

Security

Department of the Army Information Security Program

Headquarters
Department of the Army
Washington, DC
25 February 88

UNCLASSIFIED

SUMMARY of CHANGE

AR 380-5

Department of the Army Information Security Program

This revision--

- o Adds a definition of "access" (1-300).
- o Adds a definition of "applicable associated markings" (1-301).
- o Adds a definition of "classified meeting" (1-305.1).
- o Revises the definition of "COMSEC" (1-307).
- o Adds a definition of "CONUS" (1-310).
- o Adds a definition of "controlled cryptographic item (CCI)"(1-311).
- o Adds a definition of "foreign national" (1-320.1).
- o Adds a definition of "foreign representative" 1-320.2).
- o Adds a definition of "government installation/facility"(1-321.1).
- o Adds a definition of "need-to-know" (1-327).
- o Adds a definition of "representatives of a foreign interest" (1-329.1).
- o Adds a definition of "security clearance" (1-331).
- o Adds a definition of "security representative" (1-331.1).
- o Emphasizes that requests for classification authority be made only when a demonstrable need is present (1-600c1).
- o Requires that original classification authorities be indoctrinated prior to exercise of authority (1-600d).
- o Clarifies record-keeping responsibilities for classification authorities in Specified Commands (1-602a2(d)).
- o Requires, rather than encourages, challenges to classification (2-103).
- o Specifies that only the Secretary of the Army can classify information which has never been classified, but which has been disclosed (2-204g).
- o Changes the requirement for reevaluation of classified material because of compromise to incorporate the concept of classified information that has been lost (2-210).
- o Requires that original classification authorities set a date or event for declassification (2-301b).

- o Requires that proponents of classification guides include public release procedures and foreign disclosure considerations in their guides (2-400b4).
- o Incorporates Distribution Statements of DoD Directive 5230.24 for use in classification guides (2-405b).
- o Adds instructions for requesting declassification of materials in NARA records centers (3-303 1. and 2.).
- o Refers to DoD Pamphlet, "A Guide to Marking Classified Documents" (4-103c).
- o Clarifies requirement for identification of original classification authorities (4-104a1).
- o Clarifies requirement for identification of original classification authorities when more than one official is involved(4-104a3).
- o Includes guidance on identifying the classification authority on documents that contain only foreign or NATO classified information (4-104c).
- o Permits use of the marking "Unclassified" on declassified documents (4-105).
- o Specifies that "Unclassified" be used on interior page marking, and exempts blank interior pages (4-200).
- o Allows a wholly unclassified major Annex of a classified document to be marked "Unclassified" on the first page, only (4-201).
- o Clarifies that the stated reason for classification by compilation meets the requirement for a written explanation in lieu of paragraph/portion marking (4-202d).
- o Specifies that material produced on automated word processing equipment is subject to portion marking (4-202g).
- o Includes guidance on classifying by compilation portions of a document that are already classified (4-203).
- o Adds guidance for marking references and bibliographies in a classified document (4-209).
- o Provides guidance for marking a set of slides as a single document (4-302b).
- o Provides guidance on marking video tapes; eliminates the requirement for duplicate sets of associated markings (at the beginning and end of such films) (4-302c).

- o Specifies interior pages of fan-folded computer printouts will be hand- or machine-marked with their classification (4-305).
- o Eliminates a conflict with DCID 1/7 by specifying that the abbreviated form of WNINTEL (and RD and FRD) will be included in portion markings, and on interior pages (4-500a).
- o Specifies that the SF 700 will be used to record the names of those with access to security containers, etc. (5-104b3).
- o Raises the approval level for removal of classified documents after-hours to the Secretary of the Army, or the heads of Army Staff or Major Commands; imposes the requirement for a GSA-approved safe for storage (5-200b).
- o Requires use of SFs 703, 704, and 705 cover sheets for Top Secret, Secret, and Confidential material (5-201a).
- o Requires use of SFs 701 and 702 for recording the end-of-day security check of areas and safes (5-202).
- o Tightens requirements for storage of US classified material in foreign countries (5-206).
- o Establishes the activity entry and exit inspection program(5-300, 5-301 and 5-302).
- o Introduces the "loss" concept in the treatment of compromise of classified information (6-102a, 6-103, 6-104, 6-105c,6-107, and 6-108).
- o Clarifies requirements for access to classified information(clearance and need-to-know); introduces the two-person rule for areas where Top Secret and Special Access Program information is in use, stored, or accessible (7-100).
- o Updates coverage on judicial procedures by reference to DoD Directive implementing the "Classified Information Procedures Act"(7-101g).
- o Provides new guidance on access by visitors, and minimum requirements for classified visit requests (7-105).
- o Adds the requirement to review classified document distribution lists (7-207c and 7-208b).
- o States that TSCOs need not be appointed in activities unlikely to process Top Secret information (7-300a).
- o Explicitly provides that copies of Top Secret documents be numbered (7-300b2).
- o Tightens controls required for Secret material to include receipt and dispatch records (7-301).
- o Adds a requirement for designation of reproduction facilities for classified information, and requires that two persons be assigned such duties, when possible (7-305).
- o Provides clarification that contractors may transport classified material outside the US only in accordance with the ISM(8-102b).

- o Specifies use of "Constant Surveillance Service (CSS)" for classified shipments (8-103d).
- o Provides guidance on overseas shipments, by freight forwarder, of classified hardware (8-104).
- o Provides special packaging instructions for Special Access Program Materials sent via U.S. Registered Mail (8-200a).
- o Approves the use of a locked briefcase as an outer wrapper for handcarried classified material (8-200f).
- o Requires receipting for Secret information, except when handcarried (8-202b).
- o Includes the new requirement for receipt of Confidential information, as is already required for other classified information transmitted to foreign governments (8-202c).
- o Ties the storage provisions for handcarrying classified material to the tightened overseas requirements, and states that overnight storage in a contractor's facility is acceptable only in the US (8-300a).
- o States that classified information will not be left unattended under any circumstances while being handcarried (8-300c).
- o Contains an additional briefing requirement for persons who must handcarry classified information (8-300f).
- o Eliminates the requirement to issue a dependent's ID card to persons who have no other ID (for use in handcarrying missions)(8-302d2 and 3).
- o Adds several requirements that must be met before approval of handcarrying classified information outside the US (8-303b).
- o Specifies that persons destroying classified information will have a means to verify its destruction (9-100).
- o Specifies the use of cross-cut shredders, in addition to other approved means of destruction (9-101).
- o Revises destruction requirements to include acceptable alternatives such as the two-person rule, or the certificate of destruction for Secret material; adds guidance for the control of burn bags (9-102).
- o Clarifies the number of officials who must sign Top Secret destruction certificates; eliminates the requirement for Secret destruction certificates; provides guidance on burn bags (9-103).
- o Establishes a requirement to destroy classified material over 5 years old; establishes the requirement for an annual "clean out" day (9-105).
- o Provides guidance on minimum security education requirements (10-101b).
- o Provides information on initial security briefings and execution of SF 189, "Classified Information Nondisclosure Agreement" (10-102).

- o Includes the requirement to sign a security termination statement upon administrative withdrawal of a security clearance(10-105a).
- o Provides that a report be made to DIS of persons refusing to sign a security termination statement (10-105b).
- o Simplifies the marking requirements for documents that contain foreign restricted information (11-302b).
- o Clarifies portion marking requirements for foreign government information in US documents; provides guidance for marking US documents containing only foreign restricted information;provides guidance for completion of the "classified by" line(11-304).
- o Includes new marking requirements for foreign government restricted information; excludes NATO restricted material from storage as FOUO (11-401b).
- o Requires annual inspections and audits of SAPs by security, contract, and audit activities (12-102a).
- o Introduces the requirement for polygraph exams for central office personnel with access to multiple SAPs (12-103b).
- o Includes a requirement for reporting results of inspections and audits of SAPs (12-105b).
- o Requires that security inspections of SAPS at contractor facilities be conducted by professional security personnel(12-108d2).
- o Specifies that the DoD IG will conduct oversight of SAPs(12-109b).
- o Includes a requirement for conduct of unannounced security inspections (13-303).
- o Specifies that an annual sampling of classified documents will be part of local security managers' duties; that adequate training is provided security managers; that security managers have access to the activity head (13-304).
- o Establishes the Defense Information Security Committee(DISC) and membership to assist in formulation of DoD policy and procedures (13-500 and 13-501).
- o Requires that commanders and supervisors employ all means necessary against employees who violate security rules (14-102).
- o Identifies the current OSD recipients of security violation reports (14-104a).
- o Adds the requirement to report employees who are responsible for repeated, serious security violations and provides for readjudication of their clearances (14-104d).

Effective 1 March 88

Security

Department of the Army Information Security Program

By Order of the Secretary of the Army:

CARL E. VUONO
General, United States Army
Chief of Staff

Official:

R. L. DILWORTH
Brigadier General, United States Army
The Adjutant General

History. This UPDATE printing publishes a revision that is effective 1 March 1988. This publication has been reorganized to make it compatible with the Army electronic publishing database. No content has been changed.

Summary. This regulation implements the policies and procedures set forth in Executive Order 12356, "National Security Information," 2 April 1982. It establishes a system for classification, downgrading, and declassification of information requiring protection in the interest of national security. This regulation contains policy and procedures for safeguarding such information; it provides for program oversight and administrative sanctions for violations. This version contains all of DoD

5200.1-R, "DoD Information Security Program Regulation," dated June 1986, including all recommendations of the Stilwell Commission approved for implementation. Army implementing instructions in this regulation are set in boldface type. The provisions of paragraph 5-300, 5-301, 5-302, and 5-303 pertaining to the Activity Entry and Exit Inspection Program will be implemented upon issuance of DD Form 2501 (Courier Authorization Card) or one year from the effective date of this Regulation whichever occurs earlier.

Applicability. This regulation applies to all military and civilian members of the Active Army, Army National Guard (ARNG), and US Army Reserve (USAR).

Proponent and exception authority. Not applicable.

Army management control process. This regulation is subject to the requirements of AR 11-2. It contains internal control provisions but does not contain checklists for conducting internal control reviews. These checklists are contained in DA Circular 11-87-1, May 5, 1987.

Supplementation. Supplementation of this regulation is prohibited unless prior approval is obtained from HQDA (DAMI-CIS), WASH DC 20310-1051.

Interim changes. Interim changes to this

regulation are not official unless they are authenticated by the Adjutant General. Users will destroy interim changes on their expiration dates unless sooner superseded or rescinded.

Suggested Improvements. The proponent agency of this regulation is the Office of the Deputy Chief of Staff for Intelligence. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to HQDA (DAMI-CIS)WASH DC 20310-1051.

Distribution. Distribution of this publication is made in accordance with DA Form 12-9A-R requirements for 380 series publications. The number of copies distributed to a given subscriber is the number of copies requested in Blocks 326, 327, 328, 329, and 330 of the subscriber's DA Form 12-9A-R. AR 380-5 distribution is A, B, C, D, and E for the Active Army, the ARNG, and the USAR. Existing account quantities will be adjusted and new account quantities will be established upon receipt of a signed DA Form 12-9U-R (Subscription for Army UPDATE Publications Requirements) from the publications account holder.

Contents (Listed by paragraph and page number)

Chapter 1

General Provisions, page 1

Section 1

References, page 1

References • 1-100, *page 1*

Section 2

Purpose and Applicability, page 2

Purpose • 1-200, *page 2*

Applicability • 1-201, *page 2*

Nongovernment operations • 1-202, *page 2*

Combat operations • 1-203, *page 2*

Atomic energy material • 1-204, *page 2*

Sensitive compartmented and communications security information
• 1-205, *page 2*

Automatic data processing systems • 1-206, *page 3*

Section 3

Definitions, page 3

Access • 1-300, *page 3*

Applicable doubted markings • 1-301, *page 3*

Carve-out • 1-302, *page 3*

Classification authority • 1-303, *page 3*

Classification guide • 1-304, *page 3*

Classified Information • 1-305, *page 3*

Classified meeting • 1-305.1, *page 3*

Classifier • 1-306, *page 3*

Communications security (COMSEC) • 1-307, *page 3*

Compromise • 1-308, *page 3*

Confidential source • 1-309, *page 3*

Continental United States (CONUS) • 1-310, *page 3*

Controlled Cryptographic Item (CCI) • 1-311, *page 3*

Critical Nuclear Weapon Design Information • 1-312, *page 3*

Custodian • 1-313, *page 3*

Declassification • 1-314, *page 3*

Declassification event • 1-315, *page 3*

Derivative classification • 1-316, *page 3*

*This regulation supersedes AR 380-88, 21 January 1985 and AR 380-5, 1 August 1983.

Contents—Continued

Document • 1-317, *page 3*
DoD component • 1-318, *page 3*
Downgrade • 1-319, *page 3*
Foreign government Information • 1-320, *page 4*
Foreign national • 1-320.1, *page 4*
Foreign representative • 1-320.2, *page 4*
Formerly Restricted Data • 1-321, *page 4*
Government installation/facility • 1-321.1, *page 4*
Information • 1-322, *page 4*
Information security • 1-323, *page 4*
Intelligence activity • 1-324, *page 4*
Material • 1-325, *page 4*
National security • 1-326, *page 4*
Need-to-know • 1-327, *page 4*
Original classification • 1-328, *page 4*
Regrade • 1-329, *page 4*
Representatives of a foreign Interest • 1-329.1, *page 4*
Restricted Data • 1-330, *page 4*
Security clearance • 1-331, *page 4*
Security representative • 1-331.1, *page 4*
Sensitive compartmented information • 1-332, *page 4*
Special Access Program • 1-333, *page 4*
Special activity • 1-334, *page 4*
Unauthorized disclosure • 1-335, *page 4*
United States and its territories, possessions, administrative, and commonwealth areas • 1-336, *page 4*
Upgrade • 1-337, *page 5*

Section 4

Policies, page 5
Classification • 1-400, *page 5*
Classification • 1-401, *page 5*
Safeguarding • 1-402, *page 5*

Section 5

Security Classification Designations, page 5
General • 1-500, *page 5*
Top Secret • 1-501, *page 5*
Secret • 1-502, *page 5*
Confidential • 1-503, *page 5*

Section 6

Authority to Classify, Downgrade, and Declassify, page 5
Original classification authority • 1-600, *page 5*
Derivative classification responsibility • 1-601, *page 6*
Record and report requirements • 1-602, *page 6*
Declassification and down-grading authority • 1-603, *page 7*

Chapter II

Classification, *page 7*

Section 1

Classification Responsibilities, page 7
Accountability of classifiers • 2-100, *page 7*
Classification approval • 2-101, *page 7*
Classification planning • 2-102, *page 7*
Challenges to classification • 2-103, *page 7*

Section 2

Classification Principles, Criteria, and Considerations, page 8
Reasoned judgment • 2-200, *page 8*
Identification of specific information • 2-201, *page 8*
Specific classifying criteria • 2-202, *page 8*
Presumption of damage • 2-203, *page 8*
Limitations on classification • 2-204, *page 8*
Classifying scientific research data • 2-205, *page 8*
Classifying documents • 2-206, *page 9*
Classifying material other than documents • 2-207, *page 9*

State of the art and Intelligence • 2-208, *page 9*
Effect of open publication • 2-209, *page 9*
Reevaluation of classification because of compromise • 2-210, *page 9*
Compilation of Information • 2-211, *page 9*
Extracts of information • 2-212, *page 9*

Section 3

Duration of Original Classification, page 9
General • 2-300, *page 9*
Duration of classification • 2-301, *page 9*
Subsequent extension of duration of classification • 2-302, *page 10*

Section 4

Classification Guides, page 10
General • 2-400, *page 10*
Multiservice interest • 2-401, *page 10*
Research, development, test, and evaluation • 2-402, *page 10*
Project phases • 2-403, *page 10*
Review of classification guides • 2-404, *page 10*
Distribution of classification guides • 2-405, *page 10*
Index of security classification guides • 2-406, *page 11*

Section 5

Resolution of conflicts, page 11
General • 2-500, *page 11*
Procedures • 2-501, *page 11*
Final decision • 2-502, *page 11*
Timing • 2-503, *page 11*

Section 6

Obtaining classification Evaluations., page 11
Procedures • 2-600, *page 11*

Section 7

Information Developed by Private Sources, page 11
General • 2-700, *page 11*
Patent Secrecy Act • 2-701, *page 11*
Independent research and development • 2-702, *page 12*
Other private information • 2-703, *page 12*

Section 8

Regrading, page 12
Raising to a higher level of classification • 2-800, *page 12*
Classification of information previously determined to be unclassified • 2-801, *page 12*
Notification • 2-802, *page 12*
Downgrading • 2-803, *page 12*

Section 9

Industrial Operations, page 12
Classification in Industrial operations • 2-900, *page 12*
Contract Security Classification Specification • 2-901, *page 12*

Chapter III

Declassification and Downgrading, *page 12*

Section 1

General Provisions, page 12
Policy • 3-100, *page 12*
Responsibility of officials • 3-101, *page 13*
Declassification coordination • 3-102, *page 13*
Declassification by the Director of the ISOO • 3-103, *page 13*

Section 2

Systematic Review, page 13
Assistance to the Archivist of the United States • 3-200, *page 13*
Systematic review guideline • 3-201, *page 13*

Contents—Continued

- Systematic review procedures • 3–202, *page 13*
- Systematic review of classified cryptologic information • 3–203, *page 13*
- Systematic review of intelligence information • 3–204, *page 13*

Section 3

- Mandatory Declassification Review, page 13*
- Information covered • 3–300, *page 13*
- Presidential information • 3–301, *page 13*
- Cryptologic Information • 3–302, *page 13*
- Submission of requests for mandatory declassification review • 3–303, *page 13*
- Requirements for processing • 3–304, *page 14*
- Foreign government information • 3–305, *page 14*
- Prohibition • 3–306, *page 14*
- Restricted Data and Formerly Restricted Data • 3–307, *page 14*

Section 4

- Declassification of Transferred Documents or Material, page 14*
- Material officially transferred • 3–400, *page 14*
- Material not officially transferred • 3–401, *page 14*
- Transfer for storage or retirement • 3–402, *page 15*

Section 5

- Downgrading, page 15*
- Automatic downgrading • 3–500, *page 15*
- Downgrading upon reconsideration • 3–501, *page 15*

Section 6

- Miscellaneous, page 15*
- Notification of changes in declassification • 3–600, *page 15*
- Foreign relations series • 3–601, *page 15*
- Reproduction for declassification review • 3–602, *page 15*

Chapter IV

Marking, *page 15*

Section 1

- General Provisions, page 15*
- Designation • 4–100, *page 15*
- Purpose of designation • 4–101, *page 15*
- Exceptions • 4–102, *page 15*
- Documents or other material in general • 4–103, *page 15*
- Identification of classification authority • 4–104, *page 16*
- Wholly unclassified material • 4–105, *page 16*

Section 2

- Specific Markings on Documents, page 16*
- Overall and page marking • 4–200, *page 16*
- Marking components • 4–201, *page 16*
- Portion marking • 4–202, *page 16*
- Compilations • 4–203, *page 17*
- Subjects and titles of documents • 4–204, *page 17*
- File, folder, or group of documents • 4–205, *page 17*
- Transmittal documents • 4–206, *page 18*
- Electronically transmitted messages • 4–207, *page 18*
- Translations • 4–208, *page 18*
- Markings references and bibliographies • 4–209, *page 18*

Section 3

- Markings on Special Categories of Material, page 18*
- General provisions • 4–300, *page 18*
- Charts, maps, and drawings • 4–301, *page 18*
- Photographs, films, and recordings • 4–302, *page 18*
- Decks of ADP punched cards • 4–303, *page 19*
- Removable ADP and word processing storage media • 4–304, *page 19*
- Documents produced by ADP equipment • 4–305, *page 19*

- Material for training purposes • 4–306, *page 19*
- Miscellaneous material • 4–307, *page 20*
- Special Access Program documents and material • 4–308, *page 20*
- Secure telecommunications and information handling equipment • 4–309, *page 20*
- Associated markings • 4–310, *page 20*

Section 4

- Classification Authority, Duration, and Change in Classification Markings, page 20*
- Declassification and regrading marking procedures • 4–400, *page 20*
- Applying derivative declassification dates • 4–401, *page 20*
- Commonly used markings • 4–402, *page 20*
- Upgrading • 4–403, *page 21*
- Limited use of posted notice for large quantities of material • 4–404, *page 21*

Section 5

- Additional Warning Notices, page 21*
- General provisions • 4–500, *page 21*
- Restricted Data • 4–501, *page 21*
- Formerly Restricted Data • 4–502, *page 21*
- Intelligence sources or methods Information • 4–503, *page 21*
- COMSEC material • 4–504, *page 21*
- Dissemination and reproduction notice • 4–505, *page 21*
- Other notations • 4–506, *page 21*

Section 6

- Remarking Old Material, page 21*
- General • 4–600, *page 21*
- Earlier declassification and extension of classification • 4–601, *page 22*

Chapter V

Safekeeping and Storage, *page 22*

Section 1

- Storage and Storage Equipment, page 22*
- General policy • 5–100, *page 22*
- Standards for storage equipment • 5–101, *page 22*
- Storage of classified information • 5–102, *page 22*
- Procurement and phase-in of new storage equipment • 5–103, *page 23*
- Designations and combinations • 5–104, *page 23*
- Repair of damaged security containers or vault doors • 5–105, *page 24*
- Turn-In or transfer of security equipment • 5–106, *page 24*

Section 2

- Custodial Precautions, page 24*
- Responsibilities of custodians • 5–200, *page 24*
- Care during working hours • 5–201, *page 25*
- End-of day security checks • 5–202, *page 25*
- Emergency planning • 5–203, *page 25*
- Telecommunications conversations • 5–204, *page 27*
- Security of meetings and conferences • 5–205, *page 27*
- Safeguarding of U.S. classified information located in foreign countries • 5–206, *page 29*

Section 3

- Activity Entry and Exit Inspection Program, page 29*
- Policy • 5–300, *page 29*
- Inspection frequency • 5–301, *page 30*
- Inspection procedures and Identification • 5–302, *page 30*
- Local records • 5–303, *page 30*

Contents—Continued

Chapter VI

Compromise of Classified Information, page 30

Policy • 6–100, page 30

Cryptographic and sensitive compartmented information • 6–101, page 31

Responsibility of discoverer • 6–102, page 31

Preliminary inquiry • 6–103, page 31

Investigation • 6–104, page 31

Responsibility of authority ordering investigation • 6–105, page 32

Responsibility of originator • 6–106, page 32

System of control of damage assessments • 6–107, page 32

Compromises involving more than one agency • 6–108, page 32

Espionage and deliberate compromise • 6–109, page 32

Unauthorized absentees • 6–110, page 32

Suicide and attempted Suicide • 6–111, page 32

Unauthorized disclosure of classified information to the public • 6–112, page 33

Chapter VII

Access, Dissemination, and Accountability, page 33

Section 1

Access, page 33

Policy • 7–100, page 33

Access by persons outside the Executive Branch • 7–101, page 34

Access by foreign nationals, foreign governments, and international organizations • 7–102, page 35

Other situations • 7–103, page 35

Access required by other Executive Branch Investigative and law enforcement agents • 7–104, page 35

Access by visitors • 7–105, page 35

Student officers attending civilian institutions and faculty members of civilian institutions • 7–106, page 35

Section 2

Dissemination, page 36

Policy • 7–200, page 36

Restraints on special access requirements • 7–201, page 36

Information originating in a non-DoD department or agency • 7–202, page 36

Foreign intelligence information • 7–203, page 36

Restricted Data and Formerly Restricted Data • 7–204, page 36

NATO Information • 7–205, page 36

COMSEC information • 7–206, page 36

Dissemination of Top Secret information • 7–207, page 36

Dissemination of Secret and Confidential information • 7–208, page 36

Code words, nicknames, and exercise terms • 7–209, page 36

Scientific and technical meetings • 7–210, page 36

Section 3

Accountability and Control, page 36

Top Secret information • 7–300, page 36

Secret information • 7–301, page 38

Confidential information • 7–302, page 38

Receipt of classified material • 7–303, page 38

Working papers • 7–304, page 38

Restraint on reproduction • 7–305, page 38

Chapter VIII

Transmission, page 39

Section 1

Methods of Transmission or Transportation, page 39

Policy • 8–100, page 39

Top Secret information • 8–101, page 39

Secret information • 8–102, page 39

Confidential Information • 8–103, page 40

Transmission of classified material to foreign governments

• 8–104, page 40

Consignor-consignee responsibility for shipment of bulky material

• 8–105, page 41

Transmission of COMSEC information • 8–106, page 41

Transmission of Restricted Data • 8–107, page 41

Section 2

Preparation of Material for Transmission, Shipment, or Conveyance, page 41

Envelopes or containers • 8–200, page 41

Addressing • 8–201, page 42

Receipt systems • 8–202, page 42

Exceptions • 8–203, page 43

Section 3

Restrictions, Procedures, and Authorization Concerning Escort or Handcarrying of Classified Information, page 43

General restrictions • 8–300, page 43

Restrictions on handcarrying classified information aboard commercial passenger aircraft • 8–301, page 43

Procedure for handcarrying classified information aboard commercial passenger aircraft • 8–302, page 43

Authority to approve escort or handcarry of classified information aboard commercial passenger aircraft • 8–303, page 44

Chapter IX

Disposal and Destruction, page 44

Policy • 9–100, page 44

Methods of destruction • 9–101, page 44

Destruction procedures • 9–102, page 45

Records of destruction • 9–103, page 45

Classified waste • 9–104, page 45

Classified document retention • 9–105, page 45

Chapter X

Security Education, page 45

Responsibility and objectives • 10–100, page 45

Scope and principles • 10–101, page 45

Initial briefings • 10–102, page 46

Refresher briefings • 10–103, page 46

Foreign travel briefings • 10–104, page 46

Termination briefings • 10–105, page 46

Other requirements • 10–106, page 47

Chapter XI

Foreign Government Information, page 47

Section 1

Classification, page 47

Classification • 11–100, page 47

Duration of classification • 11–101, page 47

Section 2

Declassification, page 47

Policy • 11–200, page 47

Systematic review • 11–201, page 47

Mandatory review • 11–202, page 47

Section 3

Marking, page 47

Equivalent U.S. classification designations • 11–300, page 47

Marking NATO documents • 11–301, page 48

Marking other foreign government documents • 11–302, page 48

Marking of DoD classification determinations • 11–303, page 48

Marking of foreign government information in DoD documents • 11–304, page 48

Contents—Continued

Section 4

Protective Measures, page 48

NATO classified information • 11–400, *page 48*

Other foreign government information • 11–401, *page 48*

Chapter XII

Special Access Programs, *page 48*

Policy • 12–100, *page 48*

Establishment of Special Access Programs • 12–101, *page 48*

Review of Special Access Programs • 12–102, *page 49*

Control and administration • 12–103, *page 49*

Codewords and nicknames • 12–104, *page 49*

Reporting of Special Access Programs • 12–105, *page 49*

Accounting for Special Access Programs • 12–106, *page 50*

Limitations on access • 12–107, *page 50*

“Carve-out” contracts • 12–108, *page 50*

Oversight reviews • 12–109, *page 50*

Chapter XIII

Program Management, *page 50*

Section 1

Executive Branch Oversight and Policy Direction, page 50

National Security Council • 13–100, *page 50*

Administrator of General Services • 13–101, *page 50*

Information Security Oversight Office • 13–102, *page 50*

Section 2

Department of Defense, page 51

Management responsibility • 13–200, *page 51*

Section 3

DoD Components, page 51

General • 13–300, *page 51*

Military departments • 13–301, *page 51*

Other components • 13–302, *page 51*

Program monitorship • 13–303, *page 51*

Field program management • 13–304, *page 51*

Section 4

Information requirements • 13–400, *page 52*

Section 5

Defense Information Security Committee, page 52

Purpose • 13–500, *page 52*

Direction and membership • 13–501, *page 52*

Chapter XIV

Administrative Sanctions, *page 52*

Individual responsibility • 14–100, *page 52*

Violations subject to sanctions • 14–101, *page 52*

Correction action • 14–102, *page 53*

Administrative discrepancies • 14–103, *page 53*

Reporting violations • 14–104, *page 53*

Chapter XV

Safeguarding Joint Chiefs of Staff Papers, *page 53*

Section 1

General, page 53

Purpose • 15–100, *page 53*

References • 15–101, *page 53*

Responsibilities • 15–102, *page 53*

Section 2

Requirements, page 53

Policies • 15–200, *page 53*

Access to JCS papers • 15–201, *page 53*

Familiarization requirements • 15–202, *page 53*

Section 3

Procedures, page 53

Distribution of JCS documents • 15–300, *page 53*

Release and distribution of Joint Strategic Planning System (JSPS) documents • 15–301, *page 54*

Release and distribution of Joint Operation Planning System (JOPS) documents • 15–302, *page 54*

Release of JCS information to Army Service schools • 15–303, *page 54*

Release of information to organizations outside DA • 15–304, *page 54*

Reproduction of JCS documents • 15–305, *page 54*

Appendixes

- A. Equivalent Foreign and International Pact Organization Security Classifications, *page 55*
- B. General Accounting Office Officials Authorized to Certify Security Clearances, *page 60*
- C. Instructions Governing Use of Code Words, Nicknames and Exercise Terms, *page 61*
- D. Federal Aviation Administration Air Transportation Security Field Offices, *page 63*
- E. Transportation Plan, *page 64*
- F. Program Evaluation Guide, *page 65*
- G. Security Classification Guide Preparation, *page 70*
- H. Classified Document and Material Storage Standards and Information, *page 127*
- I. Inspection Checklist for Security Containers, *page 130*
- J. Communist Countries, *page 131*
- K. Classified Material Destruction Standards, *page 132*
- L. Section 793, Title 18, United States Code Gathering, Transmitting, or Losing Defense Information, *page 135*
- M. Section 794, Title 18, United States Code Gathering or Delivering Defense Information to Aid Foreign Government, *page 136*
- N. Section 795, Title 18, United States Code Photographing and Sketching Defense Installations, *page 137*
- O. Section 797, Title 18, United States Code Publication and Sale of Photographs of Defense Installations, *page 138*
- P. Section 798, Title 18, United States Code Disclosure of Classified Information, *page 139*

