), Executive Order 12958 and this Regulation provide the only basis for application of security classification to information within the Department of Defense.

c. Information shall be classified only when necessary in the interest of national security, and shall be declassified as soon as is consistent with the requirements of national security.

d. Information shall not be reclassified after it has been declassified and officially released to the public by proper authority.

e. Persons shall be allowed access to classified information only if they (1) possess a valid and appropriate security clearance, (2) have executed an appropriate non-disclosure agreement, and (3) have a valid need for access to the information to perform a lawful and authorized governmental function. DoD Regulation 5200.2-R contains detailed guidance on personnel security investigation, adjudication and clearance.

f. Classified information shall be protected at all times. See Chapters 6 and 7 of this Regulation.

g. Classified information shall be maintained only when it is required for effective and efficient operation of the organization or its retention is required by law or regulation.

h. Classified documents and material that constitute permanently valuable records of the Government shall be maintained and disposed of in accordance with DoD Directive 5015.2. Other classified material shall be destroyed in accordance with Chapter 6 of this Regulation.

i. Special Access Programs shall be created, continued, managed, and discontinued in conformance with Chapter 8 of this Regulation.

# Section 2

# Program Management

## 1-200 Department of Defense

**The** Secretary of Defense has designated the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I)) as the senior agency official responsible for direction and administration of the Information Security Program for the Department of Defense. The Under Secretary of Defense for Policy (USD(P)) has been designated as the senior official responsible for administering that portion of the DoD Information Security Program pertaining to Special Access Programs (SAPS), the National. Disclosure Policy (NDP), foreign government (including NATO) information, and security arrangements for international programs. These officials shall perform those functions specified in subsection 5.6(c) of Executive Order 12958 and appropriate implementing directives for the Department of Defense.

1-201 DoD Components

The head of each DoD Component shall:

a. Appoint a senior agency official to be responsible for direction and administration of the program within the Component. (The Component head may designate a separate senior official to be responsible for overseeing Special Access Programs within the Component, if necessary.);

b. Commit necessary resources to the effective implementation of the Information Security Program; and

c. Establish procedures to ensure that the head of each activity within the Component that creates, handles or stores classified information appoints an official to serve as security manager for the activity, to provide proper management and oversight of the activity's Information Security Program. Persons appointed to these positions shall be provided training as required by Chapter 9 of this regulation.

1-202 Senior **Agency Officials**

The senior agency official appointed in each Component in accordance with paragraph 1-201 a., above, shall:

a. Oversee the Component's Information Security Program;

b. Promulgate (or cause to be promulgated) implementing directives as necessary for program implementation;

c. Establish and maintain a security education program as required by Chapter 9 of this Regulation;

d. Establish and maintain an ongoing self-inspection program, to include periodic review and assessment of the Component's classified products;

e. Establish procedures to prevent unauthorized access to classified information;

f. Develop special contingency plans, as necessary, for the safeguarding of classified information used in or near hostile or potentially hostile areas;

g. Ensure that the performance contractor other system used to rate the performance of civilian and military personnel includes the management of classified information as a critical element or item to be evaluated in the rating of (1) original classification authorities, (2) security managers and security specialists, and (3) all other personnel whose duties include significant involvement with the creation or handling of classified information;

h. Account for the costs associated with the implementation of this Regulation within the Component and report those costs as required; and

i. Ensure prompt and appropriate response to any request, appeal, challenge, complaint, or suggestion arising out of the implementation of this Regulation within the Component.

## Section 3

## Special Types of Information

### 1-300 Restricted Data

Classified information in the custody of the Department of Defense marked as Restricted Data under the Atomic Energy Act of 1954 (as amended) shall be stored, protected, and destroyed as required by this Regulation for other information of a comparable level of security classification. DoD policy and procedures concerning access to and dissemination of Restricted Data within DoD are contained in DoD Directive 5210.2.

### 1-301 Sensitive Compartmented Information (SCI) and Communications Security (COMSEC) Information

SCI and COMSEC information shall be controlled and protected in accordance with applicable national policy and DoD Directives and Instructions. Security classification and declassification policies of this Regulation apply to SCI and COMSEC information in the same manner as other classified information except that Appendix D of this Regulation provides special procedures for use in systematic and mandatory review of cryptologic information.

### 1-302 Special Access Program Information

Information covered by Special Access Programs established in accordance with Chapter 8 of this Regulation shall be classified, declassified, controlled and protected as required in this Regulation and instructions issued by officials charged with management of those programs. The provisions of this Regulation pertaining to classification, declassification and marking apply, without exception, to Special Access Program information unless waivers of specific requirements are obtained in accordance with Section 4 of this Chapter.