Index

RESERVED

Chapter 1 General Provisions

Section 1 References

1-100. References

- a. DoD Directive 5200.1, "DoD Information Security Program" June 7, 1982
- b. Executive Order (E.O.) 12356, "National Security Information," April 2, 1982
- c. Information Security Oversight Office Directive No. 1, "National Security Information," June 23, 1982
- d. DoD Directive 5220.22, "Department of Defense Industrial Security Program," December 8, 1980. **AR 380-49 (Industrial Security)**
- e. DoD 5220.22-R, "Industrial Security Regulation," December 1985 (or current edition). **AR 380-49 (Industrial Security)**
- f. DoD 5220.22-M, "Industrial Security Manual for Safeguarding Classified Information," November 1986 (or current edition). **AR 380-49 (Industrial Security)**
- g. Public Law 83-703, "Atomic Energy Act of August 30, 1954," as amended
- h. DoD Directive 5200.28, "Security Requirements for Automatic Data Processing (ADP) Systems," December 18, 1972. **AR 18-7 (Data Processing Installation Management Procedures and Standards); AR 380-380 (Automation Security)**
- i. DoD 5200.28-M, "ADP Security Manual: Techniques and Procedures for Implementing, Deactivating, Testing, and Evaluating Secure Resource-Sharing ADP Systems," January 1973
- j. E.O. 12333, "United States Intelligence Activities," December 4, 1981
- k. DoD Directive 5400.7, "DoD Freedom of Information Act Program," March 24, 1980. **AR 340-17 (Release of Information and Records from Army Files)**
- l. Title 35, United States Code, Sections 181-188, "The Patent Secrecy Act of 1952"
- m. DoD Directive 5400.11, "Department of Defense Privacy Program," June 9, 1982. **AR 340-21 (The Army Privacy Program)**
- n. DoD 5200.1-H, "Writing Security Classification Guidance Handbook," October 1980
- o. DoD 5200.1-I, "DoD Index of Security Classification Guides"¹
- p. DoD Directive 5535.2, "Delegations of Authority to Secretaries of the Military Departments—Inventions and Patents," October 16, 1980. **AR 27-60 (Patents, Inventions, and Copyrights)**
- q. DoD Directive 5200.30, "Guidelines for Systematic Review of 20-Year-Old Classified Information in Permanently Valuable DoD Records," September 9, 1981
- r. Title 31, United States Code, Section 483a (Title 5, Independent Offices Appropriation Act)
- s. DoD Instruction 7230.7 "User Charges," June 12, 1979. **AR-37-30 User Charges)**
- t. DoD Directive 7920.1, "Life-Cycle Management of Automated Information Systems (AIS)," October 17, 1978
- u. DoD Instruction 5230.22, "Control of Dissemination of Intelligence Information," April 1, 1982. **AR 381-1 (Control of Dissemination of Intelligence Information); AR 105-31 (Record Communications)**
- v. National COMSEC Instruction 4005, "Safeguarding and Control of COMSEC Material," October 12, 1979. **AR 380-40 ((C) Policy for Safeguarding and Controlling COMSEC Information(U)); TB 380-41 (Procedures for Safeguarding, Accounting, and Supply Control of COMSEC Material)**
- w. National Communications Security Committee (NCSC) Policy Directive 6, January 16, 1981
- x. DoD Directive C-5200.5, "Communications Security (COMSEC) (U)," October 6, 1981
- y. DoD Directive 5210.2, "Access to and Dissemination of Restricted Data," January 12, 1978. **AR 380-150 (Access to and Dissemination of Restricted Data)**
- z. DoD Directive 5100.55, "United States Security Authority for North Atlantic Treaty Organization Affairs," April 21, 1982. **AR 380-15 ((C) Safeguarding Classified NATO Information (U))**
- aa. Joint Army-Navy-Air Force Publications (JANAP) #119 and #299
- bb. DoD Directive 5240.6, "Counter-intelligence Awareness and Briefing Program," February 26, 1986
- cc. E.O. 12065, "National Security Information," June 28, 1978
- dd. DoD Directive 5210.56, "Use of Force by Personnel Engaged in Law Enforcement and Security Duties," May 10, 1969. **AR 190-28 (Use of Force by Personnel Engaged in Law Enforcement and Security Duties)**
- ee. DoD Directive 5050.47, "National Supply System," May 27, 1971
- ff. Memorandum by the Secretary, Joint Chiefs of Staff (SM)701-76, Volume II, "Peacetime Reconnaissance and Certain Sensitive Operations," July 23, 1976
- gg. DoD Directive 3224.3, "Physical Security Equipment: Assignment of Responsibility for Research, Engineering, Procurement, Installation, and Maintenance," December 1, 1976
- hh. National COMSEC Instruction 4009, "Protected Distribution Systems," December 30, 1981
- ii. DoD Directive 5200.12, "Policy on the Conduct of Meetings Involving Access to Classified Information," September 24, 1984
- jj. DoD Instruction 5240.4, "Reporting of Counterintelligence and Criminal Violations," July 28, 1983. **AR 381-12 (Subversion and Espionage Directed Against U.S. Army (SAEDA))**
- kk. DoD Directive 5210.50, "Unauthorized Disclosure of Classified Information to the Public," October 18, 1982
- ll. DoD 5200.2-R, "DoD Personnel Security Program," January 1987. **AR 604-5 (Clearance of Personnel for Access to Classified Defense Information and Material)**
- mm. DoD Directive 5400.4, "Provision of Information to Congress," January 30 1978. **AR 1-20 (Legislative Liaison)**
- nn. DoD Directive 7650.1, "General Accounting Office Comprehensive Audits," July 9, 1958. **AR 36-2 (Processing Internal and External Audit Reports and Follow-Up on Findings and Recommendations)**
- oo. DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," December 31, 1984
- pp. Title 50, United States Code, Section 403, "National Security Act"
- qq. DoD Directive 4540.1, "Use of Air-space for United States Military Aircraft and Firings Over the High Seas," January 31, 1981
- rr. DoD Directive 5210.41, "Security Criteria and Standards for Protecting Nuclear Weapons," September 12, 1978
- ss. DoD Instruction 1000.13, "Identification Cards for Members of the Uniformed Services, Their Dependents, and Other Eligible Personnel," July 16, 1979
- tt. Public Law 76-443, "Espionage Act," March 28, 1940
- uu. Title 10, United States Code, Section 801 et seq. "Uniform Code of Military Justice"
- vv. Allied Communications Publication (ACP) # 110
- ww. DoD Directive 5230.24, "Distribution Statements on Technical Documents," November 20, 1984
- xx. DoD 5200.1-PH-1, "Classified Information Nondisclosure Agreement (SF 189)," July 1985. **DA Circular 380-85-1 (Department of the Army Implementing Instructions for the Classified Information Nondisclosure Agreement, SF 189)**
- yy. DoD 5200.1-PH, "A Guide to Marking Classified Documents," November 1982
- zz. DoD Directive C-5230.23, "Intelligence Disclosure Policy," November 18, 1983

¹ Published on an annual basis.

aaa. DoD Instruction 5230.20, "Control of Foreign Representatives," June 25, 1984

bbb. DoD TS-5105.21-M-2, "SCI Security Manual—Communications Intelligence Policy," July 1985

ccc. DoD C-5105.21-M-1, "SCI Security Manual—Administrative Security," January 1985. **AR 380-35 (SCI Security Manual—Administrative Security); TB 380-35 ((C) Security, Use, and Dissemination of Sensitive Compartmented Information (SCI) (U))**

ddd. DoD TS-5105.21-M-3, "SCI Security Manual—TK Policy," November 1985

eee. National COMSEC Instruction 4003, "Classification Guidelines for COMSEC Information," December 1, 1978

fff. National COMSEC Instruction 4006, "Reporting COMSEC Insecurities," October 20, 1983

ggg. National Telecommunications and Information Systems Security Instruction 4001, "Controlled Cryptographic Items," March 25, 1985

hhh. National COMSEC Instruction 4008, "Safeguarding COMSEC Facilities," March 4, 1983

iii. DoD Directive 5405.2, "Release of Official Information in Litigation and Testimony by DoD Personnel as Witnesses," July 23, 1985

jjj. **AR 1-210 (Participation in Activities of Private Associations)**

kkk. **AR 25-400-2 (The Modern Army Recordkeeping System (MARKS))**

lll. **AR 310-10 (Military Orders)**

mmm. **AR 340-2 (Maintenance and Disposition of Records in TOE Units of the Active Army, the Army Reserve, and the National Guard)**

nnn. **AR 340-25 (Mailing Procedures for Certain U.S. Army Activities and U.S. Citizens Overseas)**

ooo. **AR 381-20 (U.S. Army Counterintelligence (CI) Activities)**

ppp. **AR 525-10 ((C) Department of the Army Command and Control Reporting System (Short Title: DAXREP))**

qqq. **AR 530-1 (Operations Security (OPSEC))**

rrr. **AR 530-4 ((S) Control of Compromising Emanations (U))**

sss. **FM 19-30 (Physical Security)**

ttt. **DoD Directive 5230.9 (Clearance of DoD Information for Public Release) AR 360-5 (Public Information)**

uuu. **AR 380-10 (Information Disclosure, Visits and Accreditation of Foreign Nationals)**

vvv. **AR 15-6 (Procedures for Investigating Officers and Boards of Officers)**

www. **AR 310-1 (Publications, Blank Forms, and Printing Management)**

xxx. **AR 638-1 (Disposition of Personal Effects of Deceased and Missing Persons)**

yyy. **AR 530-2 (Communications Security)**

zzz. **AR 335-15 (Management Information Control System)**

aaaa. **AR 380-381 ((C) Special Access Programs (U)); DA Pamphlet 380-381 (Security for Special Access Programs)**

bbbbb. **DoD Directive 5205.7 (Special Access Programs (SAPs)), June 5, 1987.**

Section 2

Purpose and Applicability

1–200. Purpose

Information of the Department of Defense relating to national security shall be protected against unauthorized disclosure as long as required by national security considerations. This Regulation establishes a system for classification, downgrading, and declassification of information; sets forth policies and procedures to safeguard such information; and provides for oversight and administrative sanctions for violations. **This regulation gives instructions and**

assigns responsibilities for the effective implementation and application of DoD Information Security Program policies at all levels of DA.

1–201. Applicability

This Regulation governs the DoD Information Security Program and takes precedence over all DoD Component regulations that implement that Program. Under references (a), (b), and (c) it establishes, for the Department of Defense, uniform policies, standards, criteria, and procedures for the security classification, downgrading, declassification, and safeguarding of information that is owned by, produced for or by, or under the control of the Department of Defense or its Components. **This regulation applies to all military and civilian members of the Active Army, Army National Guard (ARNG), and US Army Reserve (USAR). Any violation of its requirements may subject Service members to disciplinary action under article 92, Uniform Code of Military Justice (UCMJ) civilian personnel may be subject to adverse action under Civilian Personnel Regulations (CPRs).**

1–202. Nongovernment operations

Except as otherwise provided herein, the provisions of this Regulation that are relevant to operations of nongovernment personnel entrusted with classified information shall be made applicable thereto by contracts or other legally binding instruments. (See DoD Directive 5220.22, DoD 5220.22-R, and DoD 5220.22-M, references (d), (e) and (f).)

1–203. Combat operations

The provisions of this Regulation relating to accountability, dissemination, transmission, or safeguarding of classified information may be modified by military commanders but only to the extent necessary to meet local conditions in connection with combat or combat-related operations. Classified information should be introduced into forward combat areas or zones or areas of potential hostile activity only when essential to accomplish the military mission. Military commanders should consider modification of this regulation if their tactical force are deployed against a potential enemy force with the expectation that hostilities are imminent. (See also paragraph 5-203.)

1–204. Atomic energy material

Nothing in this Regulation supersedes any requirement related to "Restricted Data" in the Atomic Energy Act of August 30, 1954, as amended (reference (g)), or the regulations of the Department of Energy under that Act. "Restricted Data" and material designated as "Formerly Restricted Data," shall be handled, protected, classified, downgraded, and declassified to conform with reference (g) and the regulations issued pursuant thereto.

1–205. Sensitive compartmented and communications security information

a. Sensitive Compartmented Information (SCI) and Communications Security (COM-SEC) Information shall be handled and controlled in accordance with applicable national directives and DoD Directives and Instructions. Other classified information, while in established SCI or COMSEC areas, may be handled in the same manner as SCI or COMSEC information. Classification principles and procedures, markings, downgrading, and declassification actions prescribed in this Regulation apply to SCI and COMSEC information. (See also paragraph 13-200 c.)

b. Pursuant to DoD Directive 5200.1 (reference (a)), the Director, National Security Agency/Chief, Central Security Service may prescribe special rule and procedures for the handling, reporting of loss, storage, and access to classified communications security devices, equipments, and materials in mobile, hand-held or transportable systems, or that are used in conjunction with commercial telephone systems, or in similar circumstances where operational demands preclude the application of standard safeguards. These special rules

may include procedures for safeguarding such devices and materials, and penalties for the negligent loss of government property.

1-206. Automatic data processing systems

This Regulation applies to protection of classified information processed, stored or used in, or communicated, displayed or disseminated by an automatic data processing (ADP) system. Additional security policy, responsibilities, and requirements applicable specifically to ADP systems are contained in DoD Directive 5200.28 and DoD 5200.28-M, references (h) and (i).

Section 3 Definitions

1-300. Access

The ability and opportunity to obtain knowledge of classified information.

1-301. Applicable doubted markings

The markings, other than classification markings, and warning notices listed or referred to in subsection 4-103.

1-302. Carve-out

A classified contract issued in connection with an approved Special Access Program in which the Defense Investigative Service has been relieved of inspection responsibility in whole or in part under the Defense Industrial Security Program.

1-303. Classification authority

The authority vested in an official of the Department of Defense to make an initial determination that information requires protection against unauthorized disclosure in the interest of national security.

1-304. Classification guide

A document issued by an authorized original classifier that prescribes the level of classification and appropriate declassification instructions for specified information to be classified derivatively. For purposes of this Regulation, this term does not include DD Form 254, "Contract Security Classification Specification."

1-305. Classified Information

Information or material that is (a) owned by, produced for or by, or under the control of the U.S. Government; and (b) determined under E.O. 12356 (reference (b)) or prior orders and this Regulation to require protection against unauthorized disclosure; and (c) so designated.

1-305.1. Classified meeting

A conference, seminar, symposium, exhibit, convention, or other gathering that is conducted by a DoD Component, or by a cleared DoD contractor, an association, institute, or society with DoD approved and sponsorship, during which classified information is disclosed.

1-306. Classifier

An individual who makes a classification determination and applies a security classification to information or material. A classifier may be an original classification authority or a person who derivatively assigns a security classification based on a properly classified source or a classification guide.

1-307. Communications security (COMSEC)

The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from the possession and study of telecommunications and to ensure the authenticity of such communications. COMSEC includes cryptosecurity, emission security, transmission security, and physical security of COMSEC material and information.

1-308. Compromise

The disclosure of classified information to persons not authorized access thereto.

1-309. Confidential source

Any individual or organization that has provided, or that may reasonably be expected to provide, information to the United States on matters pertaining to the national security with the expectation, expressed or implied, that the information or relationship, or both, be held in confidence.

1-310. Continental United States (CONUS)

United States territory, including adjacent territorial waters, located within the North American continent between Canada and Mexico.

1-311. Controlled Cryptographic Item (CCI)

A secure telecommunications or information handling equipment ancillary device, or associated cryptographic component, which is unclassified but controlled. (Note: Equipment's and components so designated bear the designator "Controlled Cryptographic Item" or "CCI.")

1-312. Critical Nuclear Weapon Design Information

That Top Secret Restricted Data or Secret Restricted Data revealing the theory of operation or design of the components of a thermonuclear or implosion-type fission bomb, warhead, demolition munition or test device. Specifically excluded is information concerning arming, fuzing, and firing systems; limited life components; and total contained quantities of fissionable, fusionable, and high explosive materials by type. Among these excluded items are the components which DoD personnel set, maintain, operate, test, or replace.

1-313. Custodian

An individual who has possession of or is otherwise charged with the responsibility for safeguarding or accounting for classified information.

1-314. Declassification

The determination that classified information no longer requires, in the interest of national security, any degree of protection against unauthorized disclosure, together with a removal or cancellation of the classification designation.

1-315. Declassification event

An event that eliminates the need for continued classification of information. **"Upon Notification of Originator (OADR)" is not a declassification event.**

1-316. Derivative classification

A determination that information is in substance the same as information currently classified, and the application of the classification markings.

1-317. Document

Any recorded information regardless of its physical form or characteristics, including, without limitation, written or printed matter, data processing cards and tapes, maps, charts, paintings, drawings, engravings, sketches, working notes and papers, or reproductions by any means or process, and sound, voice, magnetic or electronic recordings in any form.

1-318. DoD component

The Office of the Secretary of Defense (OSD), the Military Departments, the Organization of the Joint Chiefs of Staff (OJCS), the Unified and Specified Commands, and the Defense Agencies.

1-319. Downgrade

A determination that classified information requires, in the interest of national security, a lower degree of protection against unauthorized disclosure than currently provided, together with a

changing of the classification designation to reflect such lower degree of protection.

1-320. Foreign government Information

Information that is (a) provided to the United States by a foreign government or governments, an international organization of governments, or any element thereof with the expectation, expressed or implied, that the information, the source of the information, or both, are to be held in confidence; or (b) produced by the United States pursuant to or as result of a joint arrangement with a foreign government or governments or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence.

1-320.1. Foreign national

A person who is not a citizen or national of, or immigrant alien to, the United States.

1-320.2. Foreign representative

Either a foreign national or a representative of a foreign interest (RFI). (See item 1-329.1 below.)

1-321. Formerly Restricted Data

Information removed from the Restricted Data category upon a joint determination by the Department of Energy (or antecedent agencies) and the Department of Defense that such information relates primarily to the military utilization of atomic weapons and that such information can be safeguarded adequately as classified defense information. For purposes of foreign dissemination, however, such information is treated in the same manner as Restricted Data.

1-321.1. Government installation/facility

A U.S. military or civilian facility in a fixed location. This includes the facility's buildings, building equipment, and subsidiary facilities such as access and perimeter fencing. A commercial facility, when wholly or partially leased, is considered to be a Government facility, when under U.S. Government control.

1-322. Information

Knowledge that can be communicated by any means.

1-323. Information security

The result of any system of policies and procedures for identifying, controlling, and protecting from unauthorized disclosure, information whose protection is authorized by executive order or statute.

1-324. Intelligence activity

An activity that an agency within the Intelligence Community is authorized to conduct under E.O. 12333 (reference (j)).

1-325. Material

Any product or substance on, or in which, information is embodied.

1-326. National security

The national defense and foreign relations of the United States.

1-327. Need-to-know

A determination made by a possessor of classified information that a prospective recipient, in the interest of national security, has a requirement for access to, or knowledge, or possession of the classified information in order to accomplish lawful and authorized Government purposes.

1-328. Original classification

An initial determination that information requires, in the interest of national security, protection against unauthorized disclosure, together with a classification designation signifying the level of protection required.

1-329. Regrade

A determination that classified information requires a different degree of protection against unauthorized disclosure than currently provided, together with a change of classification designation that reflects such different degree of protection.

1-329.1. Representatives of a foreign interest

Citizens or nationals of the United States or immigrant aliens who, in their individual capacities or on behalf of a corporation (whether as corporate officers or officials, or as corporate employees who are personally involved with the foreign interest), are acting as representatives, officials, agents, or employees of a foreign government, firm, corporation, international organization (such as the North Atlantic Treaty Organization), or person. However, a U.S. citizen or national who has been appointed by his or her U.S. employer to be its representative in the management of a foreign subsidiary (that is, a foreign firm in which the U.S. firm has ownership of at least 51 percent of the voting stock) will not be considered a representative of a foreign interest solely because of this employment, provided the appointing employer is his or her principal employer and is a firm that possesses or is in the process of obtaining a facility security clearance.

1-330. Restricted Data

All data concerning (a) design, manufacture or utilization of atomic weapons; (b) the production of special nuclear material; or (c) the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted Data category under Section 142 of reference (g). (See also Section 115, Atomic Energy Act of 1954, as amended, and "Formerly Restricted Data," subsection 1-318.)

1-331. Security clearance

A determination that a person is eligible under the standards of DoD 5200.2-R (reference (11)) for access to classified information.

1-331.1. Security representative

An official of the sponsoring Army activity responsible for supervising all security aspects of a classified meeting.

1-332. Sensitive compartmented information

Information and material that requires special controls for restricted handling within compartmented intelligence systems and for which compartmentation is established.

1-333. Special Access Program

Any program imposing need-to-know or access controls beyond those normally required for access to Confidential, Secret, or Top Secret information. Such a program includes, but is not limited to, special clearance, adjudication, or investigative requirements; special designation of officials authorized to determine need-to-know; or special lists of persons determined to have a need-to-know.

1-334. Special activity

An activity, or functions in support of such activity, conducted in support of national foreign policy objectives abroad that is planned and executed so that the role of the U.S. Government is neither apparent nor acknowledged publicly; but that is not intended to influence U.S. political processes, public opinion, policies, or media, and does not include diplomatic activities or the collection and production of intelligence or related support functions.

1-335. Unauthorized disclosure

A communication or physical transfer of classified information to an unauthorized recipient.

1-336. United States and its territories, possessions, administrative, and commonwealth areas

The 50 States; the District of Columbia; the Commonwealth of Puerto Rico; the Territories of Guam, American Samoa, and the

Virgin Islands; the Trust Territory of the Pacific Islands; **U.S. operations in Panama; and the Possessions, Midway and Wake Islands.**

1-337. Upgrade

A determination that certain classified information requires, in the interest of national security, a higher degree of protection against unauthorized disclosure than currently provided, together with a changing of the classification designation to reflect such higher degree.

Section 4 Policies

1-400. Classification

a. Basic policy. Except as provided in the Atomic Energy Act of 1954, as amended (reference (g)), E.O. 12356 (reference (b)), as implemented by the ISOO Directive No. 1 (reference (c)), and this Regulation, provides the only basis for classifying information. It is the policy of the Department of Defense to make available to the public as much information concerning its activities as possible consistent with the need to protect the national security. Accordingly, security classification shall be applied only to protect the national security.

b. Resolution of Doubts. Unnecessary classification and higher than necessary classification should be avoided. If there is reasonable doubt about the need to classify information, it shall be safeguarded as if it were classified "Confidential" pending a determination by an original classification authority, who shall make this determination within 30 days. If there is reasonable doubt about the appropriate level of classification, it shall be safeguarded at the higher level of classification pending a determination by an original classification authority, who shall make this determination within 30 days. Upon a classification determination, markings shall be applied in accordance with Chapter IV.

c. Duration. Information shall be classified as long as required by national security considerations. Each decision to classify requires a simultaneous determination of the duration such classification must remain in force or that the duration of classification cannot be determined.

1-401. Classification

Decisions concerning declassification shall be based on the loss of the information's sensitivity with the passage of time or upon the occurrence of a declassification event.

1-402. Safeguarding

Information classified under this Regulation shall be afforded the level of protection against unauthorized disclosure commensurate with the level of classification assigned under the varying conditions that may arise in connection with its use, dissemination, storage, movement or transmission, and destruction. **Responsible officials will ensure that classified information is adequately protected from compromise. Officials must continually aware of possible threats from all-source intelligence efforts of potential adversaries. Assistance is available from the U. S. Army Intelligence and Security Command (INSCOM) under the Operations Security (OPSEC) Program (See AR 530-1.)**

Section 5 Security Classification Designations

1-500. General

Information or material that requires protection against unauthorized disclosure in the interest of national security shall be classified in one of three designations, namely: "Top Secret," "Secret," or "Confidential." The markings "For Official Use Only," and "Limited Official Use" shall not be used to identify classified information. Moreover, no other term such as "Sensitive," "conference,"

or "Agency" shall be used in conjunction with the authorized classification designations to identify classified information.

1-501. Top Secret

"Top Secret" shall be applied only to information or material the unauthorized disclosure of which reasonably could 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 or technological developments vital to national security.

1-502. Secret

"Secret" shall be applied only to information or material the unauthorized disclosure of which reasonably could 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 or intelligence operations; compromise of significant military plans or intelligence operations; and compromise of significant scientific or technological developments relating to national security.

1-503. Confidential

"Confidential" shall be applied only to information or material the unauthorized disclosure of which reasonably could be expected to cause damage to the national security. Examples of damage include the compromise of information that indicates strength of ground, air, and naval forces in the United States and overseas areas; disclosure of technical information used for training, maintenance, and inspection of classified munitions of war; revelation of performance characteristics, test data, design, and production data on munitions of war.

Section 6 Authority to Classify, Downgrade, and Declassify

1-600. Original classification authority

a. Control. Authority for original classification of information as Top Secret, Secret, or Confidential may be exercised only by the Secretary of Defense, the Secretaries of the Military Departments, and by officials to whom such authority is specifically delegated in accordance with and subject to the restrictions of this Section of the Regulation. In the absence of an original classification authority, the person designated to act in his or her absence may exercise the classifier's authority.

b. Delegation of classification authority. Original classification authority shall not be delegated to persons who only reproduce, extract, or summarize classified information, or who only apply classification markings derived from source material or as directed by a classification guide. Delegations of original classification authority shall be limited to the minimum number required for efficient administration and to those officials whose duties involve the origination and evaluation of information warranting classification at the level stated in the delegation.

(1) *Top Secret.* Only the Secretary of Defense, the Secretaries of the Military Departments, and the senior official designated by each under Section 5.3(a) of E.O. 12356 (reference (b)), provided that official has original Top Secret classification authority, may delegate original Top Secret classification authority. Such delegation may only be made to officials who are determined to have a demonstrable and continuing need to exercise such authority. **Original Top Secret classification authority is an inherent responsibility of the Secretary of the Army, the Under Secretary of the Army, the Chief of Staff, the Vice Chief of Staff, and the Director of the Army Staff. The Deputy Chief of Staff for Intelligence (DCSINT), as the senior designated official under Section 5.3(a)**

of E.O. 12356 within Army, will approve all delegations of original Top Secret classification authority.

(2) *Secret and Confidential*. Only the Secretary of Defense, the Secretaries of the Military Departments, the senior official designated by each under Section 5.3(a) of reference (b), and officials with original Top Secret classification authority, may delegate original Secret and Confidential classification authority to officials whom they determine respectively to have a demonstrable and continuing need to exercise such authority. **Delegation of original SECRET and CONFIDENTIAL classification authority must be approved by the DCSINT.**

(3) Each delegation of original classification authority shall be in writing and shall specify the title of the position held by the recipient.

c. Requests for classification authority

(1) A request for the delegation of original classification authority shall be made only when there is a demonstrable and continuing need to exercise such authority and the following conditions exist:

(a) The normal course of operations or missions of the organization results in the origination of information warranting classification;

(b) There is a substantial degree of local autonomy in operations or missions as distinguished from dependence upon a higher level of command or supervision for relatively detailed guidance;

(c) There is adequate knowledge by the originating level to make sound classification determinations as distinguished from having to seek such knowledge from a higher level of command or supervision; and

(d) There is a valid reason why already designated classification authorities in the originator's chain of command or supervision have not issued or cannot issue classification guidance to meet the originator's normal needs.

(2) Each request for a delegation of original classification authority shall:

(a) Identify the title of the position held by the nominee and the nominee's organization;

(b) Contain a description of the circumstances, consistent with 1., above, that justify the delegation of such authority; and

(c) Be submitted through established channels to the Secretary of Defense, the Secretary of the Military Department concerned, the senior official designated by each under Section 5.3(a) of E.O. 12356 (reference (b)), or the appropriate Top Secret classification authority. (See subsection 1-602.) **Requests will be sent through command channels to HQDA (DAMI-CIS) WASH DC 20310-1051, as soon as the need for a new original classification authority becomes known. This office will notify requesters of the final DCSINT decision in each case.**

d. Training requirements for original classification authorities. Heads of DoD Components shall establish procedures to ensure that all original classification authorities in their Component, to include themselves, are indoctrinated in the fundamentals of security classification, limitations on their authority to classify information, and their responsibilities as such. This indoctrination shall be a prerequisite to the exercise of such authority and shall be a matter of record that is subject to audit. Heads of DoD Components shall ensure this indoctrination is given to all present original classification authorities within 12 months of the effective date of this Regulation.

(1) **Army security managers will develop an original classification authority indoctrination program for their activity which will encompass the following minimum points:**

(a) **E.O. 12356 provides the only basis for classifying information as Top Secret, Secret, or Confidential.**

(b) **The decision to classify information may only be made by an approved original classification authority when he/she determines the unauthorized disclosure of the information could be expected to cause damage to the national security.**

(c) **Original classification authorities will apply a marking of Top Secret material when its unauthorized disclosure could be expected to cause "exceptionally grave damage" to the national security; Secret when its disclosure could be expected to cause**

"serious damage"; or Confidential when its disclosure could be expected to cause "damage" to the national security.

(d) **Original classification authorities will set a specific date or event on which automatic declassification of the information will occur. Information may be classified indefinitely only when a specific date or event cannot be determined. In such cases, the notation "Originating Agency's Determination Required (OADR)" will be applied.**

(e) **Once an original classification authority makes a classification decision, he/she is responsible for conveying that decision to others who have a need for the classified information. In addition, security classification guidance must be applied to industry when classified contracting is involved.**

(f) **Classification cannot be used to conceal violations of law, inefficiency, or administrative error, to prevent embarrassment, nor to restrain competition.**

(2) **Upon receipt of DCSINT approval for exercise of classification authority, security managers (or other knowledgeable individuals), will personally brief the original classification authority prior to exercise of such authority. The briefing should expand upon the information above, as time allows. The name of the original classification authority trained, and the date the briefing was conducted, will be recorded directly on the activity classification authority list and will serve as the official record of training.**

1-601. Derivative classification responsibility

Derivative application of classification markings is a responsibility of those who incorporate, paraphrase, restate, or generate in new form, information that is already classified, or those who apply markings in accordance with guidance from an original classification authority. Persons who apply derivative classifications should take care to determine whether their paraphrasing, restating, or summarizing of classified information has removed all or part of the basis for classification. Persons who apply such derivative classification markings shall:

a. Respect original classification decisions;

b. Verify the information's current level of classification as far as practicable before applying the markings; and

c. Carry forward to any newly created documents the assigned dates or events for declassification and any additional authorized markings.

1-602. Record and report requirements

a. Records of designations of original classification authority shall be maintained as follows (**HQDA (DAMI-CIS) will maintain all required listings for Army**):

(1) *Top Secret authorities*. A current listing by title and organization of officials designated to exercise original Top Secret classification authority shall be maintained by:

(a) The Office of the Deputy Under Secretary of Defense (Policy) (ODUSD(P)) for the Office of the Secretary of Defense; the Organization of the Joint Chiefs of Staff; the headquarters of each Unified Command and the headquarters of subordinate Joint Commands; and the Defense Agencies.

(b) The Offices of the Secretaries of the Military Departments for the officials of their respective departments, including Specified Commands but excluding officials from their respective departments who are serving in headquarters elements of Unified Commands and headquarters of Joint Commands subordinate thereto.

(2) *Secret and Confidential authorities*. A current listing by title and organization of officials designated to exercise original Secret and Confidential classification authority shall be maintained by:

(a) The ODUSD(P) for the Office of the Secretary of Defense.

(b) The offices of the Secretaries of the Military Departments for the officials of their respective departments, including Specified Commands but excluding officials from their respective departments who are serving in headquarters elements of Unified Commands and headquarters elements of Joint Commands subordinate thereto.

(c) The Director, Joint Staff, for the OJCS.

(d) The Commanders-in-Chief of the Unified Commands, for

their respective headquarters and the headquarters of subordinate Joint Commands.

(e) The Directors of the Defense Agencies, for their respective agencies.

(3) If the listing of titles of positions and organizations prescribed in subparagraphs 1. and 2., above, discloses intelligence or other information that either qualifies for security classification protection or otherwise qualifies to be withheld from public release under statute, some other means may be recommended by the DoD Component by which original classification authorities can be readily identified. Such recommendations shall be submitted to ODUSD(P) for approval. **Recommendations will be submitted through command channels to HQDA (DAMI-CIS) WASH DC 20310-1051.**

(4) The listings prescribed in subparagraphs 1. and 2., above, shall be reviewed at least annually by the senior official designated in or pursuant to paragraph 13-200a, or subsections 13-301 or 13-302 or designee to ensure that officials so listed have demonstrated a continuing need to exercise original classification authority. **Changes to designations of classification authorities (such as deletions or changes in position/organization titles) will be reported through command channels to HQDA (DAMI-CIS) WASH DC 20310-1051 as they occur.**

b. The DoD Components that maintain listings of designated original classification authorities shall, upon request, submit copies of such listings to ODUSD(P).

1-603. Declassification and down-grading authority

a. Authority to declassify and downgrade information classified under provisions of this Regulation shall be exercised as follows:

(1) By the Secretary of Defense and the Secretaries of the Military Departments, with respect to all information over which their respective Departments exercise final classification jurisdiction;

(2) By the official who authorized the original classification, if that official is still serving in the same position, by a successor, or by a supervisory official of either; and

(3) By other officials designated for the purpose in accordance with subparagraph b., below.

b. The Secretary of Defense, the Secretaries of the Military Departments, the Chairman of the Joint Chiefs of Staff, the Directors of the Defense Agencies, or their senior officials designated under subsection 13-301 or 13-302 (**the DCSINT**) may designate additional officials at the lowest practicable echelons of command and supervision to exercise declassification and downgrading authority over classified information in their functional areas of interest. **Records of officials so designated shall be maintained in the same manner as prescribed in paragraph 1-602 a.l. for records of designations of original classification authority. Records of declassification authorities will be maintained by HQDA (DAMI-CIS) WASH DC 20310-1051.**

c. **Declassification actions must always consider the current needs of national security and must conform to current Army and DoD policy.**

(1) **Heads of HQDA agencies will do the following:**

(a) **Determine the classification of information related to their staff functions.**

(b) **Assist the Chief of Military History, HQDA (DAMH-HSR), WASH, DC 20310-0200, in downgrading or declassifying material in records repositories, as required.**

(c) **Review noncurrent information for possible declassification when it is withdrawn from storage for reference or when it becomes of interest to the public.**

(2) **Heads of HQDA agencies and commanders of major Army commands (MACOMs) may designate officials at the lowest practicable level to downgrade or declassify information in their functional areas. To the maximum extent possible, trained and experienced military historians should be designated to perform this function. Designations will be reported through command channels to HQDA (DAMI-CIS) WASH DC 20310-1051.**

(3) **The Chief of Military History will do the following**

(a) **Ensure that noncurrent document originated by or transferred to DA and held in records depositories of the National Archives and Records Service (NARA), DA records centers or holding areas, and other agencies and institutions are downgraded and declassified as required.**

(b) **Jointly with the heads of other HQDA agencies ensure that mandatory reviews of classified material are made (see section 3, chapter III), and that systematic reviews are conducted in those subject areas where there is a likelihood of declassification and public or historical interest has demonstrated.**

(c) **Convene working groups to review requests for release of information as necessary. Members of the working groups will be representatives of HQDA agencies with assets in the specific subjects of the requests.**

(4) **The Commanding General, INSCOM, has HQDA responsibility for Army cryptologic matters.**

Chapter II Classification

Section 1 Classification Responsibilities

2-100. Accountability of classifiers

a. Classifiers are accountable for the propriety of the classifications they assign, whether by exercise of original classification authority or by derivative classification.

b. An official who classifies a document or other material and is identified thereon as the classifier is and continues to be an accountable classifier even though the document or material is approved or signed at a higher level in the same organization. (See subsection 4-104.)

2-101. Classification approval

a. When an official signs or approves a document or other material already marked to reflect a particular level of classification, he or she shall review the information contained therein to determine if the classification markings are appropriate. If, in his or her judgment, the classification markings are not supportable, he or she shall, at that time, cause such markings to be removed or changed as appropriate to reflect accurately the classification of the information involved.

b. A higher level official through or to whom a document or other material passes for signature or approval becomes jointly responsible with the accountable classifier for the classification assigned. Such official has discretion to decide whether a subordinate who has classification authority shall be identified as the accountable classifier when he or she has exercised that authority.

2-102. Classification planning

a. Advance classification planning is an essential part of the development of any plan, operation, program, research and development project, or procurement action that involves classified information. Classification must be considered from the outset to assure adequate protection for the information and for the activity itself, and to eliminate impediments to the execution or implementation of the plan, operations order, program, project or procurement action.

b. The official charged with developing any plan, program or project in which classification is a factor, shall include under an identifiable title or heading, classification guidance covering the information involved. The guidance shall conform to the requirements contained in section 4 of this chapter.

2-103. Challenges to classification

If holders of classified information have substantial reason to believe that the information is classified improperly or unnecessarily, they shall communicate that belief to their security manager (subsection 13-304) or the classifier of the information to bring about

any necessary correction. **Direct correspondence with the originator of the information is encouraged. Conflicts will be referred to HQDA (DAMI-CIS) WASH DC 20310-1051, for coordination with appropriate headquarters elements and final decision.**

a. Each DoD Component shall establish procedures whereby holders of classified information may challenge the decision of the classifier.

b. Challenges to classification made under this subsection shall include sufficient description of the information being challenged to permit identification of the information and its classifier with reasonable effort. Challenges to classification shall also include the reason or reasons why the challenger believes that the information is classified improperly or unnecessarily. **DA Form 1575 (Request for/or Notification of Regrading Action) may be used to make a formal challenge. The rationale supporting the challenge will be entered in the "Remarks" section of the form.**

c. Challenges received under this subsection shall be acted upon within 30 days of receipt. The challenger shall be notified of any changes made as a result of the challenge or the reasons why no change is made.

d. Pending final determination of a challenge to classification, the information or document in question shall be safeguarded as required for the level of classification initially assigned.

e. The fact that an employee or military member of the Department of Defense has issued a challenge to classification shall not in any way result in or serve as a basis for adverse personnel action.

f. The provisions of this paragraph do not apply to or affect declassification review actions undertaken under the mandatory review requirements of section 3, Chapter 111 of this Regulation or under the provision DoD Directive 5400.7 (reference (k)).

Section 2 Classification Principles, Criteria, and Considerations

2-200. Reasoned judgment

Reasoned judgment shall be exercised in making classification decisions. A positive basis must exist for classification. Both advantages and disadvantages of classification must be weighed. If, after consideration of the provisions of this section, there is reasonable doubt, the provisions of paragraph 1-400 b. apply.

2-201. Identification of specific information

Before a classification determination is made, each item of information that may require protection shall be identified. This requires identification of that specific information that comprises the basis for a particular national advantage or advantages that, if the information were compromised, would or could be damaged, minimized, or lost, thereby adversely affecting national security.

2-202. Specific classifying criteria

A determination to classify shall be made only by an original classification authority when, first, the information is within categories a. through j., below; and second, the unauthorized disclosure of the information, either by itself or in the context of other information, reasonably could be expected to cause damage to the national security. The determination involved in the first step is separate and distinct from that in the second. Except as provided in subsection 2-203, the fact that the information falls under one or more of the criteria shall not mean that the information automatically meets the damage criteria. Information shall be considered for classification if it concerns:

- a. Military plans, weapons, or operations;
- b. Vulnerabilities or capabilities of systems, installations, projects, or plans relating to the national security;
- c. Foreign government information;
- d. Intelligence activities including special activities, or intelligence sources or methods;
- e. Foreign relations or foreign activities of the United States;
- f. Scientific, technological, or economic matters relating to the national security;

g. U.S. Government programs for safe-guarding nuclear materials or facilities;

h. Cryptology;

i. A confidently source; or

j. Other categories of information that are related to national security and that require protection against unauthorized disclosure as determined by the Secretary of Defense or Secretaries of the Military Departments. Recommendations concerning the need to designate additional categories of information that may be considered for classification shall be forwarded through channels to the appropriate Secretary for determination. Each such determination shall be reported promptly to the Director of Security Plans and Programs, ODUSD(P), for promulgation in an Appendix to this Regulation and reporting to the Director, ISOO.

2-203. Presumption of damage

Unauthorized disclosure of foreign government information (see subsection 11-100), the identity of a confidential foreign source, or intelligence sources or methods is presumed to cause damage to the national security.

2-204. Limitations on classification

a. Classification may not be used to conceal violations of law, inefficiency, or administrative error, to prevent embarrassment to a person, organization or agency, or to restrain competition.

b. Basic scientific research information not clearly related to national security may not be classified. (See also subsection 2-205.)

c. A product of nongovernment research and development that does not incorporate or reveal classified information to which the producer or developer was given prior access may not be classified until and unless the Government acquires a propriety interest in the product. This prohibition does not affect the provisions of the Patent Secrecy Act of 1952 (reference (1)). (See section 7, this chapter.)

d. References to classified documents that do not reveal classified information may not be classified or used as a basis for classification.

e. Classification may not be used to limit dissemination of information that is not classifiable under the provisions of E.O.12356 (reference (b)) or this Regulation or to prevent or delay public release of such information.

f. Information may be classified or reclassified after receiving a request for it under the Freedom of Information Act (reference (k)), the Privacy Act (reference (m)), or the mandatory review provisions of this Regulation (section 3, Chapter III) if such classification is consistent with this Regulation and is accomplished personally and on a document-by-document basis, except as provided in paragraph g., below, by the Secretary or Deputy Secretary of Defense, by the Secretaries or Under Secretaries of the Military Departments, by the senior official designated by each Secretary under section 5.3(a) of reference (b), or by an official with original Top Secret classification authority. (See subsection 2-801.)

g. The Secretary of Defense and the Secretaries of the Military Departments may reclassify information previously declassified and disclosed, and they may classify unclassified information that has been disclosed, if they determine in writing that the information requires protection in the interest of national security and the information may reasonably be recovered. (See subsection 2-801.) Any such reclassification or classification shall be reported to the DUSD(P) for subsequent reporting to the Director, ISOO. **Requests for reclassification will be forwarded through command channels to HQDA (DAMI-CIS), WASH DC 20310-1051. Requests must include complete justification, a description of the circumstances surrounding the disclosure, method of recovery, and a statement that the conditions set forth in paragraph 2-801 can be met. DAMI-CIS will report such instances to ODUSD(P).**

2-205. Classifying scientific research data

Ordinarily, except for information that meets the definition of Restricted Data, basic scientific research or its results shall not be classified. However, classification would be appropriate if the information concerns an unusually significant scientific break-through

and there is sound reason to believe that it is not known or within the state-of-the-art of other nations, and it supplies the United States with an advantage directly related to national security.

2-206. Classifying documents

Each document and portion thereof shall be classified on the basis of the information it contains or reveals. The fact that a document makes reference to a classified document is not a basis for classification unless the reference citation, standing alone, reveals classified information. (See paragraph 2-204d.) The overall classification of a document or group of physically-connected documents shall be at least as high as that of the most highly classified component. The subject or title of a classified document normally should be unclassified. When the information revealed by a subject or title warrants classification, an unclassified short title should be added for reference purposes.

2-207. Classifying material other than documents

a. Items of equipment or other physical objects shall be classified only when classified information may be derived from them by visual observation of their internal or external appearance or structure, or by their operation, test, application, or use. The overall classification assigned to end items of equipment or objects shall be at least as high as the highest classification of any of its integrated parts.

b. If mere knowledge of the existence of the item of equipment or object would compromise or nullify its national security advantage, its existence would warrant classification.

2-208. State of the art and Intelligence

Classification requires consideration of the information available from intelligence sources concerning the extent to which the same or similar information is known or is available to others. It is also important to consider whether it is known, publicly or internationally, that the United States has the information or even is interested in the subject Matter. The state-of-the-art in other nations may often be a vital consideration.

2-209. Effect of open publication

Classified information shall not be declassified automatically as a result of any unofficial publication or inadvertent or unauthorized disclosure in the United States or abroad of identical or similar information. Appearance in the public domain of information currently classified or being considered for classification does not preclude initial or continued classification. However, such disclosures require immediate determination of the degree of damage to the national security and reevaluation of the information to determine whether the publication has so compromised the information that downgrading or declassification is warranted. (See also Chapter VI.) Similar consideration must be given to related items of information in all programs, projects, or items incorporating or pertaining to the compromised items of information. Holders should continue classification until advised to the contrary by a competent government authority. **Correspondence which confirms the appearance or classified information in open source publications and identifies the information in question must be classified at the level of the material that has been subjected to possible compromise.**

2-210. Reevaluation of classification because of compromise

Classified information, and information related thereto, that has been lost or possibly compromised, shall be reevaluated and acted upon as follows:

a. The original classifying authority, upon learning that a loss or possible compromise of specific classified information has occurred, shall prepare a written damage assessment and:

(1) Reevaluate the information involved and determine whether (a) its classification should be continued without change; (b) the specific information, or parts thereof, should be modified to minimize or nullify the effects of the reported compromise and the

classification retained; (c) declassification, downgrading, or upgrading is warranted; and (d) countermeasures are appropriate and feasible to negate or minimize the effect of the compromise.

(2) Give prompt notice to all holders of such information when the determination is within categories (b), (c), or (d) of subparagraph 1., above.

b. Upon learning that a compromise or probable compromise has occurred, any official having original classification jurisdiction over related information shall reevaluate the related information and determine whether one of the courses of action enumerated in subparagraph a.1., above, should be taken or, instead, whether upgrading of the related information is warranted. When such a determination is within categories (b), (c), or (d) of subparagraph a.1., above, or that upgrading of the related items is warranted, prompt notice of the determination shall be given to all holders of the related information. (See Chapter VI.) **Original classifiers within Army will forward one copy of completed segments to their activity security manager for central retention (see paragraph 6-107).**

2-211. Compilation of Information

Certain information that would otherwise be unclassified may require classification when combined or associated with other unclassified information. However, a compilation of unclassified items of information should normally not be classified. In unusual circumstances, classification may be required if the combination of unclassified items of information provides an added factor that warrants classification under subsection 2-202. **Similarly, a higher classification may be assigned to compilation of information if the compilation provides an added factor which warrants higher classification than that of its component parts.** Classification on this basis shall be fully supported by a written explanation that will be provided with the material so classified. (See also subsection 4-203.)

2-212. Extracts of information

Information extracted from a classified source shall be derivatively classified or not classified in accordance with the classification markings shown in the source. The overall and internal markings of the source should supply adequate classification guidance. If internal markings or classification guidance are not found in the source, and no reference is made to an applicable and available classification guide, the extracted information shall be classified according either to the overall marking of the source, or guidance obtained from the classifier of the source material.

Section 3

Duration of Original Classification

2-300. General

When a determination is made by an official with authority to classify originally information as Top Secret, Secret, or Confidential, such official must also determine how long the classification shall remain in effect.

2-301. Duration of classification

a. Information shall be classified as long as required by national security considerations.

b. When it can be determined, a specific date or event for declassification shall be set by the original classification authority at the time the information is classified originally. Such dates or events shall be consistent with national security. Any event specified for declassification shall be an event certain to occur.

c. Original classification authorities may not be able to predetermine a date or event for automatic declassification in which case they shall provide for the indefinite duration of classification (see Chapter IV for the marking "Originating Agency's Determination Required").

d. Information classified under predecessor orders and marked for declassification review shall remain classified until reviewed for

declassification under the provisions of this Regulation (also see paragraph 4-600 b.).

2-302. Subsequent extension of duration of classification

The duration of classification specified at the time of original classification may be extended only by officials with requisite original classification authority and only if all known holders of the information can be notified of such action before the date or event previously set for declassification. Any decision to continue classification of information designated for automatic declassification under E.O. 12065 (reference (cc)) or predecessor orders, other than on a document-by-document basis, shall be reported through HQDA (DAMI-CIS) WASH DC 20310-1051 to the DUSD(P) who shall, in turn, report to the Director, ISOO.

Section 4 Classification Guides

2-400. General

a. A classification guide shall be issued for each classified system, program, plan, or project as soon as practicable before the initial funding or implementation of the system, program, plan or project. **Army program proponents will promptly issue classification guidance for their subject areas. Activities charged with planning and coordinating Army participation in exercises will ensure that adequate classification guidance is provided to all participants. This guidance may either be published as a formal classification guide or included in exercise plans or directives.** Successive operating echelons shall prescribe more detailed supplemental guides that are considered essential to assure accurate and consistent classification. In preparing classification guides, originators should review DoD 5200.1-H (reference (n), **in appendix G of this regulation**).

b. Classification guides shall:

(1) Identify the information elements to be protected, using categorization to the extent necessary to ensure that the information involved can be identified readily and uniformly;

(2) State which of the classification designations (that is, Top Secret, Secret, or Confidential) applies to each element or category of information;

(3) State declassification instructions for each element or category of information in terms of a period of time, the occurrence of an event, or a notation that the information shall not be declassified automatically without approval of the originating agency (**normally, events identified for declassification will be finite; statements such as "Declassify 6 years from the date of generation of document" are prohibited**); and

(4) State any special public release procedures and foreign disclosure considerations.

c. Each classification guide shall be approved personally and in writing by an official who:

(1) Has program or supervisory responsibility over the information or is the senior agency official designated by the Secretary of Defense or Secretaries of the Military Departments in accordance with Section 5.3(a) of E.O. 12356 (reference (b)); and

(2) Is authorized to classify information originally at the highest level of classification prescribed in the guide.

d. **An official as described in 2-400 c. above will also approve personally and in writing all changes, errata sheets, and revision to basic guides that affect a classification. This may be done by signing the record copy of the classification guide, or initialing an action, staffing paper, or Other suitable document. Other holders of the classification guide must be notified of all changes when practicable, but no later than during the scheduled guide review.**

2-401. Multiservice interest

For each classified system, program, project, plan, or item involving more than one DoD Component, a classification guide shall be issued by (a) the element in the Office of the Secretary of Defense

that assumes or is expressly designated to exercise overall cognizance over it; or (b) the DoD Component that is expressly designated to serve as the executive or administrative agent for the particular effort. When there is doubt which Component has cognizance of the information involved, the matter shall be referred to the DUSD(P) for resolution.

2-402. Research, development, test, and evaluation

A program security classification guide shall be developed for each system and equipment development program that involves research, development, test, and evaluation (RDT&E) of classified technical information. For each such program covered by an approved Decision Coordinating Paper (DCP) or Program Objective Memorandum (POM), initial basic classification guidance applicable to technical characteristics of the system or equipment shall be developed and submitted with the proposed DCP or POM to the Under Secretary of Defense for Research and Engineering for approval. A detailed classification guide shall be developed and issued as near in time as possible to the approval of the DCP or POM.

a. **Approval of classification guides for Army research, development, and acquisition activities will be integrated into the materiel acquisition and decision process, under AR 70-1.**

b. **Load security managers must be included early on in initial development of required classification.**

c. **Classification guides become effective when approved by an original classification authority.**

2-403. Project phases

Whenever possible, classification guides shall cover specifically each phase of transition, that is, RDT&E, procurement, production, service use, and obsolescence, with changes in assigned classifications to reflect the changing sensitivity of the information involved.

2-404. Review of classification guides

a. Classification guides shall be reviewed by the originator for currency and accuracy not less than once every 2 years. Changes shall be issued promptly. If no changes are made, the originator shall so annotate the record copy and show the date of the review. **The DD Form 254 (Contract Security Classification Specification) will be reviewed at the same time the classification guide is reviewed (see paragraph 2-901). Heads of HQDA agencies and MACOM commanders responsible for issuing classification guides will set up internal suspense systems to make sure that all guides are reviewed at least once every 2 years. When guides are reviewed and changes or new editions are prepared, declassification dates should not be automatically carried forward, but carefully reevaluated**

b. Classification guides issued before August 1, 1982, that are in current use must be updated to meet the requirements of paragraph 2-400b. Such updating shall be accomplished by the next biennial review. Converting previous declassification determinations directed by classification guides shall be accomplished in accordance with the following:

(1) Automatic declassification dates or events remain in force unless changed by competent authority in accordance with subsection 2-302.

(2) Dates for declassification review shall be changed to automatic declassification dates or provide for the indefinite duration of classification.

2-405. Distribution of classification guides

a. A copy of each approved classification guide and changes thereto other than those covering SCI shall be sent to the Director of Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs), and to the Director of Security Plans and Programs, ODUSD(P). A copy of each approved classification guide covering SCI shall be submitted to and maintained by the Senior Intelligence Officer who has security cognizance over the issuing activity. **Three copies of each approved classification guide (less those for Sensitive Compartmented Information (SCI) and Special Access Programs (SAPs)), and**

changes will be forwarded to HQDA (DAMI-CIS) WASH DC 20310-1051 for review and distribution to OSD. Originators will also furnish guides to all probable users, such as test and evaluation organizations.

b. Two copies of each approved classification guide and its changes shall be sent by the originator to the Administrator, Defense Technical Information Center (DTIC), Defense Logistics Agency, unless such guide is classified Top Secret, or covers SCI, or is determined by the approval authority of the guide to be too sensitive for automatic secondary distribution to DoD Components. Each classification guide forwarded to DTIC must bear distribution statement B, C, D, E, F, or X from DoD Directive 5230.24 (reference(w)) on its front cover or first page if there is no cover.

2-406. Index of security classification guides

a. All security classification guides, except as provided in subparagraph b., below, issued under this Regulation shall be listed in DoD 5200.1-I (reference (o)), on the basis of information provided on DD Form 2024, "DoD Security Classification Guide Data Elements." The originator of each guide shall execute DD Form 2024 when the guide is approved, changed, revised, reissued, or canceled, and when its biennial review is accomplished. The original copy of each executed DD Form 2024 shall be forwarded to the Director of Security Plans and Programs, ODUSD(P), who will maintain the Index. Report Control Symbol DD-POL (B&AR)1418 applies to this information collection system. **The original and two copies of executed DD Form 2024 will be forwarded to HQDA (DAMI-CIS) WASH DC 20310-1051, who will provide copies to ODUSD(P) and OASD(PA) as required.**

b. Any classification guide that because of classification considerations is not listed in accordance with paragraph a., above, shall be reported by the originator to the Director of Security Plans and Programs, ODUSD(P). The report shall include the title of the guide, its date, the classification of the guide, and identification of the originating activity. A separate classified list of such guides will be maintained. Report Control Symbol DD-POL(B&AR)1418 applies to this information collection system. **In such cases, DD Form 2024 appropriately classified, if necessary will be forwarded to HQDA (DAMI-CIS), who will report the required information to ODUSD(P). Blocks 9 and 10 on the DD Form 2024 need not be completed.**

Section 5 Resolution of conflicts

2-500. General

When two or more offices, headquarters, or activities disagree concerning a classification, declassification, or regrading action, the disagreement must be resolved promptly.

2-501. Procedures

If agreement cannot be reached by informal consultation, the matter shall be referred for decision to the lowest superior common to the disagreeing parties. If agreement cannot be reached at the major command (or equivalent) level, the matter shall be referred for decision to the headquarters office having overall classification management responsibilities for the Component. That office shall also be advised of any disagreement at any echelon if prompt resolution is not likely to occur. **Conflicts between Army elements that cannot be resolved at the MACOM level will be referred to the HQDA agency with primary staff cognizance over the information concerned. An information copy of the referral correspondence will be furnished to HQDA (DAMI-CIS) WASH DC 20310-1051. If the appropriate HQDA agency cannot be determined, the conflict will be sent directly to DAMI-CIS.**

2-502. Final decision

Disagreements between DoD Component headquarters, if not resolved promptly, shall be referred for final resolution to the ODUSD(P). **Conflicts between Army elements, or Army elements**

and non-Army activities that may require referral to ODUSD(P) will be promptly reported through command channels to the HQDA agency with primary staff cognizance over the subject area. If the proponent cannot be determined, the case will be referred to HQDA (DAMI-CIS) WASH DC 20310-1051.

2-503. Timing

Action under this section at each level of consideration shall be completed within 30 days. Failure to reach a decision within 30 days shall be cause for referral to the next level for consideration.

Section 6 Obtaining classification Evaluations.

2-600. Procedures

If a person not authorized to classify originates or develops information that he or she believes should be safeguarded, he or she shall:

a. Safeguard the information in the manner prescribed for the intended classification (see paragraph 1-400 b.);

b. Mark the information (or cover sheet) with the intended classification designation prescribed in section 5, chapter I;

c. Transmit the information under appropriate safeguards to an appropriate classification authority for evaluation. The transmittal shall state that the information is tentatively marked to protect it in transit. If such authority is not readily identifiable, the information should be forwarded to a headquarters activity of a DoD Component, to the headquarters office having overall classification management responsibilities for a DoD Component, or to the DUSD(P). A determination whether to classify the information shall be made within 30 days of receipt **and the originator will be notified promptly;**

d. Upon decision by the classifying authority, the tentative marking shall be removed. If a classification is assigned, appropriate markings shall be applied; but

e. In an emergency requiring immediate communication of the information, after taking the action prescribed by paragraphs a. and b., above, transmit the information and then proceed in accordance with paragraph c., above.

Section 7 Information Developed by Private Sources

2-700. General

There are some circumstances in which information not meeting the definition in subsection 1-305 may warrant protection in the interest of national security.

2-701. Patent Secrecy Act

The Patent Secrecy Act of 1952 (reference (1)) provides that the Secretary of Defense, among others, may determine that disclosure of an invention by granting of a patent would be detrimental to national security. See DoD Directive 5535.2(reference (p)). A patent application on which a secrecy order has been imposed shall be handled as follows within the Department of Defense:

a. If the patent application contains information that warrants classification, it shall be assigned a classification and be marked and safeguarded accordingly.

b. If the patent application does not contain information that warrants classification, the following procedures shall be followed:

(1) A cover sheet (or cover letter for transmittal) shall be placed on the application with substantially the following language: "The attached material contains information on which secrecy orders have been issued by the U.S. Patent Office after determination that disclosure would be detrimental to national security (Patent Secrecy Act of 1952, 35 U.S.C. 181-188). Its transmission or revelation in any manner to an unauthorized person is prohibited by law. Handle as though classified CONFIDENTIAL (or such other classification as would have been assigned had the patent application been within the definition provided in subsection 1-305)."

(2) The information shall be withheld from public release; its dissemination within the Department of Defense shall be controlled;

the applicant shall be instructed not to disclose it to any unauthorized person; and the patent application (or other document incorporating the protected information) shall be safeguarded in the manner prescribed for equivalent classified material.

c. If filing of a patent application with a foreign government is approved under provisions of the Patent Secrecy Act of 1952 (reference (1)) and agreements on interchange of patent information for defense purposes, the copies of the patent application prepared for foreign registration (but only those copies) shall be marked at the bottom of each page as follows:

Withheld under the Patent Secrecy Act of 1952 (35 U.S.C.181-188).

Handle as CONFIDENTIAL (or such other level as has been determined).

2-702. Independent research and development

a. Information in a document or material that is a product of government-sponsored independent research and development conducted without access to classified information may not be classified unless the government first acquires a proprietary interest in such product.

b. If no prior access was given but the person or company conducting the independent research or development believes that protection may be warranted in the interest of national security, the person or company should safeguard the information in accordance with subsection 2-600 and submit it to an appropriate DoD element for evaluation. The DoD element receiving such a request for evaluation shall make or obtain a determination whether a classification would be assigned if it were government information. If the determination is negative, the originator shall be advised that the information is unclassified. If the determination is affirmative, the DoD element shall make or obtain a determination whether a proprietary interest in the research and development will be acquired. If so, the information shall be assigned proper classification. If not, the originator shall be informed that there is no basis for classification and the tentative classification shall be canceled.

2-703. Other private information

The procedure specified in subsection 2-600 shall apply in any case not specified in subsection 2-702, such as an unsolicited contract bid, in which private information is submitted to a DoD element for a determination of classification.