### 1-303 North Atlantic Treaty Organization and Other Foreign Government Information

North Atlantic Treaty Organization (NATO) classified information shall be safeguarded in compliance with United States Security Authority for NATO (USSAN) Instruction I-69. Other foreign government information shall be safeguarded as described herein for U.S. information except as specified in Appendix H or as required by treaties or international agreements

## Section 4

## Exceptional Situations

### 1-400 Military Operations

The provisions of this Regulation pertaining to accountability, dissemination, transmission, and storage of classified information and material may be modified by military commanders as necessary to meet local conditions encountered during military operations. Military operations include combat and peacekeeping operations as well as other operations involving military deployments. Classified information shall be introduced into combat areas or zones, or areas of potential hostile activity, only as necessary to accomplish the military mission.

### 1-401 Waivers to Requirements

a. Unless otherwise specified herein, DoD Components shall submit requests for waivers to the requirements of this Regulation through established channels, to the ASD(C3I) or, for information related to SAPS, foreign government information (including NATO) information, and security arrangements for international programs, to the Under Secretary of Defense (Policy) (USD(P)). The ASD(C3I) and USD(P) shall be responsible for promptly notifying the Director, Information Security Oversight Office of all waivers approved involving E.O. 12958 and its' implementing directives.

b. Requests for waivers shall contain sufficient information to permit a complete and thorough analysis to be made of the impact on national security of approval of the waiver. DoD Components shall maintain documentation regarding approved waivers and furnish such documentation, upon request, to other

agencies with whom classified information or secure facilities are shared.

## Section 5

## Corrective Actions and Sanctions

### 1-500 General

Heads of the DoD Components shall establish procedures to ensure that prompt and appropriate management action is taken in case of compromise of classified information, improper classification of information, violation of the provisions of this Regulation, and incidents that may put classified information at risk of compromise. Such actions shall focus on correction or elimination of the conditions that caused or occasioned the incident.

### 1-501 Sanctions

a. DoD military and civilian personnel **shall** be subject to sanctions if they knowingly, willfully, or negligently:

(1) Disclose to unauthorized persons information properly classified under this Regulation;

(2) Classify or continue the classification of information in violation of this Regulation;

(3) Create or continue a Special Access Program contrary to the requirements of this Regulation; or

(4) Violate any other provision of this Regulation.

b. Sanctions include, but are not limited to, warning, reprimand, suspension without pay, forfeiture of pay, removal, discharge, loss or denial of access to classified information, and removal of classification authority. Action may also be taken under the Uniform Code of Military Justice for violations of that Code and under applicable criminal law.

c. In case of demonstration of reckless disregard or a pattern of error in applying the classification standards of this Regulation on the part of a person holding original classification authority, the appropriate official shall, as a minimum, remove the offending individual's original classification authority.

### 1-502 Reporting of Incidents

Whenever a violation under paragraph l-501a ( 1), (2) or (3), above, occurs, the Component Senior Agency Official **shall** promptly notify the ASD(C3I) through appropriate channels. The ASD(C3I)) shall notify the Director, Information Security Oversight Office, as required by paragraph 5.7(e)(2) of Executive Order 12958. If the violation involves Special Access Program , NATO or foreign government information, it shall be promptly reported to the Assistant Deputy to the USD(P) for Policy Support, who will be responsible for all further notifications and appropriate coordination.

## Section 6

## Reports

### 1-600 **Reporting Requirements**

a. The ASD(C3I) shall establish requirements for the collection and reporting of data necessary to support fulfillment of the requirements of Executive Order 12958 and OMB and Security Policy Board implementing directives. As a minimum, DoD Components shall submit, on a fiscal year basis, a consolidated report concerning the Information Security Program of the Component on Standard Form (SF) 311, "Agency Information Security Program Data," to reach the Principal Director for Information Warfare, Security and Counterintelligence (PD(IWS&CI)), OASD(C3I), by October 20 of each year. SF311 shall be completed in accordance with the instructions thereon and augmenting instructions issued by the OASD(C3I). The OASD(C3I) shall submit the DoD report (SF311) to the Information Security Oversight Office by October 31 of each year. Interagency Report Control Number 0230-GSA-AN applies to this information collection requirement.

b. The USD(P) shall establish requirements for the collection and reporting of data necessary to the proper management of Special Access Programs within the Department.

# Section 7

# Self-Inspection

## 1-700 General

Heads of DoD Components shall establish and maintain a self-inspection program based on program needs and the degree of involvement with classified information. The purpose of the program shall be to evaluate and assess the effectiveness and efficiency of the Component's implementation of the DoD Information Security Program. Component activities that originate significant amounts of classified information should be inspected at least annually.