Section 8 Regrading

2-800. Raising to a higher level of classification

The upgrading of classified information to a higher level than previously determined by officials with appropriate classification authority and jurisdiction over the subject matter is permitted only when all known holders of the information (a) can be notified promptly of such action, and (b) are authorized access to the higher level of classification, or the information can be retrieved from those not authorized access to information at the contemplated higher level of classification. **Additionally, if properly classified information, through administrative or other error, is issued as unclassified or classified at a lower level than necessary, every effort will be made to retrieve, safeguard, and properly mark and control it.**

2-801. Classification of information previously determined to be unclassified

Unclassified information, once communicated as such, may be classified only when the classifying authority (a) makes the determination required for upgrading in subsection 2-800; (b) determines that control of the information has not been lost by such communication and can still be prevented from being lost; and (c) in the case of information released to secondary distribution centers, such as the

DTIC, determines that no secondary distribution has been made and can still be prevented (see also paragraphs 2-204 f. and 2-204 g.)

2-802. Notification

All known holders of information that has been upgraded shall be notified promptly of the upgrading action.

2-803. Downgrading

When it will serve a useful purpose, original classification authorities may, at the time of original classification, specify that downgrading of the assigned classification will occur on a specified date or upon the occurrence of a stated event.

Section 9 Industrial Operations

2-900. Classification in Industrial operations

Classification of information in private industrial operations shall be based only on guidance furnished by the government. Industrial management may not make original classification determinations and shall implement the classification decisions of the U.S. Government contracting authority.

2-901. Contract Security Classification Specification

DD Form 254, "Contract Security Classification Specification," shall be used to convey contractual security classification guidance to industrial management. **A copy of the security classification guide for a project or system may be attached to the DD Form 254. When original classification guidance is provided to a contractor via DD Form 254, and such guidance also will be needed by Government agencies or other contractors, a classification guide will be developed.** DD Forms 254 shall be changed by the originator to reflect changes in classification guidance and reviewed for currency and accuracy not less than once every 2 years. **Reviews will be made at the same time as reviews of associated security classification guides.** Changes shall conform with this Regulation and DoD 5220.22-R and DoD 5220.22-M (references (e) and (f)) and shall be provided to all holders of the DD Form 254 as soon as possible. When no changes are made as a result of the biennial review, the originator shall so notify all holders of the DD Form 254 in writing. **Reviews of DD Forms 254 will consider any difficulties or problems that have surfaced during use of the guidance, and should ensure that—**

a. **Classification is provided all contractors involved in procurement associated with the program.**

b. **Classification decisions have been personally approved by an individual with the requisite classification authority.**

c. **The guidance is current and conforms with that found in other sources. Staffing with technical experts is mandatory.**

d. **The guidance is specific and unambiguous Any problems encountered with interpretation of the guidance are specifically addressed and resolved.**

Chapter III Declassification and Downgrading

Section 1 General Provisions

3-100. Policy

Information classified under E.O. 12356 (reference (b)) and prior orders shall be declassified or downgraded as soon as national security considerations permit. Decisions concerning declassification shall be based on the loss of sensitivity of the information with the passage of time or on the occurrence of an event that permits declassification. Information that continues to meet the classification requirements of subsection 2-202 despite the passage of time will continue to be protected in accordance with this Regulation.

3-101. Responsibility of officials

Officials authorized under subsection 1-603 to declassify or downgrade information that is under the final classification jurisdiction of the Department of Defense shall take such action in accordance with this Chapter.

3-102. Declassification coordination

DoD Component declassification review of classified information shall be coordinated with any other DoD or non-DoD office, Component, or agency that has a direct interest in the subject matter.

3-103. Declassification by the Director of the ISOO

If the Director of the ISOO determines that information is classified in violation of reference (b), the Director may require the activity that originally classified the information to declassify it. Any such decision by the Director may be appealed through the Director of Security Plans and Programs, ODUSD(P), to the National Security Council (NSC). The information shall remain classified pending a prompt decision on the appeal. **Appeals of decision by the Director of the ISOO will be forwarded to HQDA (DAMI-CIS) WASH DC 20310-1051.**

Section 2 Systematic Review

3-200. Assistance to the Archivist of the United States

The Secretary of Defense and the Secretaries of the Military Departments shall designate experienced personnel to assist the Archivist of the United States in the systematic review of classified information. Such personnel shall:

- a.* Provide guidance and assistance to National Archives and Records Administration (NARA) employees in identifying and separating documents and specific categories of information within documents that are deemed to require continued classification; and
- b.* Refer doubtful cases to the DoD Component having classification jurisdiction over the information or material for resolution.

3-201. Systematic review guideline

The Director of Security Plans and Programs, ODUSD(P), in coordination with DoD Components, shall review, evaluate, and recommend revisions of DoD Directive 5200.30 (reference (q)) at least every 5 years.

3-202. Systematic review procedures

a. Except as noted in this subsection, classified information transferred to the NARA that is permanently valuable will be reviewed systematically for declassification by the Archivist of the United States with the assistance of the DoD personnel designated for that purpose under subsection 3-200 as it becomes 30 years old. Information concerning intelligence (including special activities), sources, or methods created after 1945, and information concerning cryptology created after 1945, accessioned into the NARA will be reviewed systematically as it becomes 50 years old. Such information shall be downgraded or declassified by the Archivist of the United States under E.O. 12356, the directives of the ISOO, and reference(q).

b. All DoD classified information that is permanently valuable and in the possession or control of DoD Components, including that held in Federal Records Centers or other storage areas, may be reviewed systematically for declassification by the DoD Component exercising control of such information. Systematic declassification review conducted by DoD Components and personnel designated under subsection 3-200 shall proceed as follows:

(1) Information over which the Department of Defense exercises exclusive or final original classification authority and that under reference (q), the responsible reviewer determines is to be declassified, shall be marked accordingly.

(2) Information over which the Department of Defense exercises exclusive or final original classification authority that, after review, is determined to warrant continued protection shall remain classified as long as required by national security considerations.

c. Classified information over which the Department of Defense does not exercise exclusive or final original classification authority encountered during DoD systematic review may not be declassified unless specifically authorized by the agency having classification jurisdiction over it. **Restricted Data (RD) and Formerly Restricted Data to (FRD) information is included in this category. Assistance in reviewing RD and FRD information is available from Office of Classification, U.S. Department of Energy, WASH DC 20585.**

d. **The Chief of Military History, assisted by the heads of HQDA agencies, is responsible for the review of pertinent materials held in NARA depositories, when appropriate.**

e. **The custodians of materials held in Army or other non-NARA depositories (such as technical libraries, museums, centers, and institutions) may perform systematic declassification reviews of permanent records as explained in the AR 340-18 series.**

3-203. Systematic review of classified cryptologic information

Notwithstanding any other provision of this Regulation, systematic review and declassification of classified cryptologic information shall be conducted in accordance with special procedures developed in consultation with affected agencies by the Director, National Security Agency/Chief, Central Security Service, and approved by the Secretary of Defense under E.O. 12356 and DoD Directive 5200.30 (reference (b) and (q)).

3-204. Systematic review of intelligence information

Systematic review for declassification of classified information pertaining to intelligence activities (including special activities), or intelligence sources or methods shall be in accordance with special procedures to be established by the Director of Central Intelligence after consultation with affected agencies.

Section 3 Mandatory Declassification Review

3-300. Information covered

Upon request by a U.S. citizen or permanent resident alien, a federal agency, or a state or local government to declassify and release such information, any classified information (except as provided in subsection 3-301) shall be subject to review by the originating or responsible DoD Component for declassification in accordance with this section.

3-301. Presidential information

Information originated by a President, the White House staff, committees, commissions, or boards appointed by the President, or others specifically providing advice and counsel to a President or acting on behalf of a President is exempt from the provisions of this section.

3-302. Cryptologic Information

Requests for the declassification review of cryptologic information shall be processed in accordance with the provisions of DoD Directive 5200.30 (reference (q)).

3-303. Submission of requests for mandatory declassification review

Requests for mandatory review of DoD classified information shall be submitted as follows:

a. Requests shall be in writing and reasonably describe the information sought with sufficient particularity to enable the Component to identify documents containing that information, and be reasonable in scope; for example, the request does not involve such a large number or variety of documents as to leave uncertain the identity of the particular information sought.

b. Requests shall be submitted to the Office of the Assistant Secretary of Defense (Public Affairs) (ASD(PA)) (entry point for OSD records), the Military Department, or other Component most

concerned with the subject matter that is designated under DoD Directive 5400.7 (reference (k)) to receive requests for records under the Freedom of Information Act. These offices are identified in appropriate Parts of Title 32 of the Code of Federal Regulations for each DoD Component.

(1) Requests for declassification review of materials in NARA Federal records centers will be processed in the following manner:

(a) The proponent who created and retired the records will be responsible for retrieving them from the appropriate NARA center and conducting a declassification review under current classification guides.

(b) If the creator of the material cannot be located, the Chief of Military History, HQDA (DAMH-HSR), WASH-DC 20314-0200, will review the information. The Chief of Military History will coordinate the declassification of information with the head of the HQDA agency exercising final and exclusive classification authority over the material. If the information cannot be declassified, the request will be denied under paragraph 3-304c and AR 340-17.

(2) Custodians will handle requests for declassification review of materialS in Army or other non-NARA depositories under established DoD guidelines. When DoD guidelines do not apply, and denial is evident, the Chief of Military History must be consulted before the requestor is given a final decision. The Chief of Military History will further process requests as needed. The policy in para 1, above, applies.

3-304. Requirements for processing

Unless otherwise directed by the ASD(PA), requests for mandatory review shall be processed as follows:

a. The designated office shall acknowledge receipt of the request. When a request does not satisfy the conditions of paragraph 3-303a., the requestor shall be notified that unless additional information is provided or the scope of the request narrowed, no further action will be undertaken.

b. DoD Component action upon the initial request shall be completed within 60 days (45 working days). If no determination has been made within 60 days (45 working days) of receipt of the request, the requestor shall be notified of his right to appeal and of the procedures for making such an appeal.

c. The designated office shall determine whether, under the declassification provisions of this Regulation, the requested information may be declassified, and, if so, make such information available to the requester, unless withholding is otherwise warranted under applicable law. If the information may not be released in whole or in part, the requestor shall be given a brief statement as to the reasons for denial, notice of the right to appeal the determination within 60 days (45 working days) to a designated appellate authority (including name, title, and address of such authority), and the procedures for such an appeal.

d. When a request is received for information classified by another DoD Component or an agency outside the Department of Defense, the designated office shall:

(1) Forward the request to such DoD Component or outside agency for review together with a copy of the document containing the information requested, when practicable and when appropriate, with its recommendation to withhold any of the information;

(2) Notify the requestor of the referral unless the DoD Component or outside agency to which the request is referred objects to such notice on grounds that its association with the information requires protection; and

(3) Request, when appropriate, that the DoD Component or outside agency notify the referring office of its determination.

e. If the request requires the rendering of services for which fees may be charged under Title 5 of the Independent Offices Appropriation Act (reference (r)) in accordance with DoD Instruction 7230.7 (reference (s)), the DoD Component may calculate the anticipated

amount of fees to be charged and ascertain the requestor's willingness to pay the allowable charges as a precondition to taking further action upon the request.

*f. A requestor may appeal to the head of a DoD Component or designee whenever that DoD Component has not acted on an initial request within 60 days or the requestor has been notified that requested information may not be released in whole or in part. Within 30 days after receipt, an appellate authority shall determine whether continued classification of the requested information is required in whole or in part, notify the requester of its determination, and make available to the requestor any information determined to be releasable. If continued classification is required under this Regulation, the requestor shall be notified of the reasons therefor. If so requested, an appellate authority shall communicate its determination to any referring DoD Component or outside agency. **Appeals will be forwarded to the Deputy Chief of Staff for Intelligence, HQDA (DAMI-CI) WASH DC 20310-1050.***

g. The ASD(PA) shall act as appellate authority for all appeals regarding OSD, OJCS, and Unified Command records.

3-305. Foreign government information

Requests for mandatory review for the declassification of foreign government information shall be processed and acted upon under the provisions of this section subject to subsection 11-202.

3-306. Prohibition

No DoD Component in possession of a document shall in response to a request under the Freedom of Information Act or this section refuse to confirm the existence or non-existence of the document, unless the fact of its existence or nonexistence would itself be classifiable under this Regulation.

3-307. Restricted Data and Formerly Restricted Data

Any proposed action on a request, including requests from international libraries, for DoD classified documents that are marked "Restricted Data" or "Formerly Restricted Data" must be coordinated with the Department of Energy. **See subsection 3-202c**

Section 4

Declassification of Transferred Documents or Material

3-400. Material officially transferred

In the case of classified information or material transferred under statute, E.O., or directive from one department or agency or DoD Component to another in conjunction with a transfer of functions, as distinguished from transfers merely for purposes of storage, the receiving department, agency, or DoD Component shall be deemed to be the original classifying authority over such material for purposes of downgrading and declassification.

3-401. Material not officially transferred

When a DoD Component has in its possession classified information or material originated in an agency outside the Department of Defense that has ceased to exist and such information or material has not been transferred to another department or agency within the meaning of subsection 3-400, or when it is impossible to identify the originating agency, the DoD Component shall be deemed to be the originating agency for the purpose of declassifying or downgrading such information or material. If it appears probable that another department, agency, or DoD Component may have a substantial interest in the classification of such information, the DoD Component deemed to be the originating agency shall notify such other department, agency, or DoD Component of the nature of the information or material and any intention to downgrade or declassify it. Until 60 days after notification, the DoD Component shall not declassify or downgrade such information or material without consulting the other department, agency, or DoD Component. During this period, the other department, agency, or DoD Component may express objections to downgrading or declassifying such information or material.

3-402. Transfer for storage or retirement

Whenever practicable, classified documents shall be reviewed for downgrading or declassification before they are forwarded to a Records Center for storage or to the NARA for permanent preservation. Any downgrading or declassification determination shall be indicated on each document by markings as required by Chapter IV.

Section 5 Downgrading

3-500. Automatic downgrading

Classified information marked for automatic downgrading in accordance with this or prior regulations or E.Os. is downgraded accordingly without notification to holders.

3-501. Downgrading upon reconsideration

Classified information not marked for automatic downgrading may be assigned a lower classification designation by the originator or by an official authorized to declassify the same information (see subsection 1-603). Prompt notice of such downgrading shall be provided to known holders of the information. **DA Form 1575 normally will be used for this purpose. Excluded are the following:**

a. Documents that have a wide distribution. Commands and agencies subordinate to HQDA will notify users by DA circular or similar media.

b. Recurring publications with essentially a fixed distribution. These publications may carry regrading or declassification notification of previous issues.

Section 6 Miscellaneous

3-600. Notification of changes in declassification

When classified material has been properly marked with specific dates or events for declassification, it is not necessary to issue notices of declassification to any holders. However, when declassification action is taken earlier than originally scheduled, or the duration of classification is extended, the authority making such changes shall ensure prompt notification of all holders to whom the information was originally transmitted. The notification shall specify the marking action to be taken, the authority therefor, and the effective date. Upon receipt of notification, recipients shall effect the proper changes and shall notify holders to whom they have transmitted the classified information. See subsections 4-400 and 4-404 for markings and the use of posted notices.

3-601. Foreign relations series

In order to permit the State Department editors of *Foreign Relations of the United States* to meet their mandated goal of publishing twenty years after the event, DoD Components shall assist the editors in the Department of State by easing access to appropriate classified materials in their custody and by expediting declassification review of items from their files selected for possible publication.

3-602. Reproduction for declassification review

The provisions of subsection 7-305 shall not restrict the reproduction of documents for the purpose of facilitating declassification review under the provisions of this Chapter or the Freedom of Information Act, as amended (DoD Directive 5400.7, reference (k)). After review for declassification, however, those reproduced documents that remain classified must be destroyed in accordance with Chapter IX.

Chapter IV Marking

Section 1 General Provisions

4-100. Designation

Subject to the exceptions in subsection 4-102, information determined to require classification protection under this Regulation shall be so designated. Designation by means other than physical marking may be used but shall be followed by physical marking as soon as possible.

4-101. Purpose of designation

Designation by physical marking, notation, or other means serves to warn the holder about the classification of the information involved; to indicate the degree of protection against unauthorized disclosure that is required for that particular level of classification; and to facilitate downgrading and declassification actions.

4-102. Exceptions

a. No article that has appeared, in whole or in part, in newspapers, magazines or elsewhere in the public domain, or any copy thereof, that is being reviewed and evaluated to compare its content with classified information that is being safeguarded in the Department of Defense by security classification, may be marked with any security classification, control or other kind of restrictive marking. The results of the review and evaluation, if classified, shall be separate from the article in question.

b. Classified documents and material shall be marked in accordance with subsection 4-103 unless the markings themselves would reveal a confidential source or relationship not otherwise evident in the document, material, or information.

c. The marking requirements of subparagraphs 4-103 a.4. and 4-103 b.4. do not apply to documents or other material that contain, in whole or in part, Restricted Data or Formerly Restricted Data information. Such documents or other material or portions thereof shall not be declassified without approval of the Department of Energy with respect to Restricted Data or Formerly Restricted Data information, and with respect to any other national security information contained therein, the approval of the originating agency.

4-103. Documents or other material in general

a. At the time of original classification the following shall be shown on the face of all originally classified documents (see subsection 4-402) or clearly associated with other forms of classified information in a manner appropriate to the medium involved:

*(1) The identity of the original classification authority by position title, unless he or she is the signer or approver of the document (**the identity of original Army classification authorities will be shown, by position title, regardless of whether the official is the signer or approver of the document**),*

(2) The agency and office of origin;

(3) The overall classification of the document (see subsection 1-500);

*(4) The date or event for automatic declassification or the notation "Originating Agency's Determination Required" or "OADR" (**except for documents marked under paragraphs 4-501 and 4-502**), and, if applicable,*

(5) Any downgrading action to be taken and the date or event thereof.

b. At the time of derivative classification, the following shall be shown on the face of all derivatively classified documents (see subsection 4-402) or clearly associated with other forms of classified information in a manner appropriate to the medium involved:

(1) The source of classification, that is, a source document or classification guide. If classification is derived from more than one source, the phrase "Multiple Sources" will be shown and the identification of each source will be maintained with the file or record copy of the document;

(2) The agency and office of origin of the derivatively classified document;

(3) The overall classification of the document (see subsection 1-500);

(4) The date or event for declassification or the notation "Originating Agency's Determination Required" or "OADR," carried forward from the classification source. If the classification is derived from multiple sources, either the most remote date or event for declassification marked on the sources or if required by any source, the notation "Originating Agency's Determination Required" or "OADR" shall be shown **(documents marked as Restricted Data" or Formerly Restricted Data" do not carry a date or event for declassification; also see subsection 4-401); and, if applicable,**

(5) Any downgrading action to be taken and the date or event thereof.

c. In addition to the foregoing, classified documents shall be marked as prescribed in section 2 of this chapter, Chapter XI, if the document contains foreign government information, and with any applicable special notation listed in section 5 of this chapter. Such notations shall be carried forward from source documents to derivatively classified documents when appropriate. (DoD 5200.1-PH (reference (yy)) provides illustrated guidance on the application of classification and associated markings to documents prepared by the Department of Defense.)

d. Material other than paper documents shall show the required information on the material itself or if that is not practical, in related or accompanying documentation (see subsection 4-300).

4-104. Identification of classification authority

a. Identification of a classification authority shall be shown on the "Classified by" line prescribed under subsection 4-402 and shall be sufficient, standing alone, to identify a particular official, source document or classification guide.

(1) If all information in a document or material is classified as an act of original classification, the classification authority who made the determination shall be identified on the "classified by" line, unless the classifier is also the signer or approver of the document (see subsection 4-402). **The original classification authority must be shown in the "classified by" line when all information in the document is based on an original classification decision. The identity of the original classification authority will be shown, by position title, regardless of whether the official is the signer or approver of the document.**

(2) If the classification of all information in a document or material is derived from a single source (for example, a source document or classification guide), the "Classified by" line shall identify the source document or classification guide, including its date when necessary to insure positive identification (see subsection 4-402). The date of the source document will be included in each instance.

(3) If the classification of information contained in a document or material is derived from more than one original classification authority, or an original classification authority and another source, or from more than one source document, classification guide, or combination thereof, the "Classified by" line shall be marked "Multiple Sources" and identification of all such authorities and sources shall be maintained with the file or record copy of the document (see subsection 4-402). **Whenever possible; the sources of classification will be shown on all copies of the document.**

(4) If an official with requisite classification authority has been designated by the head of an activity to approve security classifications assigned to all information leaving the activity, the title of that designated official shall be shown on the "classified by" line. The designated official shall maintain records adequate to support derivative classification actions (see subsection 4-402).

b. Guidance concerning the identification of the classification authority on electronically transmitted messages is contained in subsection 4-207.

c. Guidance concerning the identification of the classification authority on DoD documents that contain only foreign or NATO classified information is contained in paragraph 11-304 d.

4-105. Wholly unclassified material

Normally, unclassified material shall not be marked or stamped "Unclassified" unless it is essential to convey to a recipient of such material that it has been examined with a view to imposing a security classification and that it has been determined that it does not require classification. **This provision applies only to documents and material that are unclassified in their entirety. It in no way affects the page marking, component marking, or portion marking requirements for classified documents (paragraphs 4-200, 4-201, and 4-202).** However, the marking "Unclassified" may be applied to formerly classified material (see subsection 4-400).

Section 2

Specific Markings on Documents

4-200. Overall and page marking

Except as otherwise specified for working papers (see subsection 7-304), the overall classification of a document, whether or not permanently bound, or any copy or reproduction thereof, shall be conspicuously marked, stamped or affixed permanently at the top and bottom on the outside of the front cover (if any), on the title page (if any), on the first page, and on the outside of the back cover (if any). Each interior page, except those that are blank, shall be marked top and bottom according to its content, to include "Unclassified" when no classified information is contained on such a page. Alternatively, the overall classification of the document may be conspicuously marked or stamped at the top and bottom of each interior page when such marking is necessary to achieve production efficiency and the particular information to which classification is assigned is otherwise sufficiently identified consistent with the intent of subsection 4-202. In any case, the classification marking of a page shall not supplant the classification marking of portions (subsection 4-202) of the page marked with lower levels of classification.

a. **Classification markings will be in letters larger than those on the rest of the page (except as provided in paragraphs 4-207b and 4-305).**

b. **If it is not possible to mark classification in letters which are larger than the rest of the text (for example, on covers of documents or graphics), apply classification markings in any manner that is immediately noticeable.**

c. **To promote reproducibility, classification and associated markings will be applied in black or other dark ink. The use of red ink is discouraged.**

4-201. Marking components

The major components of some complex documents are likely to be used separately. In such instances, each major component shall be marked as a separate document in accordance with section 1 of this chapter. Examples include each annex, appendix, or similar component of a plan, program, or operations order; attachments and appendices to a memorandum or letter; and each major part of a report. If an entire major component is unclassified, the first page of the component may be marked at the top and bottom with the designation "UNCLASSIFIED" and a statement included, such as, "All portions of this (annex, appendix, etc.) are UNCLASSIFIED." When this method of marking is used, no further markings are required on the unclassified major component.

4-202. Portion marking

a. Each section, part, paragraph, or similar portion of a classified document shall be marked to show the level of classification of the information contained in or revealed by it, or that it is unclassified. Portions of documents shall be marked in a manner that eliminates doubt as to which of its portions contains or reveals classified information. Classification levels of portions of a document, except as provided in subsection 4-204, shall be shown by the appropriate classification symbol placed immediately following the portion's

letter or number, or in the absence of letters or numbers, immediately before the beginning of the portion. In marking sections, parts, paragraphs, or similar portions, the parenthetical symbols “(TS)” for Top Secret, “(S)” for Secret, “(U)” for Confidential, and “(IS)” for unclassified, shall be used. When appropriate, the symbols “RD” for Restricted Data and “FRD” for Formerly Restricted Data shall be added, for example, “(S-RD)” or “(C-FRD).” In addition, portions that contain Critical Nuclear Weapon Design Information (CNWDI) will be marked “(N)” following the classification, for example, “(S-RD)(N).”

b. Portion marking of DoD documents containing foreign government information shall be in accordance with subsection 11-304.

c. Illustrations, photographs, figures, graphs, drawings, charts and similar portions of classified documents will be clearly marked to show their classification or unclassified status. Such markings shall not be abbreviated and shall be prominent and placed within or contiguous to the portion. Captions of such portions shall be marked on the basis of their content alone by placing the symbol “(TS),” “(S),” “(C),” or “(U)” immediately preceding the caption.

d. If, in an exceptional situation, parenthetical portion marking is determined to be impracticable, the document shall contain a statement sufficient to identify the information that is classified and the level of such classification. Thus, for example, each portion of a classified document need not be marked separately if all portions are classified at the same level, provided a statement to that effect is included in the document. In the case of classified compilations, the explanations required by subsection 4-203 meet this requirement.

e. When elements of information in one portion require different classifications, but segregation into separate portions would destroy continuity or context, the highest classification required for any item shall be applied to that portion or paragraph.

f. Waivers of the foregoing portion marking requirements may be granted for good cause. Any request by a DoD Component senior official (see subsections 13-301 and 13-302) for a waiver of portion marking requirements shall be submitted to the DUSD(P) and include the following: (1) identification of the information or class of documents for which such waiver is sought; (2) detailed explanation of why the waiver should be granted; (3) the Component’s judgment of the anticipated dissemination of the information or class of documents for which the waiver is sought, and (4) the extent to which such information subject to the waiver may be a basis for derivative classification. Waivers shall be granted only upon a written determination by the DUSD(P) as the designee of the Secretary of Defense, that there will be minimal circulation of the specified documents or information, and minimal potential usage of these documents or information as a source for derivative classification determinations; or there is some other basis to conclude that the benefits of portion marking are clearly outweighed by the increased administrative burdens. The granting and revocation of portion marking waivers shall be reported to the Director of the ISOO by the DUSD(P). **Requests for waivers will be forwarded through command channels to HQDA (DAMI-CIS) WASH DC 20310-1051.**

g. **Documents, correspondence, text, and other human-readable output produced in a word processing mode on automated equipment will be marked with the overall and portion marking requirements of this regulation. Electronically transmitted record communications (as identified in paragraph 4-207) are also subject to these provisions. When portion marking of human-readable output is not possible, i.e., the classification of particular portions is dependent upon the input mix, the result of system calculation, etc., such output is exempt from the portion marking requirement, provided the overall and page marking requirements of paragraph 4-305 are met. A statement referring users to the source of classification and full address of the proponent will be included on the first page of the documents.**

4-203. Compilations

a. *Documents.* When classification is required to protect a compilation of unclassified information pursuant to subsection 2-211, the overall classification assigned to such documents shall be placed

conspicuously at the top and bottom of each page and on the outside of the front and back covers, if any, and an explanation of the basis for the assigned classification shall be included on the document or in its text.

b. *Portions of Documents.* If a classified document contains particular portions that are unclassified when standing alone, but classified information will be revealed when they are combined or associated, those portions shall be marked as unclassified, the page shall be marked with the highest classification of any information on or revealed by the page, and an explanation shall be added to the page, or to the document, to explain the classification of the combination or association to the holder. This method of marking also may be used if classified portions on a page, or within a document, will reveal information of a higher classification when they are combined or associated than when they are standing alone. **Segments of documents that are classified because of compilation must be portion marked. Two examples are shown below:**

(1) (S) **This is an example of a paragraph that is classified SECRET based on compilation. The lead-in contains an explanation of the added factor by which the subparagraphs, when compiled, are classified higher than each individual subparagraph. It also explains that all subparagraphs must be included in a new document before the extraction is Secret.**

(a) (C) **This portion standing alone is Confidential.**

(b) (C) **This portion is also Confidential.**

(c) (U) **This portion standing alone is Unclassified.**

(d) (U) **This portion is also Unclassified. However, when combined with subparagraphs (a), (b), and (c) above, the compilation is Secret.**

(2) (C) **This is an example of a paragraph that is classified Confidential by compilation. This lead-in contains an explanation of the added factor by which three or more of the Unclassified subparagraphs, when combined, are Confidential. This paragraph also explains that if only one or two of the subparagraphs are extracted, the extraction is Unclassified.**

(a) (U) **This portion is Unclassified.**

(b) (U) **This portion is Unclassified.**

(c) (U) **This portion, alone, is Unclassified when extracted. When combined with (a) and (b) above, this compilation is Confidential.**

(d) (U) **This portion is also Unclassified when extracted alone. When combined with two or more of the above portions, this compilation is Confidential.**

c. *Compilation Statements.* **As illustrated by the examples above, compilation statements:**

(1) **On a classified document that requires a higher classification, will identify the reason and the added factor that causes the higher classification.**

(2) **On an unclassified document that requires classification, will identify the reason and the added factor that causes the document to be classified.**

(3) **Will indicate the extent to which extractions from the compilation can be made at the unclassified level.**

4-204. Subjects and titles of documents

Subjects or titles of classified documents shall be marked with the appropriate symbol, “(TS),” “(S),” “(C),” or “(U)” placed immediately following and to the right of the item. When applicable, other appropriate symbols, for example, “(RD)” or “(FRD),” shall be added. (Subjects or titles of documents should be unclassified, if possible.)

4-205. File, folder, or group of documents

When a file, folder, or group of classified documents is removed from secure storage it shall be marked conspicuously with the highest classification of any classified document included therein or shall have an appropriate classified document cover sheet affixed. **These include: SF 703 (Orange Top Secret Cover Sheet), SF 704 (Red Secret Cover Sheet), and SF 705 (Blue Confidential Cover Sheet). Locally produced cover sheets may be used for classified material requiring Special Access Program protection. Cover**

sheets will include a conspicuous classification marking and the unclassified designate of the Special Access Program. Cover sheets, including those for Special Access Programs, will not contain classified data, nor be used to transfer or retire records.

4-206. Transmittal documents

A transmittal document, including endorsements and comments when such endorsements and comments are added to the basic communication, shall carry on its face a prominent notation of the highest classification of the information transmitted by it, and a legend showing the classification, if any, of the transmittal document, endorsement, or comment standing alone. For example, an unclassified document that transmits as an attachment a classified document shall bear a notation substantially as follows: "UNCLASSIFIED WHEN SEPARATED FROM CLASSIFIED ENCLOSURE." A transmittal document that remains classified when separated from enclosure will be marked: "REGRADED (insert classification) WHEN SEPARATED FROM ENCLOSURES." When it is practical to do so, classification markings on unclassified transmittal documents should be cancelled when the document are separated from classified enclosures. (See also paragraph 4-500 a.) Unclassified transmittal documents will not be portion marked.

4-207. Electronically transmitted messages

a. The copy of a classified message (for example, DD Form 173, Joint Messageform) approved for electronic transmission and maintained as the record copy shall be marked as required by subsection 4-103 for other documents (AR 105-31 provides specific instructions concerning where these markings will be placed on the DD Form 173 by users of Army telecommunications centers). Additionally, copies not electronically transmitted (such as, mail and courier copies) shall be marked as required by subsection 4-103.

b. The first item of information in the text of a classified electronically transmitted message shall be its overall classification. (A classified electronically transmitted message is the version of the text as taken from the DD Form 173 all placed in procedural format; it is not the DD Form 173 itself.) Paper copies of classified electronically transmitted messages shall be marked at the top and bottom with the assigned classification. Portions shall be marked as prescribed herein for paper copies of documents. When such messages are printed by an automated system, classification markings may be applied by that system, provided that page markings so applied are clearly distinguishable on the face of the document from the printed text.

c. The originator of a classified electronically transmitted message shall be considered the accountable classifier under subsection 2-100. The highest level official identified on the message as the sender or, in the absence of such identification, the head of the organization originating the message, is deemed to be the classifier of the message. Thus, a "classified by" line is not required on such messages. The originator is responsible for maintaining adequate records as required by paragraph 4-103 b. to show the source of an assigned derivative classification.

d. The last line of text of a classified electronically transmitted message shall show the date or event for downgrading, if appropriate, and the date or event for automatic declassification or "Originating Agency's Determination Required," by abbreviated markings from subsection 4-402. The foregoing is not required for messages that contain information identified as Restricted Data or Formerly Restricted Data.

e. Any document, the classification of which is based solely upon the classification of the content of a classified electronically transmitted message, shall cite the message on the "classified by" line of the newly created document. Also indicate the date-time group, subject, and originating office or headquarters.

4-208. Translations

Translations of U.S. classified information into a language other than English shall be marked to show the United States as the

country of origin, with the appropriate U.S. classification markings and the foreign language equivalent thereof (see appendix A).

4-209. Markings references and bibliographies

When references or bibliographies are included as part of a classified document, each document referenced or listed in the bibliography should clearly reflect the classification of the document listed. The following is an example of such a listing:

a. (U) AR 380-40, Policy for Safeguarding and Controlling COMSEC Information, Confidential.

b. (U) AR 604-5, DA Personnel Security Program Regulation, Unclassified.

Section 3

Markings on Special Categories of Material

4-300. General provisions

Security classification and applicable associated markings (see subsections 4-103 and 4-310) assigned by the classifier shall be conspicuously stamped, printed, written, painted, or affixed by means of tag, sticker, decal, or similar device, on classified material other than paper copies of documents, and on containers of such material, if possible. If marking the material or container is not practicable, written notification of the security classification and applicable associated markings shall be furnished to recipients. The following procedures for marking various kinds of material containing classified information are not all inclusive and may be varied to accommodate the physical characteristics of the material containing the classified information and to accommodate organizational and operational requirements.

4-301. Charts, maps, and drawings

Charts, maps, and drawings shall bear the appropriate classification marking for the legend, title, or scale blocks in a manner that differentiates between the overall classification of the document and the classification of the legend or title itself. The higher of these markings shall be inscribed at the top and bottom of each such document. When folding or rolling charts, maps, or drawings would cover the classification markings, additional markings shall be applied that are clearly visible when the document is folded or rolled. Applicable associated markings shall be included in or near the legend, title, or scale blocks.

4-302. Photographs, films, and recordings

Photographs, films (including negatives), recordings, and their containers shall be marked to assure that a recipient or viewer will know that classified information of a specified level of classification is involved. Where space is limited, the same abbreviations authorized for electronically transmitted messages may be used to indicate classification, downgrading, and declassification instructions.

a. *Photographs.* Negatives and positives shall be unmarked, whenever practicable, with the appropriate classification designation and applicable associated markings. Roll negatives or positives may be so marked at the beginning and end of each strip. Negatives and positives shall be kept in containers bearing conspicuous classification markings. All prints and reproductions shall be conspicuously marked with the appropriate classification designation and applicable associated markings on the face side of the print if possible. When such markings cannot be applied to the face side, they may be stamped on the reverse side or affixed by pressure tape label, stapled strip, or other comparable means. (NOTE: When self-processing film or paper is used to photograph or reproduce classified information, all parts of the last exposure shall be removed from the camera and destroyed as classified waste, or the camera shall be protected as classified.)

b. *Transparencies and slides.* Applicable classification markings shall be shown clearly in the image area of each transparency or slide, if possible. In the case of a 35mm or a similar size transparency or slide where the classification markings are not conspicuous

unless projected on a screen, for example, the classification markings also shall be marked on its border, holder, or frame. Duplicate classification markings in image areas and on borders, holders, or frames are required if there is any doubt that the image area markings are not conspicuous enough to be seen when the transparencies or slides are not being projected. Other applicable associated markings shall be shown in the image area, or on the border, holder, or frame, or in accompanying documentation. It is not necessary that each transparency or slide of a set of transparencies or slides bear applicable associated markings when the set is controlled as a single document. In such cases, the first transparency or slide shall bear the applicable associated markings.

c. Motion picture films and video tapes. Classified motion picture films and video tapes shall be marked at the beginning and end by titles bearing the appropriate classification markings. Applicable associated markings shall be included at the beginning of such films or tapes. All such markings shall be visible when projected. Reels and cassettes shall be marked with the appropriate classification and kept in containers bearing conspicuous classification and applicable associated markings.

d. Recordings. Sound, magnetic, or electronic recordings shall contain at the beginning and end a clear statement of the assigned classification that will provide adequate assurance that any listener or viewer will know that classified information of a specified level is involved. Recordings shall be kept in containers or on reels that bear conspicuous classification and applicable associated markings.

e. Microforms. Microforms are images, usually produced photographically on transparent or opaque materials, in sizes too small to be read by the unaided eye. Accordingly, the assigned security classification and abbreviated applicable associated markings shall be conspicuously marked on the microform medium or its container, so as to be readable by the unaided eye. These markings shall also be included on the image so that when the image is enlarged and displayed or printed, the markings will be conspicuous and readable. Such marking will be accomplished as appropriate for the particular microform involved. For example, roll film microforms (or roll microfilm employing 16, 35, 70, or 105 mm films) may generally be marked as provided for roll motion picture film in paragraph 4-302 c. and decks of "aperture cards" may be marked as provided in subsection 4-303 for decks of automatic data processing punched cards. Whenever possible, microfiche, microfilm strips, and microform chips shall be marked in accordance with this paragraph.

4-303. Decks of ADP punched cards

When a deck of classified ADP punched cards is handled and controlled as a single document, only the first and last card require classification markings. An additional card shall be added (or the job control card modified) to identify the contents of the deck and the highest classification therein. Such additional card shall include applicable associated markings. Cards removed for separate processing or use and not immediately returned to the deck shall be protected to prevent compromise of any classified information contained therein, and for this purpose shall be marked individually as prescribed in subsection 4-200.

4-304. Removable ADP and word processing storage media

a. External. Removable information storage media and devices, used with ADP systems and typewriters or word processing systems, shall bear external markings clearly indicating the classification of the information and applicable associated markings. Included are media and devices that store information recorded in analog or digital form and that are generally mounted or removed by the users or operators. Examples include magnetic tape reels, cartridges, and cassettes; removable discs, disc cartridges, disc packs and diskettes; paper tape reels, and magnetic cards. **The following labels will be used to indicate the classification of magnetic computer tape reels and other ADP media:**

- (1) **SF 706 (Orange Top Secret Label)**
- (2) **SF 707 (Red Secret Label)**

(3) **SF 708 (Blue Confidential Label)**

(4) **SF 710 Green Unclassified Label).**

b. Internal. ADP systems and word processing systems employing such media shall provide for internal classification marking to assure that classified information contained therein that is reproduced or generated, will bear applicable classification and associated markings. An exception may be made by the DoD Component head, or designee, for the purpose of exempting existing word processing systems when the internal classification and applicable associated markings cannot be implemented without extensive system modification, provided procedures are established to ensure that users and recipients of the media, or the information therein, are clearly advised of the applicable classification and associated markings. For ADP systems, exceptions may be authorized by the DoD Component Designated Approving Authority or Authorities, designated under DoD Directive 5200.28 (reference (h)). For purposes of these exemption provisions, "existing systems" means word processing and ADP systems already acquired, or, in the case of associated automated information systems, those for which the life cycle management process has already progressed beyond the "definition/design" phase as set forth in DoD Directive 7920.1 (reference (i)). Requirements for the security of nonremovable ADP storage media and clearance or declassification procedures for various ADP storage media are contained in DoD 5200.28-M (reference (i)).

4-305. Documents produced by ADP equipment

The first page, and the front and back covers, if any, of documents produced by ADP equipment shall be marked as prescribed in subsection 4-200. Interior pages also shall be marked as prescribed in subsection 4-200 except that the classification markings of interior pages of fanfolded printouts may be applied by the ADP equipment. **Overall pages, as well as portions, paragraphs, subparagraphs, etc., may be marked automatically with their classification (i.e., the automated information system (AIS) has a feature that produces the markings). Automated markings on output must not be relied upon to be accurate unless the security features and assurances of the AIS meet the requirements for a minimum security class B1 as specified in DoD 5200.28-STD (reference (h)).** When the application of associated markings prescribed by subsection 4-103 by the ADP equipment is not consistent with economical and efficient use of such equipment, such markings may be applied to a document produced by ADP equipment by superimposing upon the first page of such document a "Notice of Declassification Instructions and Other Associated Markings." Such notice shall include the date or event for declassification or the notation "Originating Agency's Determination Required" or "OADR" and all other such applicable markings. **If the B1 standard above is not met, but automated controls are used, all output will be protected at the highest classification level of the information handled by the AIS until manually reviewed by an authorized person. The output will then be marked with the highest level of actual contents before dissemination.** If individual pages of a document produced by ADP equipment are removed or reproduced for distribution to other users, each such page or group of pages shall be marked as prescribed in subsection 4-103 or by superimposing upon each such page or group of pages, a copy of any "Notice of Declassification Instructions and Other Associated Markings" applicable to such page or group of pages. **The same abbreviations authorized for electronically transmitted messages may be used on ADP printouts. The abbreviated instructions may be printed at the bottom of the first page or title page, or in a similar conspicuous place immediately below or adjacent to the classification markings. Subsequent pages will also reflect the overall classification marking of the first page.**

4-306. Material for training purposes

In using unclassified documents or material to simulate classified documents or material for training purposes, such documents or material shall be marked clearly to indicate the actual unclassified

status of the information, for example, "(insert classification designation) for training, otherwise unclassified" or "UNCLASSIFIED SAMPLE."

4-307. Miscellaneous material

Documents and material such as rejected copy, typewriter ribbons, carbons, and similar items developed in connection with the handling, processing, production, and use of classified information shall be handled in a manner that assures adequate protection of the classified information involved and destruction at the earliest practicable time (see section 2, Chapter V). Unless a requirement exists to retain this material or documents for a specific purpose, there is no need to mark, stamp, or otherwise indicate that the information is classified.

4-308. Special Access Program documents and material

Additional markings as prescribed in directives, regulations and instructions relating to an approved Special Access Program shall be applied to documents and material containing information subject to the special access program. Such additional markings shall not serve as the sole basis for continuing classification of the documents or material to which the markings have been applied. When appropriate, such markings shall be excised to ease timely declassification, downgrading, or removal of the information from special control procedures. (See chapter XII of this regulation, DoD Directive 5205.7, AR 380-381 and DA Pamphlet 380-381 (references (aaaa) and (bbbb)).)

4-309. Secure telecommunications and information handling equipment

Applicable classification or Controlled Cryptographic Item (CCI) markings shall be applied to secure telecommunications and information handling equipment or associated cryptographic components. Safeguarding and control procedures for classified and CCI equipment and for safeguarding COMSEC facilities are contained in references (v), (w), (x), (eee), (fff), (ggg), and (hhh).

4-310. Associated markings

Other applicable associated markings required for documents by subsection 4-103 shall be accomplished as prescribed in this section or in any other appropriate manner.

Section 4 Classification Authority, Duration, and Change in Classification Markings

4-400. Declassification and regrading marking procedures

When classified information is downgraded or declassified in accordance with the assigned downgrading or declassification markings, such markings shall be a sufficient notation of the authority for such action. Whenever classified information is downgraded or declassified earlier than originally scheduled, or upgraded, the material shall be marked promptly and conspicuously to indicate the change, the authority for the action, the date of the action and the identity of the person taking the action. In addition, except for upgrading (see subsection 4-403), prior classification markings shall be canceled, if practicable, but in any event those on the cover (if any) and first

page shall be canceled, and the new classification markings, if any, shall be substituted. **When Information on microform is regraded, the markings on the microform itself will not be updated. Rather, the markings on the microform container will be updated. Procedures will be established locally to ensure that markings are entered promptly on all enlarged copies.**

4-401. Applying derivative declassification dates

a. New material that derives its classification from information classified on or after August 1, 1982, shall be marked with the declassification date, event, or the notation "Originating Agency's Determination Required" or "OADR" assigned to the source information.

b. New material that derives its classification from information classified prior to August 1, 1982, shall be treated as follows:

(1) If the source material bears a declassification date or event, that date or event shall be carried forward to the new material

(2) If the source material bears no declassification date or event, or bears an indeterminate date or event such as "Upon Notification by Originator," "Cannot Be Determined," or "Impossible to Determine," or is marked for declassification review, the new material shall be marked with the notation "Originating Agency's Determination Required" or "OADR"; or

(3) If the source material is foreign government information bearing no date or event for declassification or is marked for declassification review, the new material shall be marked with the notation "Originating Agency's Determination Required" or "OADR."

c. New material that derives its classification from a classification guide issued prior to August 1, 1982, that has not been updated to conform with this Regulation shall be treated as follows:

(1) If the guide specifies a declassification date or event, that date or event shall be applied to the new material; or

(2) If the guide specifies a declassification review date, the notation "Originating Agency's Determination Required" or "OADR" shall be applied to the new material.

4-402. Commonly used markings

Each classified document is marked on its face with one or more of the following markings:

a. *Original Classification.* The following markings are used in original classification (paragraph 4-103 a.):

Classified by ___ (See Note 1)

Declassify on ___ (See Note 2)

Message Abbreviation:

DECL ___ (See Note 3)

b. *Derivative Classification.* The following markings are used in derivative classification (paragraph 4-103 b.):

Classified by ___ (See Note 4)

Declassify on ___ (See Note 5)

Message Abbreviation:

DECL ___ (See Note 3)

c. *Downgrading.* The following marking is used to specify a downgrading (paragraphs 4-103 a. and 4-103 b.):

Downgrade to ___ on ___ (See Note 6)

Message Abbreviation:

DNG/___/___ (See Note 7)

Note 1: Insert identification (position title) of the original classification authority. This line may be omitted if the original classification authority is also the signer or approver of the document. **The identity of the original classification authority will be entered on the "Classified by" line, regardless of whether the official is the signer or approver of the document.**

Note 2: Insert the specific date, an event certain to occur, or the notation "Originating Agency's Determination Required" or "OADR."

Note 3: Insert day, month, and year for declassification, for example, "6 Jun 90," an event certain to occur, or "OADR."

Note 4: Insert identity of the single security classification guide, source document, or other authority for the classification. If more than one such source is applicable, insert the phrase "Multiple Sources."

Note 5: Insert the specific date or event for declassification or the notation "Originating Agency Determination Required" or "OADR." When multiple sources are used, either the most remote date or event for declassification marked on the sources or, if present on any source, the notation "Originating Agency's Determination Required" or "OADR" is applied to the new document.

Note 6: Insert Secret or Confidential and specific date or event, for example, "Downgrade to CONFIDENTIAL on 6 July 1988."

Note 7: Insert "S" or "C" to indicate the downgraded classification and specific date or event, for example, "DNG/C/6 Jun 87."

d. There is no requirement for adding declassification instructions on documents with Restricted Data or Formally Restricted Data markings (see paragraph 4-102 c., and subsections 4-501 and 4-502). Except for electronically transmitted messages, only a completed “Classified by” line is added to documents so marked.

e. Electronically transmitted messages do not require a “Classified by” line (see paragraph 4-207 c.).

f. DoD 5200.1-PH (reference (yy)) provides additional marking guidance.

g. When portions of a document are to be declassified or downgraded earlier than the date shown on the front of the document, originators must indicate what information in interior portions is eligible for earlier declassification or downgrading.

4-403. Upgrading

When material is upgraded it shall be promptly and conspicuously marked as prescribed in section 4-400 except that in all such cases the old classification markings shall be canceled and new markings substituted.

4-404. Limited use of posted notice for large quantities of material

a. When the volume of material is such that prompt remarking of each classified item cannot be accomplished without unduly interfering with operations, the custodian may attach downgrading and declassification notices to the storage unit instead of the remarking required by subsection 4-400. Each notice shall specify the authority for the downgrading or declassification action, the date of the action; and the storage unit to which it applies.

b. When individual documents or materials are permanently withdrawn from storage units, they shall be remarked promptly as prescribed by subsection 4-400. However, when documents or materials subject to a downgrading or declassification notice are withdrawn from one storage unit solely for transfer to another, or a storage unit containing such documents or materials is transferred from one place to another, the transfer may be made without remarking if the notice is attached to or remains with each shipment.

Section 5 Additional Warning Notices

4-500. General provisions

a. In addition to the marking requirements prescribed in subsection 4-103, the warning notices prescribed in this section shall be displayed prominently on classified documents or materials, when applicable. In the case of documents, these warning notices shall be marked conspicuously on the outside of the front cover, or on the first page if there is no front cover. Transmittal documents, including those that are unclassified (subsection 4-206), also shall bear these additional warning notices, when applicable. In addition, abbreviated forms of the notices set forth in subsections 4-501, 4-502, and 4-503 shall be included in portion markings, as applicable. Further, the warning notice in subsection 4-503, in its short form, shall be included at least once on interior pages, as applicable.

b. When display of warning notices on other materials is not possible, their applicability to the information shall be included in the written notification of the assigned classification.

4-501. Restricted Data

Classified documents or material containing Restricted Data as defined in the Atomic Energy Act of 1954, as amended (reference (g) and AR 380-150 (reference (y))), shall be marked as follows:

RESTRICTED DATA

This material contains Restricted Data as defined in the Atomic Energy Act of 1954. Unauthorized disclosure subject to administrative and criminal sanctions.

4-502. Formerly Restricted Data

Classified documents or material containing Formerly Restricted Data, as defined in Section 142.d, Atomic Energy Act of 1954, as amended (reference (g)), but no Restricted Data, shall be marked as follows:

FORMERLY RESTRICTED DATA

Unauthorized disclosure subject to administrative and criminal sanctions. Handle as Restricted Data in foreign dissemination. Section 144.b, Atomic Energy Act, 1954.

4-503. Intelligence sources or methods information

a. Documents that contain information relating to intelligence sources or methods shall include the following marking unless otherwise prescribed by DoD Instruction 5230.22 (reference (u)): “WARNING NOTICE—Intelligence Sources or Methods Involved.”

b. Existing stamps or preprinted labels containing the caveat “Warning Notice Intelligence Sources and Methods Involved” may be used on documents created on or after the effective date of this Regulation until replacement is required. Any replacement or additional stamps or labels purchased after the effective date of this Regulation shall conform to the wording of paragraph a., above.

c. The following additional caveats prescribed by AR 381-1 (DoD Instruction 5230.22 (reference (u))) will be used on intelligence information, under the conditions specified for each in the regulation:

- (1) **NOFORN (Not Releasable to Foreign Nationals)**
- (2) **ORCON (Dissemination and Extraction of Information Controlled by Originator)**
- (3) **NOCONTRACT (Not Releasable to Contractors/Consultants)**
- (4) **PROPIN (Caution—Proprietary Information Involved)**
- (5) **REL (Authorized for Release to (insert name of foreign country(ies))).**

4-504. COMSEC material

Before release to contractors, COMSEC documents will indicate on the title page, or first page if no title page exists, the following notation: “COMSEC Material—Access by Contractor Personnel Restricted to U.S. Citizens Holding Final Government Clearance.” This notation shall be placed on COMSEC documents or material when originated and when release to contractors can be anticipated. Other COMSEC documents or material shall be marked in accordance with National COMSEC Instruction (NACSI) 4003 (reference (eee)). **See AR 380-40 and TB 380-41 (reference (v)).** Foreign dissemination of COMSEC information is governed by NCSC Policy Directive 6 (reference (w)).

4-505. Dissemination and reproduction notice

Classified information that the DoD originator has determined to be subject to special dissemination or reproduction limitations shall include, as applicable, a statement or statements on its cover sheet, first page, or in the text, substantially as follows: “Reproduction requires approval of originator or higher DoD authority” and/or “Further dissemination only as directed by (insert appropriate office or official) or higher DoD authority.”

4-506. Other notations

Other notations of restrictions on reproduction, dissemination or extraction of classified information may be used as authorized by DoD Directive C-5200.5, DoD Instruction 5230.22, DoD Directive 5210.2, DoD Directive 5100.55, DoD Directive 5200.30, Joint Army-Navy-Air Force Publication 119, DoD Directive 5230.24, and NACSI 4003 (references (x), (u), (y), (z), (q), (aa), (ww), and (eee) respectively).

Section 6 Remarking Old Material

4-600. General

a. Documents and material classified under E.O. 12065 (reference (cc)) and predecessor E.Os. that are marked for automatic downgrading or automatic declassification on a specific date or event shall be downgraded and declassified pursuant to such markings. Declassification instructions on such documents or material need not be restated to conform with subsection 4-202. (See also subsection 4-400). Information extracted from these documents or material for use in new documents or material shall be marked for declassification on the date specified in accordance with paragraph 4-103 b.

b. Documents and material classified under reference (cc) and predecessor E.Os. that are not marked for automatic downgrading or automatic declassification on a specific date or event shall not be downgraded or declassified without authorization of the originator. Declassification instructions on such documents or material need not be restated to conform with subsection 4-202. Information extracted from these documents or material for use in new documents or material shall be marked for declassification upon the determination of the originator, that is, the "Declassify on" line shall be completed with the notation "Originating Agency's Determination Required" or "OADR" in accordance with paragraph 4-103 b.

4-601. Earlier declassification and extension of classification

Nothing in this section shall be construed to preclude declassification under Chapter III or subsequent extension of classification under subsection 2-302.

Chapter V Safekeeping and Storage

Section 1 Storage and Storage Equipment

5-100. General policy

Classified information shall be stored only under conditions adequate to prevent unauthorized persons from gaining access. The requirements specified in this Regulation represent the minimum acceptable security standards. DoD policy concerning the use of force for the protection of property or information is specified in DoD Directive 5210.56 (reference (dd)). **Items having only monetary value (such as cash, precious metals, jewelry, narcotics, and so forth) will not be stored in vaults, security containers, or areas designated for storage of classified information or material.**

5-101. Standards for storage equipment

The GSA establishes and publishes minimum standards, specifications, and supply schedules for containers, vault doors, alarm systems, and associated security devices suitable for the storage and protection of classified information. Heads of DoD Components may establish additional controls to prevent unauthorized access. Security filing cabinets conforming to federal specifications bear a Test Certification Label on the locking drawer, attesting to the security capabilities of the container and lock. (On some older cabinets the label was affixed on the inside of the locked drawer compartment.) Cabinets manufactured after February 1962 indicate "General Services Administration Approved Security Container" on the outside of the top drawer. **The GSA-approved changeable combination padlock built to Federal Specification FF-P110 (Sargent and Greenleaf Model 8077A), is intended for use only as an indoor or sheltered area reusable seal. This padlock:**

a. **Is not intended for use outdoors, or to protect against**

forced entry. (See paragraph 5-102d for information on approved outdoor security padlocks.)

b. **Is the only padlock approved for use with locking bar type containers. (Due to this vulnerability to the use of force, locking bar-type containers are restricted to storage of information classified no higher than Confidential, unless situated in a vault or alarmed area)**

5-102. Storage of classified information

Classified information that is not under the personal control and observation of an authorized person, will be guarded or stored in a locked security container as prescribed below:

a. **Top Secret.** Top Secret information shall be stored in:

(1) A safe-type steel file container having a built-in, three-position, dial-type combination lock approved by the GSA or a Class A vault or vault type room that meets the standards established by the head of the DoD Component concerned (see **Army standards in appendix H**). When located in buildings, structural enclosures, or other areas **in the United States, supplemental controls are mandatory if:**

(a) **The area is not under U.S. Government control, (as defined in paragraph 1-321.1), or if the area does not meet the structural standards of appendix H.**

(b) **In such cases, the storage container vault, or vault-type room must be protected by an alarm system or guarded (i.e., supplemental controls are required) during nonoperating hours.**

(2) An alarmed area, provided such facilities are adjudged by the local responsible official to afford protection equal to or better than that prescribed in a.1., above. **Coordinate with the Chief, Intelligence Materiel Activity (IMA), (AMXIM-PS), Fort Meade, MD 20755-5313, for evaluation of protection "equal to or better."** When an alarmed area is used for the storage of Top Secret material, the physical barrier must be adequate to prevent (a) surreptitious removal of the material, and (b) observation that would result in the compromise of the material. The physical barrier must be such that forcible attack will give evidence of attempted entry into the area. The alarm system must provide immediate notice to a security force of attempted entry. **If a security force is not capable of responding in 5 minutes or less, the area must be continuously occupied by at least two persons whose principal duty is access control into and out of the alarmed area. Alarm system response time when under two-person control must not exceed 15 minutes. If these conditions cannot be met, then alarmed-area storage of Top Secret material will not be permitted.** Under field conditions, the field commander will prescribe the measures deemed adequate to meet the storage standards contained in a. 1. and 2., above. **Heads of HQDA agencies and MACOM commanders or their designees may approve use of alarmed areas. Approvals will be in writing.**

(3) **For Top Secret information stored outside the United States, one or more of the following supplemental security controls is required:**

(a) **The area that houses the security container or vault will be subject to the continuous protection of guard or duty personnel;**

(b) **Guard or duty personnel will inspect the security container or vault at least once every 2 hours; or**

(c) **The security container or vault will be controlled by an alarm system to which a force will respond in person within 15 minutes.**

b. **Secret and Confidential.** Secret and Confidential information shall be stored in the manner prescribed for Top Secret; or in a Class B vault, or a vault-type room, strong room, or secure storage room that meets the standards prescribed by the head of the DoD Component; or, until phased out, in a steel filing cabinet having a built-in, three-position, dial type combination lock; or, as a last resort, an existing steel filing cabinet equipped with a steel lock bar, provided it is secured by a GSA-approved changeable combination padlock (the padlock described in subsection 5-101 will be used). In this latter instance, the keeper or keepers and staples must be secured to the cabinet by welding, rivets, or peened bolts and DoD

Components must prescribe supplementary controls to prevent unauthorized access. **Secret material may be stored in such cabinets only when the container is situated in a vault or alarmed area (see subsection 5-101).** Heads of HQDA agencies and MACOM commanders may delegate authority to approve exceptions to the storage standards in appendix H. Exceptions will be made, in writing, only if the protection provided at least equivalent to that provided by equipment meeting the referenced standards. **Proposed exceptions should be coordinated with the Chief, IMA.**

c. Specialized security equipment:

(1) *Field safe and one-drawer container.* One-drawer field safes, and GSA-approved security containers are used primarily for storage of classified information in the field and in transportable assemblages. Such containers must be securely fastened or guarded to prevent their theft.

(2) *Map and plan file.* A GSA-approved map and plan file has been developed for storage of odd-sized items such as computer cards, maps, and charts.

d. Other storage requirements. Storage areas for bulky material containing classified information, other than Top Secret, shall have access openings secured by GSA-approved changeable combination padlocks (federal specification FF-P110 series) or key-operated padlocks with high security cylinders (exposed shackle, military specification P-43951 series, or shrouded shackle, military specification P-43607 series) **or the key-operated locking device covered by military specification L-29151(YD).**

(1) When combination padlocks are used, the provisions of subsections 5-101 and 5-104 apply.

(2) When key-operated high security padlocks **or locking devices (MIL-L-29151(YD))** are used, keys shall be controlled as classified information with classification equal to that of the information being protected and:

(a) A key and lock custodian shall be appointed to ensure proper custody and handling of keys and locks;

(b) A key and lock control register shall be maintained to identify keys for each lock and their current location and custody;

(c) Keys and locks shall be audited each month;

(d) Keys shall be inventoried with each change of custodian;

(e) Keys shall not be removed from the premises;

(f) Keys and spare locks shall be protected in a secure container;

(g) Locks shall be changed or rotated at least annually, and shall be replaced upon loss or compromise of their keys;

(h) Master keying is prohibited **unless required by another regulation or maintained under a two-person control system;**

(i) **Any one of the nine high-security padlock hasps designed to MILSPEC-H-43905 should be used (when available through channels, a new, Navy-designed hasp which encloses the padlock should be used in high-security applications; it enhances security by affording the lock greater protection from attack by force); and**

(j) **Chain, when required, should be used only with the exposed 1/2-inch-diameter shackle padlock, MILSPEC-P-43951. Use 3/8-inch trade-size, tool-resistant, case-hardened security chain or 3/8-inch trade-size, grade 80 alloy steel chain conforming to Federal specification RR-C-271 or NACM specification.**

(3) **Additional security safeguards to be applied under these storage requirements will be in compliance with paragraphs 5-102 a or b and guidance found in appendix H, part II.**

e. Considerations. Perfect or absolute security is always the goal, but a state of absolute security can never be attained. No object is so well protected that it cannot be stolen, damaged, destroyed, or observed by unfriendly eyes. Therefore, the first step in developing physical security measures for the facility, installation, post, etc., is to assess the threat to the information or material to be protected. Then, based upon the threat, institute appropriate physical security measures designed to make access so difficult that an intruder will hesitate to attempt penetration, or to provide for the intruder's apprehension should he or she be successful. Physical security must be built on a system of defense in depth or upon accumulated delay time. FM 19-30

(reference (sss)) provides additional information to assist the security manager in achieving that end.

5-103. Procurement and phase-in of new storage equipment

a. Preliminary survey. DoD activities shall not procure new storage equipment until:

(1) A current survey has been made of on-hand security storage equipment and classified records; and

(2) Based upon the survey, it has been determined that it is not feasible to use available equipment or to retire, return, declassify or destroy enough records on hand to make the needed security storage space available.

b. Purchase of new storage equipment. New security storage equipment shall be procured from those items listed on the GSA Federal Supply Schedule. Exceptions may be made by heads of DoD Components, with notification to the DUSD(P). **Under no condition will new locking bar containers be fabricated from either existent old steel containers or newly procured steel containers as a means of circumventing the intent of this paragraph. Requests for exceptions will be forwarded through command channels to HQDA (DAMI-CIS), WASH DC 20310-1051.**

c. Nothing in this chapter shall be construed to modify existing Federal Supply Class Management Assignments made under DoD Directive 5030.47 (reference (ee)).

5-104. Designations and combinations

a. Numbering and designating storage facilities. There shall be no external mark as to the level of classified information authorized to be stored therein. For identification purposes each vault or container shall bear externally an assigned number or symbol.

b. Combinations to containers.

(1) *Changing.* Combinations to security containers shall be changed only by individuals having that responsibility and an appropriate security clearance. **The Chief, IMA, (AMXIM-PS), Ft. Meade MD 20755-5313, will furnish information on the proper methods of changing combinations upon request. The request should include the type of equipment and any problems encountered.** Combinations shall be changed:

(a) When placed in use;

(b) Whenever an individual knowing the combination no longer requires access;

(c) When the combination has been subject to possible compromise;

(d) At least annually;

(e) When taken out of service. Built-in combination locks shall be reset to the standard combination 50-25-50; combination padlocks shall be reset to the standard combination 10-20-30; or

(f) **Every 6 months when NATO information is stored in the security container.**

(2) *Classifying combinations.* The combination of a vault or container used for the storage of classified information shall be assigned a security classification equal to the highest category of the classified information authorized to be stored therein.

(3) *Recording storage facility data.* A record shall be maintained for each vault, secure room, or container used for storing classified information, showing location of the container, the names, home addresses, and home telephone numbers of the individuals having knowledge of the combination. Standard Form 700, "Security Container Information" shall be used for this purpose. **(The Standard Form 700 replaces DA Form 727. Use of this Standard Form is required when existing supplies of similar purpose forms are exhausted or by September 30, 1986, whichever occurs earlier). A current record for all security containers, vault doors, and padlock combinations will be kept on Standard Form 700.**

(a) **Complete Part 1 and Part 2A, SF 700. (Include the name and signature of the person making the combination change in Item 9, Part 1.)**

(b) **Part 1, SF 700 will be posted on the inside of the lock drawer of the security container.**

(c) Parts 2 and 2A, SF 700 will be marked with the highest classification of material stored in the container.

(d) Part 2A, SF 700 will be detached and inserted in the envelope. (Part 2A, SF 700 used to record a Top Secret combination will be accounted for in the same manner as other Top Secret documents, except that a DA Form 969 (Top Secret Document Record) is not required (since the Top Secret information would not be disclosed to personnel handling the sealed envelope). Upon change of a Top Secret combination, the old Part 2A is automatically declassified, and may be deleted from the Top Secret register (or DA Form 3964).

(e) Only Part 1, SF 700 need be completed for security containers storing two-person control material. Parts 2 and 2A need be used only if there is a specific need for recording the combination.

(4) *Dissemination.* Access to the combination of a vault or container used for the storage of classified information shall be granted only to those individuals who are authorized access to the classified information stored therein.

c. *Electrically actuated locks.* Electrically actuated locks (for example, cypher and magnetic strip card locks) do not afford the required degree of protection of classified information and may not be used as a substitute for the locks prescribed in subsection 5-102.

5-105. Repair of damaged security containers or vault doors

Neutralization of lock-outs or repair of any damage that affects the integrity of a security container or vault door approved for storage of classified information shall be accomplished only by authorized persons who are cleared or continuously escorted while so engaged.

a. A GSA-approved security container or vault door is considered to have been restored to its original state of security integrity if:

(1) All damaged or altered parts (for example, locking drawer, and drawer head) are replaced; or

(2) When a container or vault door has been drilled immediately adjacent to or through the dial ring to neutralize a lock-out, the replacement lock is equal to the original equipment, and the drilled hole is repaired with a tapered, hardened tool-steel pin, or a steel dowel, drill bit, or bearing with a diameter slightly larger than the hole and of such length that when driven into the hole there shall remain at each end of the rod a shallow recess not less than 1/8 inch nor more than 3/16 inch deep to permit the acceptance of substantial welds, and the rod is welded both on the inside and outside surfaces. The outside of the drawer head or vault door shall then be puttied, sanded, and repainted in such a way that no visible evidence of the hole or its repair remains on the outer surface after replacement of the damaged parts (for example, new lock).

b. GSA-approved containers or vault doors that have been drilled in a location or repaired in a manner other than as described in paragraph a., above, will not be considered to have been restored to their original state of security integrity. The Test Certification Label on the inside of the locking drawer and the "General Services Administration Approved Security Container" label, if any, on the outside of the top drawer shall be removed from such containers.

c. If damage to a GSA-approved security container or vault door is repaired with welds, rivets, or bolts that cannot be removed and replaced without leaving evidence of entry, the cabinet or vault is limited thereafter to the storage of Secret and Confidential material.

d. If the damage is repaired using methods other than those permitted in paragraphs a. and c., above, use of the container or vault will be limited to unclassified material and a notice to this effect will be permanently marked on the front of the container or vault door. (See appendix I for information on preventive maintenance for security containers.)

5-106. Turn-in or transfer of security equipment

In addition to having combinations reset before turn-in (see paragraph 5-104b.1.(e) above), security equipment will be inspected before turn-in or transfer to ensure that classified material is not left in the container. The turn-in procedure will include

removal of each container drawer and inspection of the interior to ensure that all papers and other materials have been removed and the container is completely empty.

Section 2 Custodial Precautions

5-200. Responsibilities of custodians

a. Custodians of classified information (i.e., any individual possessing classified material) shall be responsible for providing protection and accountability for such information at all times and for locking classified information in appropriate security equipment whenever it is not in use or under direct supervision of authorized persons. Custodians shall follow procedures that ensure that unauthorized persons do not gain access to classified information.

b. Only the head of a DoD Component, or single designee at the headquarters and major command levels, may authorize removal of classified information from designated working areas in off-duty hours, for work at home or otherwise, provided that a GSA-approved security container is furnished and appropriate regulations otherwise provide for the maximum protection possible under the circumstances. (See also section 3, chapter VII.) **The Secretary of the Army, the Under Secretary of the Army, the Assistant Secretaries of the Army, Chief of Staff, Vice Chief of Staff, the Director of the Army Staff, heads of Army Staff agencies, and MACOM commanders have the authority to remove classified information under the above arrangements when an operational requirement exists.** Any such arrangements approved before the effective date of this Regulation shall be reevaluated and, if continued approval is warranted, compliance with this paragraph is necessary. **Security managers for the above Army officials will determine whether arrangements currently exist, develop and maintain attendant records, and reverify the need for the arrangement. All arrangements will be reverified annually and upon a change in the occupant of the position.**

c. The removal of classified information after hours by persons other than the above authorities, must be approved in advance, in writing by one of the above Army officials. A bona-fide operational requirement for short-term or overnight storage of classified information must exist for consideration of such requests. This authority may not be delegated, except to individuals acting in an official's absence. The following requirements apply:

(1) Requests will be handled individually; blanket requests will not be considered. Personal convenience is not justification for approval.

(2) Authorization will be granted only when an operational requirement exists and there are adequate safeguards for the material (a GSA-approved security container will be paced where after-hours work is to be performed).

(3) Top Secret SCI, and/or SAP materials will not be removed under any circumstances.

(4) Signature accountability is required for all information removed (a DA Form 3964 is not required, but recommended). Reconciliation of material is required upon its return.

(5) Procedures will be established to ensure the return of classified information in the event of emergencies, such as death, hospitalization, or extended absence from duty (more than 30 days).

(6) Classified information will not be stockpiled under this arrangement, but returned to the regular work site as soon as possible.

(7) Army approval authorities will reverify the need for existing arrangements annually.

(8) Security managers will establish and maintain records of individuals so authorized.

(9) Approvals granted prior to the effective date of this regulation are void. Existing arrangements will be reevaluated within 90 days in accordance with the provisions of this regulation.

d. The protection of classified information is the responsibility of each person who has knowledge of the material, regardless of how it was obtained. Security regulations do not guarantee protection and cannot be written to cover all situations. Basic security principles, common sense, and a logical interpretation of the regulations must be applied; Collecting, obtaining, recording, or removing for any personal use whatsoever of any matter classified in the interest of national security is prohibited.

5-201. Care during working hours

DoD personnel shall take precaution to prevent unauthorized access to classified information.

a. Classified documents removed from storage shall be kept under constant surveillance and face down or covered when not in use. Cover sheets shall be Standard Forms 703, 704, and 705 for, respectively, Top Secret, Secret, and Confidential documents. (Use of these Standard Forms is required when existing supplies of similar purpose forms are exhausted or by September 30, 1986, whichever occurs earlier.)

b. Preliminary drafts, carbon sheets, plates, stencils, stenographic notes, worksheets, typewriter ribbons, and other items containing classified information shall be either destroyed immediately after they have served their purpose; or shall be given the same classification and secure handling as the classified information they contain.

c. Destruction of typewriter ribbons from which classified information can be obtained shall be accomplished in the manner prescribed for classified working papers of the same classification. After the upper and lower sections have been cycled through and overprinted five times in all ribbon or typing positions, fabric ribbons may be treated as unclassified regardless of their classified use thereafter. Carbon and plastic typewriter ribbons and carbon paper that have been used in the production of classified information shall be destroyed in the manner prescribed for working papers of the same classification after initial usage. However, any ribbon in a typewriter that uses technology which enables the ribbon to be struck several times in the same area before it moves to the next position may be treated as unclassified.

5-202. End-of day security checks

Heads of activities that process or store classified information shall establish a system of security checks at the close of each working day to ensure that the area is secure; Standard Form 701, "Activity Security Checklist" shall be used to record such checks. An integral part of the security check system shall be the securing of all vaults, secure rooms, and containers used for the storage of classified material; Standard Form 702, "Security Container Check Sheet" shall be used to record such actions. In addition; Standard Forms 701 and 702 shall be annotated to reflect after-hours, weekend, and holiday activity. (Use of these Standard Forms is required when existing supplies of similar purpose forms are exhausted or by September 30, 1986, whichever occurs earlier.) Within Army:

a. **SF 702 will be displayed conspicuously on each piece of equipment used to store classified material. (SF 702 need not be used for facilities secured by high security locks, provided the key and lock control register provides an audit capability in the event of unsecured facilities,) SF 702 is used to record the date and time of each instance when security container is opened and closed. The following procedures apply:**

(1) **Properly cleared personnel will record the date and time whenever they unlock or lock the security equipment during the day (including after hours, weekends, and holidays), followed by their initials.**

(2) **If a security container is locked and the room in which it is located is to be left unattended, whenever possible a person other than the locker will check the container to make sure it is properly secured. The checker will record the time the container was checked and initial the form. The locker will see that the check is made.**

(3) **Containers not opened during a work-day will be checked and the action recorded as in 5-202 a. 2, above.**

(4) **Notations will also be made on SF 702 if containers are opened after hours, on weekends, and on holidays, as provided above.**

(5) **It is recommended the SF 702 be retained at least 24 hours following the last entry.**

b. **Reversible "OPEN-CLOSED" or "OPEN-LOCKED" signs will be used on each security container or vault in which classified information is stored. Signs are available through normal supply channels.**

c. **A person discovering a security container or security storage area open and unattended will:**

(1) **Keep the container or area under guard or surveillance.**

(2) **Notify one of the persons listed on Part 1, SF 700 affixed to the inside of the security container lock drawer. If one of these individuals cannot be contacted, the duty officer, security manager, or other appropriate official will be notified.**

d. **Individuals contacted when a container or area is found open or unattended will:**

(1) **Report personally to the location; check the contents of the container or area for visible indications or evidence of tampering, theft, or compromise. If any evidence of tampering, theft, or compromise is noted:**

(a) **Installation or activity security personnel (if not at the scene) will be immediately notified so that a preliminary investigation can be initiated.**

(b) **The custodian will cease examination of the container and its contents (to prevent destruction of physical evidence) unless otherwise instructed by security personnel.**

(c) **A lock technician will be called to determine the nature of the tampering, and whether the security container is operating properly.**

(2) **Change the combination and lock the container. If the combination cannot be changed immediately, the security container will be locked and placed under guard until the combination can be changed; or the classified contents will be transferred to another container or secure area.**

(3) **If not previously accomplished, report the incident to the commander or security manager immediately for action relative to compromise or possible compromise.**

e. **After-duty-hours security checks of desks may be conducted, provided:**

(1) **Each military member and civilian employee is notified of local policy and procedures pertaining to after-hours inspections, locking of desks, and maintenance of duplicate keys or combinations. Notification must be in writing, and in advance of any after-hours inspection program.**

(2) **After-duty-hours inspections are conducted only by military or civilian security personnel, and for the sole purpose of detecting improperly secured classified information.**

5-203. Emergency planning

a. Plans shall be developed for the protection, removal, or destruction of classified material in case of fire, natural disaster, civil disturbance, terrorist activities, or enemy action. Such plans shall establish detailed procedures and responsibilities for the protection of classified material to ensure that the material does not come into the possession of unauthorized persons. These plans shall include the treatment of classified information located in foreign countries.

b. These emergency planning procedures do not apply to material related to COMSEC. Planning for the emergency protection including emergency destruction under nonnotice conditions of classified COMSEC material shall be developed in accordance with the requirements of NSA KAG I-D (reference (bb)).

c. Emergency plans shall provide for the protection of classified material in a manner that will minimize the risk of injury or loss of life to personnel. In the case of fire or natural disaster, the immediate placement of authorized personnel around the affected area, preinstructed and trained to prevent the removal of classified material by unauthorized personnel, is an acceptable means of protecting

classified material and reducing casualty risk. Such plans shall provide for emergency destruction to preclude capture of classified material when determined to be required. This determination shall be based on an overall commonsense evaluation of the following factors:

(1) Level and sensitivity of classified material held by the activity;

(2) Proximity of land-based commands to hostile or potentially hostile forces or to communist-controlled countries;

(3) Flight schedules or ship deployments in the proximity of hostile or potentially hostile forces or near communist-controlled countries;

(4) Size and armament of land-based commands and ships;

(5) Sensitivity of operational assignment; and

(6) Potential for aggressive action of hostile forces.

d. When preparing emergency destruction plans, consideration shall be given to the following:

(1) Reduction of the amount of classified material held by a command as the initial step toward planning for emergency destruction;

(2) Storage of less frequently used classified material at more secure commands in the same geographical area (if available);

(3) Transfer of as much retained classified material to microforms as possible, thereby reducing the bulk that needs to be evacuated or destroyed

(4) Emphasis on the priorities for destruction, designation of personnel responsible for destruction, and the designation of places and methods of destruction. Additionally, if any destruction site or any particular piece of destruction equipment is to be used by more than one activity or entity, the order or priority for use of the site or equipment must be clearly delineated;

(5) Identification of the individual who is authorized to make the final determination when emergency destruction is to begin and the means by which this determination is to be communicated to all subordinate elements maintaining classified information (**emergency destruction plans will clearly identify the position titles of these individuals, or deteriorating even which serve as the basis to initiate emergency destruction of classified material;**

(6) Authorization for the senior individual present in an assigned space containing classified material to deviate from established plans when circumstances warrant; and

(7) Emphasis on the importance of beginning destruction sufficiently early to preclude loss of material. The effect of premature destruction is considered inconsequential when measured against the possibility of compromise.

e. The emergency plan shall require that classified material holdings be assigned a priority for emergency evacuation or destruction. Priorities should be based upon the potential effect on national security should such holdings fall into hostile hands, in accordance with the following general guidelines:

(1) *Priority One.* Exceptionally grave damage (Top Secret material);

(2) *Priority Two.* Serious damage (Secret material); and

(3) *Priority Three.* Damage (Confidential material).

f. If, as determined by appropriate threat analysis, Priority One material cannot otherwise be afforded a reasonable degree of protection from hostile elements in a no-notice emergency situation, provisions shall be made for installation of Anticompromise Emergency Destruct (ACED) equipment to ensure timely initiation and positive destruction of such material² in accordance with the following standard: "With due regard for personnel and structural safety, the ACED system shall reach a stage in destruction sequences at which

positive destruction is irreversible within 60 minutes at shore installations, 30 minutes in ships, and 3 minutes in aircraft following activation of the ACED system."³ **Until the ACED system is available, the M-610 incendiary file destroyers and thermite grenades, employed primarily to destroy crypto materials, will be used for an PRIORITY ONE emergency destruction within appropriate Army activities Adequate of the M-610, or other comparable devices, will be maintained for PRIORITY ONE bulk emergency destruction purposes in lieu of the ACED system.**

g. An ACED requirement is presumed to exist and provisions shall be made for an ACED system to protect Priority One material in the following environments:

(1) Shore-based activities located in or within 50 miles of potentially hostile countries, or located within or adjacent to countries with unstable governments.

(2) Reconnaissance aircraft, both manned and unmanned, that operate within JCS-designated reconnaissance reporting areas (see Memorandum by the Secretary, Joint Chiefs of Staff (SM) 701-76, Volume II, "Peacetime Reconnaissance and Certain Sensitive Operations" (reference (ff))⁴;

(3) Naval surface noncombatant vessels operating in hostile areas when not accompanied by a combatant vessel;

(4) Naval subsurface vessels operating in hostile areas; and

(5) U.S. Navy Special Project ships (Military Sealift Command operated) operating in hostile areas.

h. Except in the most extraordinary circumstances, ACED is not applicable to commands and activities located within the United States. Should there be reason to believe that an ACED requirement exists in environments other than in those listed in paragraph g., above, a threat and vulnerability study should be prepared and submitted to the head of the DoD Component concerned or his designee for approval. The threat and vulnerability study should include, at a minimum, the following data, classified if appropriate:

(1) Volume and type of Priority One material held by the activity, that is, paper products, microfilms, magnetic tape, and circuit boards;

(2) A statement certifying that the amount of Priority One material held by the activity has been reduced to the lowest possible level;

(3) An estimate of the time, beyond the time frames cited above, required to initiate irreversible destruction of Priority One material held by the activity, and the methods by which destruction of that material would be attempted in the absence of an ACED system,

(4) Size and composition of the activity;

(5) Location of the activity and the degree of control it, or other United States authority, exercises over security; and

(6) Proximity to potentially hostile forces and potential for aggressive action by such forces.

i. When a requirement is believed to exist for ACED equipment not in the GSA or DoD inventories, the potential requirement shall be submitted to the DUSD(P) for validation in accordance with subsection V. B. of DoD Directive 3224.3 (reference (gg))^{5,5}

j. In determining the method of destruction of other than Priority One material, any method specified for routine destruction or any other means that will ensure positive destruction of the material may be used. Ideally, any destruction method should provide for early attainment of a point at which the destruction process is irreversible. Additionally, classified material may be jettisoned at sea to prevent its easy capture. It should be recognized that such disposal may not prevent recovery of the material. Where none of the methods previously mentioned can be employed, the use of other means, such as dousing the classified material with a flammable liquid and

² Technological limitations, particularly as to personnel and structural safety, place constraints on the amount of material that can be accommodated in buildings, ships and aircraft by current ACD systems; therefore, only Priority One material reasonable can be so protected at this time. Nevertheless, after processing Priority One material in an emergency situation involving possible loss to hostile forces, it is imperative that Priority Two material and then Priority Three material be destroyed insofar as is possible by whatever means available.

³ The time frames indicated above are those for the initiation of irreversible

⁴ SM 701-76 is available on a strict need-to-know basis from the Chief, Documents Division, Joint Secretariat, OJCS.

⁵ Information on ACED systems may be obtained from the Office of the Chief of Naval Operations (OP-09N) Navy Department, Washington, DC 20350.

igniting it, or putting to use the facility garbage grinders, sewage treatment plants, and boilers should be considered.

k. Under emergency destruction conditions, destruction equipment may be operated at maximum capacity and without regard to pollution, preventive maintenance, and other constraints that might otherwise be observed.

l. Commands and activities that are required to maintain an ACED system pursuant to paragraph g., above, shall conduct drills periodically to ensure that responsible personnel are familiar with the emergency plan. Such drills should be used to evaluate the anticipated effectiveness of the plan and the prescribed equipment and should be the basis for improvements in planning and equipment use. Actual destruction should not be initiated during drills.

5-204. Telecommunications conversations

Classified information shall not be discussed in telephone conversations except as authorized over approved secure communications circuits, that is; cryptographically protected circuits or protected circuits systems installed in accordance with National COMSEC Instruction 4009 (referenced)).

5-205. Security of meetings and conferences

Security requirements and procedures governing disclosure of classified information at conferences, symposia, conventions, and similar meetings, and those governing the sponsorship and attendance of U.S. and foreign personnel at such meetings, are set forth below, as stated in DoD Directive 5200.12, DoD Instruction 5230.20, DoD 5220.22-R, and DoD 5220.22-M (references (ii), (aaa), (e), and (f), respectively).

a. Policy

(1) **Classified meetings will be conducted in support of an official Army or U.S. Government purpose. Security safeguards and procedures will be established for each meeting to control access and prevent the compromise of classified information presented. Army components desiring to conduct a classified meeting are responsible for obtaining approval (when required) to sponsor the meeting, and for ensuring all security measures are met.**

(2) **DCSINT approval is required before an Army activity may sponsor or conduct classified meetings to be attended by foreign nationals.**

(3) **A meeting at which classified information will be disclosed will be held only at a secure location at a U.S. Army or other U.S. Government installation, or at a cleared U.S. contractor facility.**

b. General

(1) **DCSINT approval is not required for in-house meetings. In these instances, the Army activity responsible for conducting the meeting will ensure the security requirement of this section are met. The following are examples of in-house meetings:**

(a) **Meetings attended only by Federal Government employees or U.S. military personnel.**

(b) **Meetings related to a specific contract or project. These include preproposal or preaward meetings, as well as postaward briefings conducted by the Army contracting activity.**

(c) **Meetings conducted by cleared contractors and attended only by cleared contractors directly involved in the performance of an Army (or other U S Government) contract or project.**

(d) **Meetings between military members of U.S overseas commands and their foreign counterparts.**

(2) **Advance DCSINT approval (HQDA (DAMI-CIT) WASH DC 20310-1052) is required before an Army activity conferences, symposia, and conventions, usually attended by formal invitation, such as:**

(a) **Advance planning briefings for industry.**

(b) **Conferences attended by personnel from government, industries, commercial organizations, and educational institutions.**

(c) **Association cosponsored meetings (i.e, ADPA, AUSA, Association of Old Crows, etc) which will involve access to classified information (See paragraph f below.)**

c. Meetings disclosing classified information

(1) **Army classified conferences may only be held by an activity which accepts responsibility for meeting the security requirements of this section. An individual will be appointed in each case to ensure that security measures are followed.**

(2) **Authorized foreign industry representatives will be included in all acquisition-related classified meetings which involve U. S. industry.**

(3) **HQDA (DAMI-CIT) WASH DC 20310-1051 approval is required for sponsorship of meetings involving foreign attendance Submit requests at least 120 days prior to the planned conference date.**

(4) **Public announcement of meetings involving classified information is prohibited until the requirement in paragraphs c. 1 through 3, above, are met.**

d. Procedures

(1) **Army activities having significant interest in the subject matter of the meeting may act as sponsors after determining that:**

(a) **It is in the best interest of the Army to do so.**

(b) **Conventional dissemination channels will not accomplish the purpose of the meeting.**

(c) **Adequate security measures and access control procedures have been developed and will be implemented.**

(d) **The meeting site ensures proper physical control, storage, protection, and dissemination o classified information.**

(2) **Army activities accepting sponsorship of a classified meeting will appoint a security representative who will institute procedures which comply with appropriate security measures, and ensure that:**

(a) **The meeting site is appropriate for the level of classification involved.**

(b) **Adequate storage facilities are available, when required (A GSA-approved security container will be used for overnight storage of presentations or notes taken during classified session when note-taking is allowed.)**

(c) **Access to classified sessions of the conference are limited to persons whose clearance and need to know have been positively established, as follows:**

1. **Military and Federal Government civilian personnel will provide a written visit request or security clearance certification to the conference security representative The visit request will contain the full name of the conference attendee, social security number, date and place of birth, citizenship, security clearance level and date granted, and security manager's certification.**

2. **U. S. defense contractor personnel will provide the above information, as well as the following contract number, project, or program which pertains to the subject matter of the classified meeting, level of classified access authorized under said contract, project, or program, purpose justification for attendance at the classified conference, and U. S. Government contracting officer's certification of the individual's need to attend the conference(need-to know).**

3. **The sponsoring Army activity will request approval from HQDA (DAMI-CIT) WASH DC 20310-1051 for the disclosure of classified information to the countries of foreign nationals expected to attend (see AR 380-10 (reference (uuu)). Foreign nationals from approved countries may then submit visit requests through their embassies to HQDA (DAMI-CIT). Upon approval, HQDA will notify the Army activity of foreign nationals allowed to attend the conference**

(d) **The names of all cleared/certified personnel meeting the need-to-know requirements for attendance at the conference are included on the approved access roster.**

(e) **Each attendee shows proper identification (driver's license, ID cards etc.) before entering classified sessions during the conference.**

(f) **Each classified paper, speech, vugraph, etc. has been reviewed and its release authorized in advance of the conference. Ensure that written approval has been obtained before releasing**

any classified information at the meeting. Authorization to release classified information:

1. By DoD personnel, to wholly cleared U. S. audiences must be obtained from the originator.

2. To an audience that induces foreign nationals, must be obtained from HQDA (DAMI-CIT) WASH DC 20310-1051 (see AR 380-10(reference (uuu))).

3. By contractor personnel, must be approved in writing by the Army contracting activity having jurisdiction over the information involved. The contracting officer will ensure that a security review is conducted of the material to be presented, and that written approval/denial is provided the contractor prior to the conference date. (See paragraph 9.e, DoD 5220.22-M, Industrial Security Manual)(reference (f).)

(g) All announcements and invitations are reviewed for accuracy and to ensure that they are unclasped, prior to their dissemination.

(h) Notices of, or invitations to attend the classified meeting are issued only to cleared or authorized foreign personnel Representatives of and nationals from the following countries will not be invited: Afghanistan, Albania, Angola, Bulgaria, Cambodia (Kampuchea), People's Republic of China (including Tibet), Cuba, Czechoslovakia, Ethiopia, German Democratic Republic (East Germany, including the Soviet Sector of Berlin), Hungary, Iran, Iraq, Laos, Libyan Arab Republic, Mongolian People's Republic (Outer Mongolia), Nicaragua, North Korea, Poland, Rumania, Southern Yemen, Syria, Union of Soviet Socialist Republics (including Estonia, Latvia, Lithuania, and all other constituent Republics, Kurile Island, and South Sakhalin (Karafuto)), Vietnam, and Yugoslavia.

(i) Policies and procedures governing attendance by foreign representatives, and disclosures of information to foreign individuals, contained in AR 380-10 (reference (uuu)) are followed:

(j) The meeting is monitored to ensure that discussions are limited to authorized disclosures; individuals making oral presentations give attendees sufficient classification guidance to enable them to identify what information is classified or unclassified.

(k) Notes, minutes, summaries, proceedings, recordings, reports, and other documents containing classified information originated at the meeting are correctly marked, safeguarded, and distributed.

(l) Additional security safeguards are provided as required. For example, security representatives should ensure that:

1. Conference spaces are cleared for the discussion of classified information.

2. The integrity of the cleared area is maintained during the classified session.

(m) The loss or compromise of any classified information at the meeting is promptly reported by message to HQDA (DAMI-CIS) WASH DC 20310-1051 indicating full circumstances involved in the incident, and initiatives taken HQDA will notify ODUSD(P) of the incident.

(3) Army contractors may occasionally wish to conduct meetings and invite members of non-DoD organizations to attend. To do so, contractors must obtain written approval from the Army contracting activity primarily interested in the topic of discussion. The names of proposed attendees who are not U. S. citizens or immigrant aliens must be included. Approval is not necessary when contractors conduct a classified meeting and all of the following conditions are met:

(a) The meeting is conducted by the contractors at their own cleared facilities.

(b) The meeting is attended only by cleared contractors employed by the firm and/or U. S. Government personnel.

(c) The meeting pertains to a specific contract, program, project, etc. on which the contractor is performing.

e. Attendance by foreign nationals

(1) Army activities will notify HQDA (DAMI-CIT) WASH DC 20310-1052 in writing of any classified meeting involving, or

likely to involve, participation by foreign representatives. Notification is required upon an activity's request for security sponsorship, usually 120 days prior to the planned conference date.

(2) As DoD has entered into numerous reciprocal procurement agreements and offset purchase arrangements with U. S. allies, foreign participation in meetings, conferences, and symposia related to acquisition of materiel is presumed Army activities may not exclude authorized foreign attendees from such meetings in which U.S. industry will participate.

(3) Notification to HQDA must include (but is not limited to) the following:

(a) Subject of the meeting, overall classification, topical outline, and the classification of each topic.

(b) Date and location of meeting.

(c) Identity of sponsoring activity; name, grade, and telephone number of activity point of contact.

(d) Foreign countries to which the sponsoring activity desires to issue invitations, or from which requests to participate may reasonably be expected; or, a fully justified proposal to exclude foreign participants who would otherwise be eligible.

(e) Classified meetings may not be announced to the public nor invitations issued until written sponsorship approval is received from HQDA (DAMI-CIT).

f. Association cosponsored meetings

(1) Each year, DoD supports a large number of meetings and conferences sponsored by nongovernment associations (i.e., AUSA, ADPA, Association of Old Crows, etc.), aimed at a useful and necessary dialogue between DoD and industry. An increasing number of such conferences involve classified information.

(2) To ensure the maximum control of classified material while allowing for essential exchange of information, DUSD(P) has established a formal reporting procedure which applies to all association-sponsored, and cosponsored conferences, symposia, demonstrations, and chapter meetings wherein classified information is to be presented.

(3) Army activities planning to conduct a classified conference sponsored or cosponsored by a nongovernment association will provide the following information to HQDA (DAMI-CIT) WASH DC 20310-1052, 120 days prior to the planned conference date (include this information in the activity request for sponsorship):

(a) A topical outline, including a summary of each subject, its level, and source of classified information

(b) The name of the association/organization holding the meeting.

(c) The location of the meeting, including a physical security confirmation (i.e., the conference site is a cleared contractor or U.S. Government facility).

(d) The sponsoring Army activity; including the name, address, and phone number of the Army activity point of contact.

(e) The reason for the symposium.

g. Waiver requests

(1) Location of classified meetings. DoD policy requires that all classified meetings be held at U. S. Government installations or cleared contractor facilities. Authority to waive this requirement is limited exclusively to the DUSD(P). Requests for waiver to allow classified meetings to be held in an unclassified public facility (such as a hotel) will be considered individually. Blanket waivers will not be granted. The Army activity responsible for conduct of the classified meeting may submit a request to HQDA (DAMI-CIS) WASH DC 20310-1051, 120 days prior to the planned conference date. In addition to basic information, the waiver request must include.

(a) Full, detailed justification for the waiver.

(b) The reason appropriately cleared sites were not suitable and/or available

(c) A description of cost for the site, and the benefit to the Government in conducting the conference at the site.

(d) A detailed security plan describing procedures to be followed to ensure access control for classified sessions, and other

physical security measures which will preclude access by the public. A floor plan for the conference area should be included.

(2) **Exclusion of foreign nationals. Army activities may not arbitrarily designate an acquisition related meeting or session as "US Only." Authority to exclude foreign nationals from acquisition-related meetings at which U. S. contractors are invited is limited to the DUSD(P) Each request for exclusion will be considered individually. Submit such requests to HQDA (DAMI-CIT) WASH DC 20310-1052, at least 120 days prior to the planned conference date with full justification for the exclusion.**

5-206. Safeguarding of U.S. classified Information located in foreign countries

Except for classified information that has been authorized for release to a foreign government or international organization pursuant to DoD Directive 5320.11 (reference (oo)), and is under the security control of such government or organization, the retention of U. S. classified material in foreign countries may be authorized only when that material is necessary to satisfy specific U. S. Government requirements. This includes classified material temporarily transferred into a foreign country via U. S. Government personnel authorized to escort or handcarry such material pursuant to Chapter VIII, Section 3, as applicable. Whether permanently or temporarily retained, the classified materials shall be stored under U. S. Government control as follows (**Requests for exception to the provisions of any of the following subparagraphs will be forwarded HQDA (DAMI-CIS) WASH DC 20310-1051 with full justification**):

a. At a U. S. military installation, or a location where the United States enjoys extraterritorial status, such as an embassy or consulate.

b. At a U. S. Government activity located in a building used exclusively by U. S. Government tenants, provided the building under 24 hour control by U.S. Government personnel.

c. At a U. S. Government activity located in a building not used exclusively U. S. Government tenants nor under host government control, provided the classified material is stored in security containers approved by the GSA and is placed under 24-hour control by U. S. Government personnel.

d. At a U. S. Government activity located in a building not used exclusively by U. S. Government tenants but which is under host government control, provided the classified material is stored in GSA-approved security containers which are further secured in a locked room or area to which only U.S. personnel have access.

e. When host government and U. S. personnel are collocated, U.S. classified material that has not been authorized for release to the host government pursuant to DoD Directive 5230.11 (reference (oo)), shall, to the extent possible, be segregated from releasable classified material to facilitate physical control and prevent inadvertent compromise. However, U. S. classified material that is releasable to the host country need not be subject to the 24-hour U.S. control requirement provided the host government exercises its own control measures over the pertinent areas or containers during non-duty hours.

f. Foreign nationals shall be escorted while in areas where non-releasable U. S. classified material is handled or stored. However, when required by operational necessity, foreign nationals may be permitted, during duty hours, unescorted entry to such areas provided the nonreleasable information is properly stored or is under the direct personal supervision and control of cleared U. S. personnel who can prevent unauthorized access.

Section 3

Activity Entry and Exit Inspection Program

5-300. Policy

a. Commanders and heads of **Army Major Commands and Headquarters** activities shall establish and maintain an inspection program to deter and detect unauthorized introduction or removal of classified material from DoD owned or leased installations and

facilities. This program does not replace existing programs for facility and installation security and law enforcement inspection requirements.

b. The inspection program shall be implemented in a manner which does not interfere unduly with the performance of assigned missions.

c. The inspection program shall be implemented in a manner which does not significantly disrupt the ingress and egress of persons who are employees of, or visitors to, defense installations and facilities.

d. Inspections carried out under this program shall be limited to the extent feasible to areas where classified work is being performed, and cover only persons employed within, or visiting, such areas.

e. Inspections carried out under this program shall be performed at a sufficient frequency to provide a credible deterrent to those who would be inclined to remove classified materials without authority from the installation or facility in question.

f. The method and frequency of such inspections at a given installation or facility is at the discretion of the commander or head of the installation or facility, or other designated official. Such inspections shall conform to the procedures set forth below.

g. **MACOM commanders and heads of Army Staff elements will develop written procedures for executing the inspection requirement in coordination with legal, law enforcement, and security personnel. The procedures will be applicable to the MACOM or Army Staff agency, as well as subordinate elements. All individuals, regardless of rank, are subject to the provisions of this policy.**

(1) **Prior to commencing local inspections, activities will ensure that guard, law enforcement, and all other personnel involved in the inspections are fully trained in their responsibilities under the program. At a minimum, the training will address.**

(a) *Who is to be searched.* **All individuals entering or exiting an Army installation, building, or once during the inspection period, regardless of rank or grade, are subject to search by designated inspection personnel.**

(b) *The purpose of the search.* **Inspection will be conducted for the sole purpose of detecting and deterring the unauthorized introduction or removal of classified information. Inspections will not be used to target, single out, harass, or otherwise treat any individual differently than other persons entering and exiting the activity.**

(c) *What to look for.* **Designated security personnel will examine envelopes, packages, diskettes, diskette containers and other ADP media, tapes, film, microfiche, etc., likely to contain classified information. Sealed envelopes and packages are also subject to inspection. If an individual refuses to open a sealed envelope, or will not allow the inspector to do so, he or she will be asked for written courier orders, card, pass, or other documented proof of authorization to handcarry classified information. If the person does not have such authorization, he or she will be referred to the activity's predesignated office or other control center for further action.**

(d) *What is to be searched.* **While inspections are being conducted, authorized personnel will search all briefcases, shoulder or handbags, luggage, athletic bags, packages, and other similar containers carried into and out of the facility by visitors and employees. Personnel conducting the searches are expected to use discretion in inspecting any item that could reasonably be expected to contain classified information.**

(e) *What will not be searched.* **Inspectors will not search items that are obviously personal, such as wallets, change purses, and clothing or cosmetic cases. They will not search the individual's person.**

(f) *How to inspect.* **Personnel designated to conduct inspections will be polite and courteous at all times. During the designated period, inspectors will inform each person to be searched of the requirements to inspect items brought into and out of the facility. Inspectors:**

1. Will not open or handle a woman's handbag. The woman will be asked to open her handbags and to move or remove all items necessary to allow the inspector a reasonable view of all contents.

2. Will personally open, or have the individual open, an other items to be inspected. Items will be moved and all envelopes and parcels opened as necessary to allow the inspector a reasonable view of all contents.

(g) *Method of inspection.* Either of two methods may be used random or continuous (See paragraph 5-301c below). Inspectors will be consistent in conducting searches in the method chosen by the head of the activity.

(h) *Procedures to be followed in the event classified information is found.* If classified information is found, the individual being searched will be asked to produce written courier orders, DD Form 2501 (Courier Authorization card), pass, or other documented proof of authorization to hand-carry classified material. If the individual appears not to have such authorization, he or she will be referred to the activity's predesignated office or order control center for further action.

(i) *When and how often inspections will be conducted.* Subordinate commanders will ensure that local inspections are conducted for the minimum number of hours established by the MACOM commander or Army Staff head. The date or period for such inspections is at the discretion of the local commander.

(2) The commander's inspection program will be extensively publicized and disseminated to ensure that all personnel are notified of the policy. If possible, the inspection policy should also be posted at entry and exit points. Personnel must be notified of inspection program at least 2 months prior to the date inspections begin.

h. Army activities located on other than Army-controlled, U.S. Government installations will abide by the host's entry/exit inspection program. Host-tenant agreements should provide for acceptance of DD Form 2501 or other written authorization as proof of an Army military or civilian member's approval to handcarry classified information locally.

5-301. Inspection frequency

a. Inspections may be a periodic, that is, at irregular interval.

b. Inspections may be accomplished at one or more-designated entry/exit points; they need not be carried out at all entry/exit points at the same time.

c. Inspections may be done on a random basis using any standard which may be appropriate, for example, every third person; every tenth person; every hundredth person, at the entry/exit point(s) designated. **If the local commander prefers, continuous inspections, that is, checks of all individuals entering or exiting the activity during the designated inspection period, may be conducted in lieu of random inspections. Either method (random or continuous) may be chosen for a particular inspection period. Once chosen, however, that method must be used for the entire inspection period.**

d. Inspections at a particular entry/exit point(s) may be limited as appropriate to various periods of time, for example, one week, one day, or one hour.

e. Inspections shall be conducted at all entry/exit points after normal duty hours, including weekends and holidays, on a continuous basis, if practicable.

f. **Army activities will maintain a log or other appropriate local record of inspections conducted under this section.**

5-302. Inspection procedures and Identification

a. Inspections shall be limited to that which is necessary to determine whether classified material is contained in briefcases, shoulder or handbags, luggage, athletic bags, packages, or other similar containers being removed from or taken into the premises. Inspections shall not be done of wallets, change purses, clothing, cosmetics cases, or other objects of an unusually personal nature.

b. DoD Components shall provide employees who have a legitimate need to remove classified material from the installation or activity with written or printed authorizations to pass through designated entry/exit points (See paragraph 8-300 f.) This may include:

(1) The authorization statements prescribed in Chapter VIII, section 3. **Courier cards will not be used to provide authorization to handcarry classified information on commercial passenger aircraft, within the United States or abroad.**

(2) If authorized in Component instructions, wallet-size cards which describe in general terms the purpose(s) for authorizing the employee to remove classified material from the facility (for example, use at meetings or transmission to authorized recipients). **The DD Form 2501 (Courier Authorization card) will be used by personnel required to handcarry classified information locally within designated geographical limits (see paragraph 8-300). The cards will be issued and controlled by local security managers.**

c. Inspectors are to ensure that personnel are not removing classified material without authorization where inspectors determine that individuals do not appear to have appropriate authorization to remove classified material they shall request such individual **go to the activity security office**, or another predesignated control office, to obtain; appropriate authorization before exiting the premises. If due to the circumstances, this is not feasible, the inspector **should then contact personnel in the predesignated control office who will attempt to verify by telephone the authority of the individual in question to remove the classified material with the employing office.** When such verification cannot be obtained, and if removal cannot be prevented, the inspector shall **not attempt to detain the individual physically, but will record the person's name, activity, and the time in an inspection log if possible. This record will be provided the activity security office or designated control office. These personnel will advise the individual's employing office and/or appropriate security office as soon as feasible that classified material was removed by the named individual at a particular time and without apparent authorization.**

d. If the employing office determines that classified material was removed by one of its employees without authority, it shall request an investigation of the circumstances of the removal by appropriate investigative authorities. Where such investigation confirms a violation of security procedures, other than espionage or deliberate compromise, for which subsection 6-109 applies, appropriate administrative, disciplinary, or legal action shall be taken.

5-303. Local records

Army MACOMs and Staff agencies will maintain records of:

a. **The date(s) and number of entry/exit inspections conducted by the activity and subordinate elements during the previous quarter.**

b. **The number of instances during the quarter in which persons handled classified information without apparent authorization.**

c. **Problems encountered in the conduct of the entry/exit security inspection program.**

Chapter VI Compromise of Classified Information

6-100. Policy

Compromise of classified information presents a threat to the national security. Once a compromise is known to have occurred, the seriousness of damage to U.S. interests must be determined and appropriate measures taken to negate or minimize the adverse effect of such compromise. When possible, action also should be taken to regain custody of the documents or material that were compromised. In all cases, however, appropriate action must be taken to identify the source and reason for the compromise and remedial action taken to ensure further compromises do not occur. The provisions of DoD

Instruction 5240.4 and DoD Directive 5210.50 (references (jj) and(kk)) apply to compromises covered by this Chapter.

6-101. Cryptographic and sensitive compartmented information

a. The procedures for handling compromises of cryptographic information are set forth in NACSI 4006, (reference (fff)), AR 380-40 and TB 380-41 series (reference (v)), and implementing instructions.

b. The procedures for handling compromises of SCI information are set forth in DoD TS-5105.21-M-2 (reference (bbb)) and DoD C-5105.21-M-1 (reference (ccc)).

6-102. Responsibility of discoverer

a. Any person who has knowledge of the loss or possible compromise of classified information shall immediately report such fact to the security manager of the person's activity (see subsection 13-304) or to the commanding officer or head of the activity in the security manager's absence.

b. Any person who discovers classified information out of proper control shall take custody of such information and safeguard it in an appropriate manner, and shall notify immediately an appropriate security authority. **The local activity security manager will be promptly notified of each such incident. That official will advise the commander of the action to be taken.**

c. **DA Form 2134 (Security Violation(s) Report) may be used to report a violation of transmission requirements (for example, failure to doublewrap material) to the sender of a classified document, or to report other discrepancies in marking or handling. Use of this report does not eliminate the requirement for an inquiry when needed to determine the probability of compromise.**

6-103. Preliminary inquiry

The immediate commander, supervisor, security manager, or other authority shall initiate a preliminary inquiry to determine the circumstances surrounding the loss or possible compromise of classified information. **A properly cleared and disinterested commissioned officer, warrant officer, noncommissioned officer (E-7 or above), or DA civilian (GS-7 or above) may conduct the preliminary inquiry. Individuals appointed to conduct preliminary inquiries are authorized to take sworn statements in accordance with AR 15-6 (reference (vvv)), when necessary. When a specific individual could be involved in the circumstance surrounding the violation, the person conducting the inquiry will possess a rank or grade at least equal to that individual's.** The preliminary inquiry shall establish one of the following:

a. That a loss or compromise of classified information did not occur;

b. That a loss or compromise of classified information did occur but the compromise reasonably could not be expected to cause damage to the national security. If, in such instances, the official finds no indication of significant security weakness, the report of preliminary inquiry will be sufficient to resolve the incident and, when appropriate, support the administrative sanctions under subsection 14-101; or

c. That the loss or compromise of classified information did occur and that the compromise reasonably could be expected to cause damage to the national security or that the probability of damage to the national security cannot be discounted. Upon this determination, the responsible official shall:

(1) Report the circumstances of the compromise to an appropriate authority as specified in DoD Component instructions;

(a) **A report that fully identifies the information compromised will be submitted through appropriate channels to HQDA (DAMI-CIS) WASH DC 20310-1051 when the preliminary inquiry indicates that Top Secret or Secret information was compromised, and a probability of damage to the national security exists.**

(b) **Reports concerning the compromise of Confidential information will be submitted to the commander.**

(2) If the responsible official is the originator, take the action prescribed in subsection 6-106; and

(3) If the responsible official is not the originator, notify the originator of the known details of the compromise, including identification of the classified information. If the originator is unknown, notification will be sent to the office specified in DoD Component instructions

(4) **When the findings of the preliminary inquiry report are determined to be sufficient for final disposition, the inquiry thrill be closed.**

d. **At minimum, the preliminary inquiry will include the following:**

(1) **Where and when the violation occurred.**

(2) **Who reported the violation and to whom.**

(3) **A summary of the incident, identity of the document or material, and its classification.**

(4) **An estimate of the cause of the violation, including contributing factors and identity of the persons or persons responsible, if known.**

(5) **One of the following findings:**

(a) **Compromise did not occur.**

(b) **Compromise did occur.**

(c) **Probability of compromise is remote.**

(d) **Probability of compromise is not remote.**

(6) **If compromise did occur, or if the probability is not remote, a statement is required concerning the following:**

(a) **An estimate of the damage to the national security.**

(b) **A comment that the provisions of paragraph 2-210(reevaluation of classification) have been complied with.**

(7) **A summary of corrective and disciplinary action taken or anticipated, if applicable.**

(8) **A recommendation on the need for further investigation.**

This is required only when it is concluded that further investigation would reveal with reasonable assurance the cause or causes, responsibility, and compromise aspects of the violation (See paragraph 6-104h.)

6-104. Investigation

If it is determined that farther investigation is warranted, such investigation will include the following:

a. Identification of the source, date, and circumstances of the compromise

b. Complete description and classification of each item of classified information compromised;

c. A thorough search for the classified information;

d. Identification of any person or procedure responsible for the compromise. Any person so identified shall be apprised of the nature and circumstances of the compromise and be provided an opportunity to reply to the violation charged. If such person does not choose to make a statement, this fact shall be included in the report of investigation;

e. An analysis and statement of the known or probable damage to the national security that has resulted or may result (see subsection 2-210), and the cause of the loss or compromise; or a statement that compromise did not occur or that there is minimal risk of damage to the national security;

f. An assessment of the possible advantage to foreign powers resulting from the compromise; and

g. A compilation of the data in paragraphs a. through f., above, in a report to the authority ordering the investigation to include an assessment of appropriate corrective, administrative, disciplinary, or legal actions (Also see subsection 14-104).

h. **Further investigation is authorized only in the event of one of the following:**

(1) **After the preliminary inquiry finds that an actual compromise did occur or that damage to the national security is probable, provided further investigation would clarify the causes, responsibility, or compromise aspects of the violation.**

(2) When a MACOM commander or Headquarters agency head personally decides it might be useful.

i. Under the circumstances in subsection h, above, the responsible official will begin proceedings under AR 15-6 (reference (vvv)) and this regulation, or request a higher official in the chain of command to do so.

6-105. Responsibility of authority ordering investigation

a. The report of investigation shall be reviewed to ensure compliance with this Regulation and instructions issued by DoD Components.

b. The recommendations contained in the report of investigation shall be reviewed to determine sufficiency of remedial, administrative, disciplinary, or legal action proposed and, if adequate, the report of investigation shall be forwarded with recommendations through supervisory channels. See subsections 14-101 and 14-102.

c. Whenever an action is contemplated against any person believed responsible for the compromise of classified information, damage assessments shall be coordinated with the legal counsel of the DoD Component where the individual responsible is assigned or employed. Whenever a violation of criminal law appears to have occurred and a criminal prosecution is contemplated, the DoD Component responsible for the damage assessment shall apprise the General Counsel, Department of Defense. HQDA (DAMI-CIS) WASH DC 20310-1051 will ensure that a legal review is conducted of appropriate cases prior to apprising the General Counsel. See subsection 14-104.

d. Reports of investigation will be reviewed for compliance with AR 15-6 (reference (vvv)) and this regulation. If no compromise has occurred, the official ordering the inquiry or investigation may dispose of the incident. Whenever possible, the commander ordering disposition of the case will consider implementing the recommendations of the investigating officer. All persons notified of the possible compromise must also be notified of final actions in the case.

e. Reports of investigation that cannot be disposed of (d above) will be settled to the extent authorized to the convening authority. MACOM commanders and Headquarters agency heads may dispose of incidents involving classified information up to and including the level of original classification authority (OCA) delegated to them.

f. Final reviewing authorities will review the report of investigation for adequacy of subordinate command action. If further action is necessary, the report of investigation, together with pertinent instructions, will be sent to the subordinate command. One copy of each completed report of investigation of the probable or actual compromise of Top Secret or Secret information will be sent through channels to HQDA (DAMI-CIS) WASH DC 20310-1051 DA Form 1574 (Report of Proceedings by Investigating Officer/Board of Officers) or similar report of investigation and action of the convening and final reviewing authority is sufficient. Exhibits or enclosures need not be forwarded.

6-106. Responsibility of originator

The originator or an official higher in the originator's supervisory chain shall, upon receipt of notification of loss or probable compromise of classified information, take action as prescribed in subsection 2-210.

6-107. System of control of damage assessments

Each DoD Component shall establish a system of controls and internal procedures to ensure that damage assessments are conducted when required and that records are maintained in a manner that facilitates their retrieval and use within the Component. DA security managers will maintain a central record of damage assessments developed on programs or project for which the activity is the proponent. Damage assessments will be developed in response to a request from another agency or when a local inquiry or investigation of a security incident reveals a probable

or actual compromise of classified information. At a minimum, records will reflect:

- a. The requestor of the damage assessment (activity).
- b. Reason for the assessment (actual or probable compromise).
- c. Date the damage assessment was requested.
- d. Date the assessment was developed, and by whom.
- e. Program, project, or information involved.
- f. Classification of information involved; damage to national security that resulted.
- g. Action taken or recommended to mitigate damage to the program, project, or information and to the national security.
- h. Notification to holders of the information.

6-108. Compromises involving more than one agency

a. Whenever a compromise involves the classified information or interests of more than one DoD Component or other agency, each such activity undertaking a damage assessment shall advise the others of the circumstances and findings that affect their information and interests. Whenever a damage assessment incorporating the product of two or more DoD Components or other agencies is needed, the affected activities shall agree upon the assignment of responsibility for the assessment. In general, primary responsibility for developing age assessments when another agency is involved rests with the agency possessing a majority of the information subjected to compromise. In such cases, the agency having primary interest will coordinate the conduct of assessments with other agencies, and compile the final damage assessment report HQDA (DAMI-CIS) WASH DC 20310-1051 will be advised via command channels of any cases meeting the criteria of this paragraph prior to an Army activity's acceptance of primary responsibility. DAMI-CIS will conduct the necessary coordination with OSD.

b. Whenever a compromise of U. S. classified information is the result of actions taken by foreign nationals, by foreign government officials or by U. S. nationals employed by international organizations, the activity performing the damage assessment shall ensure, through appropriate intergovernmental liaison channels, that information pertinent to the assessment is obtained. Whenever more than one activity is responsible for the assessment, those activities shall coordinate the request prior to transmittal through appropriate channels. Army activities will refer cases under this paragraph to HQDA (DAMI-CIS) DAMI-CIS will work through intergovernmental liaison channels and Army staff elements to obtain information pertinent to the damage assessment.

6-109. Espionage and deliberate compromise

Cases of espionage and deliberate unauthorized disclosure of classified information to the public shall be reported in accordance with DoD Instruction 5240.4 and DoD Directive 5210-50 (references (jj) and (kk)) and implementing issuances. Regardless of the classification involved, cases of suspected or actual espionage and other deliberate compromise of classified information will be reported under AR 381-12 (reference (jj)).

6-110. Unauthorized absentees

When an individual who has had access to classified information is on unauthorized absence, an inquiry as appropriate under the circumstances, to include consideration of the length of absence and the degree of sensitivity of the classified information involved, shall be conducted to detect if there are any indications of activities, behavior, or associations that may be inimical to the interest of national security. When such indications are detected, a report shall be made to the DoD Component counterintelligence organization.

6-111. Suicide and attempted Suicide

When a person who has had access to classified information attempts or commits suicide, an inquiry will be initiated to determine the possible security implications. If such implications are discovered or suspected, action will be taken to report the

matter under AR 604-5. The inquiry must determine why suicide was attempted or committed before security implications may be addressed.

6-112. Unauthorized disclosure of classified information to the public

a. This subsection applies to unauthorized appearances of classified information in the public media and to unauthorized disclosures of classified information to a person likely to release that information to the public, whether or not the information is actually disclosed to the public. This subsection also applies to suspected incidents of this nature.

b. Army personnel will promptly report incidents or suspected incidents described in subsection a, above, to their commander or activity security manager.

c. Army officials notified of such incidents will immediately report them through command channels to HQDA (DAMI-CIS) WASH DC 20310-1051. This report does not preclude action that must be taken under paragraphs 6-103, 6-104, and 6-105 above. To speed reporting, electronically transmitted messages should be used whenever possible.

(1) All reports will include:

(a) Identification of the classified information involved.

(b) Nature and circumstances of the incident, to include complete and exact identification of the publication or broadcast in which the information appeared.

(2) If the reporting activity is the proponent, the report will also include as much of the following as possible:

(a) Accuracy of the information.

(b) Level and source of classification.

(c) Preliminary estimate of the nature and degree of damage to the national security caused by the disclosure.

(d) Available information about the source of the information (document, briefing, etc.) and the extent to which the information was disseminated.

(e) Available information about individuals who may have been responsible for the disclosure.

d. The Director of Counterintelligence and Security Countermeasures (DAMI-CI) will:

(1) Evaluate reports of incidents in consultation with the Assistant Secretary of Defense (Public Affairs) and officials having primary security classification jurisdiction over the information concerned; determine whether investigation of the incident would be in the interest of national security.

(2) Refer the incident to the appropriate investigation agency, when necessary.

(3) Report incidents to the DUSD(P) in accordance with DoD Directive 5210.50 (reference (kk)); coordinate requests for investigative assistance from non-Army agencies with the DUSD(P).

(4) Advise MACOM commanders and Headquarters agency heads of information developed during investigations that indicates the need for corrective action, including disciplinary or administrative action.

(5) Advise MACOM commanders and Headquarters agency heads of the compromise or possible compromise of information under their security in connection with incidents described in subsection a, above.

e. The Commanding General, U.S. Army Intelligence and Security Command (INSCOM), will:

(1) Investigate incidents described in subsection a, above, that fall within his or her investigative jurisdiction on referral from the Director of Counterintelligence and Security Countermeasures (DAMI-CI).

(2) Provide assistance to non-Army investigative agencies when requested to do so by the Director of Counterintelligence and Countermeasures (DAMI-CI).

f. MACOM commanders and Headquarters agency:

(1) Provide information and assistance to the Director of Counterintelligence and Security Countermeasures (DAMI-CI),

the Commanding General, INSCOM, and non-Army investigative agencies to aid in the evaluation and investigation of incidents described in subsection a, above.

(2) Ensure that prompt and effective corrective action is taken as needed. Corrective action may include procedural changes or action described in chapter XIV.

(3) Reevaluate the classification of information appearing in the public domain that falls under their security classification jurisdiction (see paragraphs 2-209 and 2-210).

g. Information subjected to unauthorized disclosure will be classified as provided under subsection 2-209.

Chapter VII Access, Dissemination, and Accountability

Section 1 Access

7-100. Policy

a. Except as otherwise provided for in subsection 7-101, no person may have access to classified information unless that person has been determined to be trustworthy and unless access is essential to the accomplishment of lawful and authorized Government purposes, that is, the person has the appropriate security clearance and a need-to-know. Further, cleared personnel may not have access until they have been given an initial security briefing (see subsection 10-102). Procedures shall be established by the head of each DoD Component to prevent unnecessary access to classified information. There shall be a demonstrable need for access to classified information before a request for a personnel security clearance can be initiated. The number of people cleared and granted access to classified information shall be maintained at the minimum number that is consistent with operational requirements and needs. No one has a right to have access to classified information solely by virtue of rank or position. The final responsibility for determining whether an individual's official duties require possession of or access to any element or item of classified information, and whether the individual has been granted the appropriate security clearance by proper authority, rests upon the individual who has authorized possession, knowledge, or control of the information and not upon the prospective recipient. These principles are equally applicable if the prospective recipient is a DoD Component, including commands and activities, other federal agencies, DoD contractors, foreign governments, and others.

b. Because of the extreme importance to the national security of Top Secret information and information controlled within approved Special Access Programs, employees shall not be permitted to work alone in areas where such information is in use or stored and accessible by those employees. This general policy is an extra safeguarding measure for the nation's most vital classified information and it is not intended to cast doubt on the integrity of DoD employees. The policy does not apply in those situations where one employee with access is left alone for brief periods during normal duty hours. When compelling operational requirements indicate the need, DoD Component heads may waive this requirement in specific, limited cases. This waiver authority may be delegated to the senior official (subsections 13-301 and 13-302) of the DoD Component who may redelegate the authority but only if so authorized by the head of the DoD Component (Any waiver should include provisions for periodically ensuring the health and welfare of individuals left alone in vaults or secure areas.)

(1) Each MACOM commander and Headquarters agency head is responsible for ensuring that the spirit and intent of the two-person integrity rule is met within his or her organization. The Secretary of the Army, Under Secretary, Assistant Secretaries of the Army, the Chief of Staff, Vice Chief of Staff, the Director of the Army Staff, and the heads of MACOMs and

Army Headquarters agencies may selectively waive the requirement when deemed necessary for mission accomplishment. This authority may not be further delegated.

(2) Waiver requests will be considered on an individual basis, and must be approved *personally*, and in writing, by an appropriate official. Security managers will retain records of approved waivers for reporting purposes. Two kinds of waivers should be considered either *permanent* or *temporary*:

(a) *Permanent*. The personal approval of an official listed in subparagraph 1, above, is required to waive the two-person integrity rule permanently in office or other areas where the rule simply cannot be applied, where alternative means and procedures cannot be used, and if the circumstances causing the request for waiver will not change in the foreseeable future. A copy of each approved permanent waiver will be forwarded to HQDA (DAMI-CIS) WASH DC 20310-1051.

(b) *Temporary*. In last-minute, emergency situations, the two-person integrity requirement may be temporarily waived by any general officer. Temporary waivers apply only to a particular instance, last minute requirement, or short-duration assignment involving work on Special Access Program or Top Secret information by a single individual. Repeated requests for temporary waiver of the rule from the same individual or office may indicate that permanent waiver is appropriate. The security manager will retain records of a temporary waivers granted by authorized officials. For reporting purposes, DAMI-CIS may periodically asks activities to provide the number of temporary waivers granted.

7-101. Access by persons outside the Executive Branch

Classified information may be made available to individuals or agencies outside the Executive Branch provided that such information is necessary for performance of a function from which the Government will derive a benefit or advantage, and that such release is not prohibited by the originating department or agency. Heads of DoD Components shall designate appropriate officials to determine, before the release of classified information, the propriety of such action in the interest of national security and assurance of the recipient's trustworthiness and need-to-know. **MACOM commanders, original Top Secret classification authorities, and officials they designate will make these determinations.**

a. *Congress*. Access to classified information or material by Congress, its committees, members, and staff representatives shall be in accordance with DoD Directive 5400.4 (reference (mm)). Any DoD employee testifying before a congressional committee in executive session in relation to a classified matter shall obtain the assurance of the committee that individuals present have a security clearance commensurate with the highest classification of the information that may be discussed. Members of Congress, by virtue of their elected positions, are not investigated or cleared by the Department of Defense.

(1) **U.S. Army activities may make information available to the Congress in confidence and in executive or closed sessions of committees to enable the Congress to perform its functions. U.S. Army activities not part of joint or combined commands will contact the Chief of Legislative Liaison (CLL), Office of the Secretary of the Army, WASH DC 20310-1600, for necessary guidance and assistance.**

(2) A person presenting oral testimony will advise the congressional committee of the classification of the information presented and of the need for protecting the national security. If the committee requests defense information that the witness does not know and must furnish later in writing, or if the committee needs only a specific part of the testimony in writing, the written material must the correct classification markings. Receipts will be obtained.

(3) National security information requested by a congressional committee through a member of the committee or a professional staff member may be furnished when needed for the performance of official committee functions. As necessary,

Army personnel will contact OCLL for guidance and assistance. National security information originated in an agency other than Army, but in Army custody, will not be released without the consent of the originating agency. All material furnished must bear correct classification markings. Receipts will be obtained.

(4) National security information will be given to any member of the Congress who requests it in writing. The rules in paragraph 3, above, apply.

(5) When members and staff of the Congress and congressional committees visit military installations, commanders may release national security information to them. The following procedures apply:

(a) The Secretary of the Army, through the OCLL, will authorize information to be released to committees of the Congress traveling under Army sponsorship.

(b) The sponsoring service will decide how much information is to be released to those traveling under the sponsorship of the other military services.

(c) If time permits, clearances will be obtained by message from the HQDA OCLL before releasing national security information to those not traveling under the sponsorship of the military services. When time does not allow, a commander may decide how much information to release.

(d) When a question arises on whether to release certain national security information to a member of the Congress or a congressional committee, no final refusal will be made until the case is submitted to the Secretary of the Army through the HQDA OCLL.

b. *Government Printing Office (GPO)*. Documents and material of all classifications may be processed by the GPO, which protects the information in accordance with the DoD/GPO Security Agreement of February 20, 1981.

c. *Representatives of the General Accounting Office (GAO)*. Representatives of the GAO may be granted access to classified information originated by and in possession of the Department of Defense when such information is relevant to the performance of the statutory responsibilities of that office, as set forth in DoD Directive 7650.1 (reference (nn)). Officials of the GAO, as designated in Appendix B, are authorized to certify security clearances, and the basis therefor. Certifications will be made by these officials pursuant to arrangements with the DoD Component concerned. Personal recognition or presentation of official GAO credential cards are acceptable for identification purposes.

d. *Industrial, educational, and commercial entities*.

(1) Bidders, contractors, grantees, educational, scientific or industrial organizations may have access to classified information only when such access is essential to a function that is necessary in the interest of the national security, and the recipients are cleared in accordance with DoD 5220.22-R (reference (e)).

(2) Contractor employees whose duties do not require access to classified information are not eligible for personnel security clearance and cannot be investigated under the DISP. In exceptional situations, when a military command is vulnerable to sabotage and its mission is of critical importance to national security, National Agency Checks may be conducted for suitability purposes on such individuals with the approval of the DUSD(P). **The DCSINT is the DA designee for this purpose. Completely justified requests will be forwarded through command channels to HQDA (DAM-CIS) WASH DC 20310-1051 in accordance with paragraph 3-601, AR 604-5 (reference (ll)).**

e. *Historical researchers* Persons outside the Executive Branch who are engaged in historical research projects may be authorized access to classified information provided that an authorized official within the DoD Component with classification jurisdiction over the information:

(1) Makes a written determination that such access is clearly consistent with the interests of national security in view of the intended use of the material to which access is granted by certifying that the requester has been found to be trustworthy pursuant to paragraph 7-100 a.;

(2) Limits such access to specific categories of information over which that DoD Component has classification jurisdiction and to any other category of information for which the researcher obtains the written consent of a DoD Component or non-DoD department or agency that has classification jurisdiction over information contained in or revealed by documents within the scope of the proposed historical research;

(3) Maintains custody of the classified material at a DoD installation or activity or authorizes access to documents in the custody of the NARS;

(4) Obtains the researcher's agreement to safeguard the information and to submit any notes and manuscript for review by all DoD Components or non-DoD departments or agencies with classification jurisdiction for a determination that no classified information is contained therein by execution of a statement entitled, "Conditions Governing Access to Official Records for Historical Research Purposes"; and

(5) Issues an authorization for access valid for not more than 2 years from the date of issuance that may be renewed under regulations of the issuing DoD Component.

(6) **Classified Army historical records and files normally contain material over which the Army does not possess final and exclusive classification authority. In most cases, the proponent agencies for these materials do not grant unofficial historical access to them, and the Army respects these conditions. Consequently, unofficial historical researchers will not be granted access to such Army files unless the researcher presents evidence of clearance for access by all other asset holders and concerned proponents. The Chief of Military History, however, will review individual Army classified documents for declassification when requested by researchers. Custodians of classified files in U.S.-Army records centers, records holding areas, libraries, collections, archives, institutions, and other repositories will establish similar procedures for files under their control.**

f. Former presidential appointees. Persons who previously occupied policy making positions to which they were appointed by the President may not remove classified information upon departure from office as all such material must remain under the security control of the U.S. Government. Such persons may be authorized access to classified information that they originated, received, reviewed, signed, or that was addressed to them while serving as such an appointee, provided that an authorized official within the DoD Component with classification jurisdiction for such information:

(1) Makes a written determination that such access is clearly consistent with the interests of national security in view of the intended use of the material to which access is granted and by certifying that the requester has been found to be trustworthy pursuant to paragraph 7-100 a.h 7-100 a.;

(2) Limits such access to specific categories of information over which that DoD Component has classification jurisdiction and to any other category of information for which the former appointee obtains the written consent of a DoD Component or non-DoD department or agency that has classification jurisdiction over information contained in or revealed by documents with the scope of the proposed access;

(3) Retains custody of the classified material at a DoD installation or activity or authorizes access to documents in the custody of the National Archives and Records Service; and

(4) Obtains the former presidential appointee's agreement to safeguard the information and to submit any notes and manuscript for review by all DoD Components or non-DoD departments or agencies with classification jurisdiction for a determination that no classified information is contained therein.

g. Judicial proceedings. DoD Directive 5405.2 (reference (iii)) governs the release of classified information in litigation.

h. Reserve Officers' Training Corps (ROTC). Confidential information may be released to cleared U.S. national members who are of the ROTC if the commanding general of the ROTC region or higher authority deems it necessary. The individuals making the final release of classified material will ensure that-

(1) **The material is marked and transmitted properly.**

(2) **The recipient has the facilities for, and is aware of the requirements for, safeguarding, handling, storing, and destroying the material.**

7-102. Access by foreign nationals, foreign governments, and international organizations

a. Classified information may be released to foreign nationals, foreign governments, and international organizations only when authorized under the provisions of the National Disclosure Policy and DoD Directive 5230.11 (reference (oo) **and AR 380-10**(reference (uuu))); **and**

b. Access to COMSEC information by foreign persons and activities shall be in accordance with policy issuances of the National Telecommunications and Information Systems Security Committee (NTISSC). (**Refer to AR 380-40** (reference (uuu)).)

7-103. Other situations

When necessary in the interests of national security, heads of DoD Components, or their single designee, may authorize access by persons outside the federal government, other than those enumerated in subsections 7-101 and 7-102, to classified information upon determining that the recipient is trustworthy for the purpose of accomplishing a national security objective; and that the recipient can and will safeguard the information from unauthorized disclosure. **The DCSINT is the Army designee for this purpose. Completely justified requests will be forwarded through command channels to HQDA (DAMI-CIS) WASH DC 20310-1051.**

7-104. Access required by other Executive Branch Investigative and law enforcement agents

a. Normally, investigative agents of other departments or agencies may obtain access to DoD information through established liaison or investigative channels.

b. When the urgency or delicacy of a Federal Bureau of Investigation (FBI), Drug Enforcement Administration (DEA), or Secret Service investigation precludes use of established liaison or investigative channels, FBI, DEA, or Secret Service agents may obtain access to DoD information as required. However, this information shall be protected as required by its classification. Before any public release of the information so obtained the approval of the head of the activity or higher authority shall be obtained.

7-105. Access by visitors

Procedures shall be established to control access to classified information by visitors. (DoD Instruction 5230.20(reference (aaa)) provides further guidance regarding foreign visitors.)

a. Except when a continuing, frequent working relationship is established, through which current security clearance and need-to-know are determined, DoD personnel visiting other activities of the Department of Defense, its contractors, and other agencies shall provide advance notification of the pending visit that establishes the visitor's security clearance and the purpose of the visit. Visit requests shall be signed by an official other than the visitor who is in a position to verify the visitor's security clearance.

b. Visit requests normally should include the following:

(1) Full name, date and place of birth, social security number, and rank or grade of visitor;

(2) Security clearance of the visitor;

(3) Employing activity of the visitor;

(4) Name and address of activity to be visited;

(5) Date and duration of proposed visit;

(6) Purpose of visit in sufficient detail to establish need-to-know; and

(7) Names of persons to be contacted.

c. Visit requests may remain valid for not more than 1 year.

7-106. Student officers attending civilian institutions and faculty members of civilian institutions

a. Classified collateral information, Secret and below, may be

released to student officers and faculty members of civilian institutions who have been granted clearance under AR 604-5 (reference (II)). Release of classified material will be made to the Professor of Military Science (PMS) at the institution. Only the PMS will release classified material to the student or faculty member under proper receipt, handling, and storage requirement.

b. All requests for classified material will be made in writing through the PMS. The PMS in turn will forward the request through the U.S. Army agency sponsoring the officer's attendance at the institution to the DA agency having primary interest in the material. If the institution has no PMS, the closest Army installation commander or senior Army instructor, as determined by the student officer's sponsoring agency, will handle the request. Requests must be for specific documents; blanket requests for classified files will be denied.

c. A thesis containing information from classified material will reflect the classification of the source document, as well as the source's downgrading/declassification instructions, and portion markings required by this regulation.

d. Before any classified thesis is submitted to a board of review, the PMS will ensure that members of the board have been cleared. The thesis will be delivered and retrieved by the PMS. If this is impractical, the registrar of the institution may be made a member of the board and will secure the thesis. Secretarial notes and related drafts will be disposed of as classified waste.

e. A student may prepare an abridged version of the thesis with no classified information for inclusion in the open files of the institution. Authorization by the student and the PMS is required for release of the open files.

Section 2 Dissemination

7-200. Policy

DoD Components shall establish procedures consistent with this Regulation for the dissemination of classified material. **A positive, realistic application of need-to-know and security clearance in allowing access to classified information should be followed to further, not hamper, military operations. Increased security risks dictate that need-to-know and clearance receive command consideration before classified material is transmitted to addressees located in hazardous or unfriendly areas.** The originating official or activity may prescribe specific restrictions on dissemination of classified information when necessary. (See subsection 4-505.)

7-201. Restraints on special access requirements

Special requirements with respect to access, distribution, and protection of classified information shall require prior approval in accordance with Chapter XII.

7-202. Information originating in a non-DoD department or agency

Except under rules established by the Secretary of Defense, or as provided by Section 102 of the National Security Act (reference (pp)), classified information originating in a department or agency other than Department of Defense shall not be disseminated outside the Department of Defense without the consent of the originating department or agency.

7-203. Foreign intelligence information

Dissemination of foreign intelligence information shall be in accordance with the provisions of DoD Instruction 5230.22 (AR 381-1) (reference (u)) and DoD Directive C-5230.23 (reference (zz)).

7-204. Restricted Data and Formerly Restricted Data

Information bearing the warning notices prescribed in subsection 4-501 and 4-502 shall not be disseminated outside authorized channels without the consent of the originator. Access to and dissemination

of Restricted Data by DoD personnel shall be subject to DoD Directive 5210.2 (reference (y)).

7-205. NATO Information

Classified information originated by NATO shall be safeguarded in accordance with DoD Directive 5100.55 (reference(z)).

7-206. COMSEC information

COMSEC information shall be disseminated in accordance with NACSI 4005 (reference (v)) and implementing instructions.

a. *JCS information.* Classified JCS information will be handled as prescribed in Chapter XV, Safeguarding JCS papers.

7-207. Dissemination of Top Secret information

a. Top Secret information, originated within the Department of Defense, may not be disseminated outside the Department of Defense without the consent of the originating DoD Component, or higher authority. **As an exception, information may be given out if operational necessity dictates that it be expeditiously given to non-DoD agencies, such as collocated representatives of other elements of the Executive Branch.**

b. Top Secret information, whenever segregable from classified portions bearing lower classifications, shall be distributed separately **unless this would be impractical.**

c. Standing distribution requirements for Top Secret information and materials, such as distribution lists, shall be reviewed at least annually to verify the recipients' need-to-know. **Army proponents for Top Secret materials containing an automatic distribution list will obtain annual reverification in writing from recipients certifying a continuing need for the information. Activity that do not respond to a request for need-to-know reverification will be deleted from the Top Secret distribution list.**

7-208. Dissemination of Secret and Confidential information

a. Secret and Confidential information, originated within the Department of Defense, may be disseminated within the Executive Branch, unless prohibited by the originator. (See subsection 4-505.)

b. Standing distribution requirements for Secret and Confidential information and materials, such as distribution lists, shall be reviewed at least annually to verify the recipients need-to-know. **Army proponents for Secret and Confidential documents containing a standard distribution list will obtain annual reverification in writing from document recipients certifying their continuing need for the information. Activities that do not respond to a request for need-to-know reverification will be deleted from that Secret or Confidential document distribution list.**

7-209. Code words, nicknames, and exercise terms

The use of code words, nicknames, and exercise terms is subject to the provisions of Chapter XII and Appendix C.

7-210. Scientific and technical meetings

Use of classified information in scientific and technical meetings is subject to the provisions of DoD Directive 5200.12 (reference (ii)).

Section 3 Accountability and Control

7-300. Top Secret information

DoD activities shall establish the following procedures:

a. *Control Officers.* Top Secret Control Officers (TSCOs) and alternates shall be designated within offices to be responsible for receiving, dispatching, and maintaining accountability registers of Top Secret documents. Such individuals shall be selected on the basis of experience and reliability, **and must already possess a minimum grade of GS-07 or rank of E-7 or SFC**, and shall have Top Secret security clearances. TSCOs need not be appointed in those instances where there is no likelihood of processing Top

Secret documentation. (In such circumstances, Army activity security managers should record the fact that a TSCO has not been appointed.) TSCOs or their alternates will—

(1) Maintain access to a current record of each person within the activity, command, office, or element who is cleared for, and has been authorized access to, Top Secret information.

(2) Maintain a current, accurate system of accountability within the activity for all Top Secret material.

(3) Ensure that TSCOs and alternates are cleared of accountability for Top Secret material when relieved of their responsibilities.

(4) Maintain the lowest number of Top Secret document possible consistent with current requirements. Destroy nonrecord and reading file copies as soon as practical. Ensure an annual review of all record copies of Top Secret documents for possible destruction, downgrading, declassification, or retirement.

(5) Conduct a monthly 10-percent inventory of Top Secret documents to ensure, by the tenth month, a 100-percent reconciliation of all documents or material on hand with those listed in the Top Secret accountability register.

b. Accountability

(1) *Top Secret registers.* Top Secret accountability registers shall be maintained by each office originating or receiving Top Secret information. Such registers shall be retained for 2 years and shall, as a minimum, reflect the following:

(a) Sufficient information to identify adequately the Top Secret document or material to include the title or appropriate short title, date of the document, and identification of the originator;

(b) The date the document or material was received;

(c) The number of copies received or later reproduced; and

(d) The disposition of the Top Secret document or material and all copies of such documents or material.

(e) **Identification of documents on DA Form 455 (Mail and Document Register) or a suitable substitute record. TSCOs will record the receipt, dispatch, downgrading, source, movement from one office to another, destruction, and current custodian of all Top Secret material for which they are responsible. DA Form 3964 (Classified Document Accountability Record) may be used as a single-entry register. These forms will also be used in subordinate elements to show the receipt, dispatch, downgrading, or destruction of all Top Secret material.**

(2) *Serialization and copy numbering.* Top Secret documents and material shall be numbered serially. In addition, each Top Secret document shall be marked to indicate its copy number, for example, copy -1- of -2-copies. Top Secret documents will be numbered in sequence as they are received in a calendar year series. This number will be posted to the document and control register. Changes to controlled documents will be assigned the same control number as the basic document, except that a suffix (such as "Change 4") will be added. The change will be incorporated immediately into the basic document; a notation will be added to the description block on the document register.

(3) *Disclosure records.* Each Top Secret document or item of material shall have appended to it a Top Secret disclosure record. The name and title of all individuals, including stenographic and clerical personnel to whom information in such documents and materials has been disclosed, and the date of such disclosure, shall be recorded thereon. Disclosures to individuals who may have had access to containers in which Top Secret information is stored, or who regularly handle a large volume of such information need not be so recorded. Such individuals, when identified on a roster, are deemed to have had access to such information. Disclosure records shall be retained for 2 years after the documents or materials are transferred, downgraded, or destroyed.

(a) **DA Form 969 will be used to record the required disclosure accounting. This form will be attached to the first page or cover of the document under the Top Secret Cover Sheet (SF 703). DA Form 969 will be maintained as follows:**

1. The Top Secret documents attached will be clearly and completely identified.

2. The names of persons granted access to the document and the date of initial access will be legibly recorded (typed or neatly printed).

(b) When a Top Secret document is transferred outside the office of origin, the DA Form 969 will be filed with the record copy.

(c) When a Top Secret document is received within an agency or command, the form will be prepared and attached to the document. When a document is dispatched, destroyed, or transferred, the form will be detached and filed in the office of record for 2 years.

(d) When an addressee distributes to subordinate commands or other agencies copies of, or Top Secret extracts from, a Top Secret document, a record of the additional distribution will be kept with the form.

1. The person having physical custody of the document is responsible for recording the names of those who have access.

2. If release is approved outside Army, or to a foreign government, the name of the receiving organization will be recorded on the DA Form 969 maintained by the lender.

c. Inventories. All Top Secret documents and material shall be inventoried at least once annually. **Within Army, TSCOs will conduct a monthly 10-percent inventory of Top Secret documents.** The inventory shall reconcile by the tenth month, the Top Secret accountability register with **100 percent of the Top Secret documents or material on hand.** At such time, each document or material shall be examined for completeness. DoD Component senior officials (subsections 13-301 and 13-302) may authorize the annual inventory of Top Secret documents and material in repositories, libraries, or activities that store large volumes of Top Secret documents or material to be limited to documents and material to which access has been granted within the past year, and 10 percent of the remaining inventory. If a storage system contains large volumes of information and security measures are adequate to prevent access by unauthorized persons, a request for waiver of the annual inventory requirement accompanied by full justification may be submitted through HQDA (DAMI-CIS) WASH DC 20310-1051 to the DUSD(P).

(1) **A 10 percent physical inventory of all Top Secret material in Army custody will be conducted each month so as to complete a 100-percent inventory on or about 1 April each year. The TSCO will conduct the inventories. A property cleared official with neither personal nor supervisory responsibility for the document will witness the 10-percent inventory report each month. Each monthly inventory will consist of a physical signing of the material or written evidence of authorized disposition, such as certificate of destruction or transfer receipt. Discrepancies found during the monthly inventory will be resolved immediately. Monthly inventory reports will be filed under AR 340-2 (reference (mmm)) or AR 340-18 series.**

(2) **Limited physical inventories (10 per-cent or less of total amount of Top Secret material on hand) may be authorized by MACOM commanders and heads of Army Headquarters agencies.**

d. Retention. Top Secret information shall be retained only to the extent necessary to satisfy current requirements. Custodians shall destroy nonrecord copies of Top Secret documents when no longer needed. Record copies of documents that cannot be destroyed shall be reevaluated and, when appropriate, downgraded, declassified, or retired to designated records centers.

e. Receipts. Top Secret documents and material will be accounted for by a continuous chain of receipts. Receipts shall be maintained for 2 years.

f. Transfer of accountability.

(1) **Before leaving a command or agency, each TSCO or alternate will account by joint inventory for Top Secret documents and material for which he or she has custodial responsibility. The commander or head of the agency will prescribe appropriate procedures. Such joint inventories are required under the following circumstances:**

(a) On change of duty assignment within an office, activity, or installation.

(b) On permanent change of station.

(c) On temporary absence of more than 30 calendar days.

(d) On separation from the military service or termination of employment with the Army.

(2) Transfer of accountability will be by formal written procedure and will be approved by the commander or agency head, consistent with the accountability requirements in this regulation. One hundred percent of the Top Secret material in the custody of or charged to a person must be properly accounted for before the person is given a final clearance from a unit or installation.

(3) On the death of a TSCO or alternate, or on hospitalization for more than 30 days, a commander will appoint an officer to conduct a complete inventory of Top Secret documents formerly in the individual's custody. This inventory should begin as soon as practicable. Written results of the inventory should be retained in the files of the local office of interest.

7-301. Secret information

Administrative procedures shall be established by each DoD Component for controlling Secret information and material originated or received by an activity; distributed or routed to a sub-element of such activity; and disposed of by the activity by transfer of custody or destruction. The control system for Secret information must be determined by a practical balance of security and operating efficiency and must meet the following minimum requirements:

a. It must provide a means to ensure that Secret material sent outside a major subordinate element (the activity) of the DoD Component concerned has been delivered to the intended recipient. Such delivery may be presumed where the material is sent electronically over secure voice or data circuits. Ensuring physical delivery may be accomplished by use of a receipt as provided in paragraph 8-202 b. or through hand-to-hand transfer when the receiving party acknowledges responsibility for the Secret material. **Army activities will use the DA Form 3964 as a means to verify an addressee's receipt of Secret material sent by mail outside the activity. Individuals handcarrying Secret material will obtain the recipient's verbal acknowledgment that the recipient will assume responsibility for the material.**

b. It must provide a record of receipt and dispatch of Secret material by each major subordinate element. The dispatch record requirement may be satisfied when the distribution of Secret material is evident from addressees or distribution lists for classified documentation. Records of receipt and dispatch are required regardless of the means used to ensure delivery of the material (see paragraph a., above). **The DA Form 3964 returned by the recipient of a Secret document will serve as a record of receipt. The distribution lists for Secret document will serve as dispatch records for the material.**

c. Records of receipt and dispatch for Secret material shall be retained for a minimum of 2 years. **DA Forms 3964 and document distribution lists that serve as official records of receipt and dispatch (paragraphs a and b, above) will be retained for 2 years.**

7-302. Confidential information

Administrative controls shall be established to protect Confidential information received, originated, transmitted, or stored by an activity. **Administrative controls for Confidential information beyond those prescribed by this regulation are prohibited.**

7-303. Receipt of classified material

Procedures shall be developed within DoD activities to protect incoming mail, bulk shipments, and items delivered by messenger until a determination is made whether classified information is contained therein. Screening points shall be established to limit access to classified information to cleared personnel. **This protection is required only for material transmitted or transported by a**

means authorized for classified information as specified in chapter VIII of this regulation. It is recommended for other material whenever practicable.

7-304. Working papers

a. Working papers are documents and material accumulated or created in the preparation of finished documents and material. **Working papers recorded on diskettes or other word processing media are subject to the provisions of this paragraph (refer to AR 380-380 (reference (h)) for additional security requirements and procedures which apply to these items).** Working papers containing classified information shall be:

(1) Dated when created **and marked to indicate they are working papers;**

(2) Marked with the highest classification of any information contained therein;

(3) Protected in accordance with the assigned classification;

(4) Destroyed when no longer needed; and

(5) Accounted for, controlled, and marked in the manner prescribed for a finished document of the same classification when:

(a) Released by the originator outside the activity or transmitted electrically or through message center channels within the activity **(Army is an "activity" for purposes of this paragraph);**

(b) Retained more than 90 days from date of origin;

(c) Filed permanently; or

(d) Top Secret information is contained therein.

b. Heads of DoD Components, or their single designees, may approve waivers of accountability, control, and marking requirements for working papers containing Top Secret information for activities within their Components on a case-by-case basis provided a determination is made that:

(1) The conditions set forth in subparagraphs a.5.(a), (b), or(c), above, will remain in effect;

(2) The activity seeking a waiver routinely handles large volumes of Top Secret working papers and compliance with prescribed accountability, control, and marking requirements would have an adverse affect on the activity's mission or operations; and

(3) Access to areas where Top Secret working papers are handled is restricted to personnel who have an appropriate level of clearance, and other safeguarding measures are adequate to preclude the possibility of unauthorized disclosure.

(e) In all cases in which a waiver is granted under b., above, the DUSD(P) shall be notified. **Requests for waivers will be submitted through command channels to HQDA (DAMI-CIS), WASH DC 20310-1051. Requests must address the conditions specified in paragraph b, above.**

7-305. Restraint on reproduction

Except for the controlled initial distribution of information processed or received electrically or as provided by subsections 1-205 and 3-602, portions of documents and materials that contain Top Secret information shall not be reproduced without the consent of the originator or higher authority. Any stated prohibition against reproduction shall be observed strictly (See subsection 4-505) To the extent possible, DoD Components **and individual Army activities** shall establish classified reproduction facilities where only designated personnel can reproduce classified materials and institute key control systems for reproduction areas Also, when possible, two people shall be involved in the reproduction process to help assure positive control and safeguarding of all copies The following additional measures apply to reproduction equipment and to the reproduction of classified information:

a. Copying of documents containing classified information shall be minimized;

b. Officials authorized to approve the reproduction of Top Secret and Secret information shall be designated by position title and shall review the need for reproduction of classified documents and material with a view toward minimizing reproduction **(commanders, agency heads, and activity heads will designate such officials.**

DA Form 3964, DD Form 844 (Requisition for Local Duplicating Service), or other substitute record may be used to indicate reproduction approval);

c. Specific reproduction equipment shall be designated for the reproduction of classified information. Rules for reproduction of classified information shall be posted on or near the designated equipment (**Information on hazards associated with various types of reproduction equipment may be obtained from the Chief, Intelligence Materiel Activity, ATTN: AMXIM-PS, Fort Meade, MD 20755-5313.**);

d. Notices prohibiting reproduction of classified information shall be posted on equipment used only for the reproduction of unclassified information;

e. DoD Components shall ensure that equipment used for reproduction of classified information does not leave latent images in the equipment or on other material (**reproduction equipment that leaves latent images on material within the equipment, such as intermediate paper rolls, may be used for reproduction of classified information only if the material can be properly safeguarded and disposed of as classified waste**);

f. All copies of classified documents reproduced for any purpose including those incorporated in a working paper are subject to the same controls prescribed for the document from which the reproduction is made; and

g. Records shall be maintained for 2 years to show the number and distribution of reproduced copies of all Top Secret documents, of all classified documents covered by special access programs distributed outside the originating agency, and of all Secret and Confidential documents that are marked with special dissemination and reproduction limitations. (See subsection 4-505.)

Chapter VIII Transmission

Section 1 Methods of Transmission or Transportation

8-100. Policy

Classified information may be transmitted or transported only as specified in this chapter.

8-101. Top Secret information

Transmission of Top Secret information shall be effected only by:

- a. The **Defense Courier Service (DCS)**;
- b. Authorized DoD Component Courier Services;
- c. If appropriate, the Department of State Courier System;
- d. Cleared and designated U.S. military personnel and Government civilian employees traveling on a conveyance owned, controlled, or chartered by the U.S. Government or DoD contractors;
- e. Cleared and designated U.S. Military personnel and government civilian employees by surface transportation;
- f. Cleared and designated U.S. Military personnel and government civilian employees on scheduled commercial passenger aircraft within and between the United States, its Territories, and Canada, when approved in accordance with paragraph 8-303 a.
- g. Cleared and designated U.S. Military personnel and government civilian employees on scheduled commercial passenger aircraft on flights outside the United States, its territories, and Canada, when approved in accordance with paragraph 8-303 b.
- h. Cleared and designated DoD contractor employees within and between the United States and its Territories provided that the transmission has been authorized in writing by the appropriate contracting officer or his designated representative, and the designated employees have been briefed on their responsibilities as couriers or escorts for the protection of Top Secret material. Complete guidance for Top Secret transmission is specified in DoD 5220.22-R and DoD 5220.22-M (references (e) and (f)).

- i. A cryptographic system authorized by the Director, NSA, or

via a protected distribution system designed and installed to meet the standards included in the National COMSEC and Emanations Security (EM-SEC) Issuance System.

8-102. Secret information

Special Access Program information may be forwarded by any means approved for transmission of Top Secret information, provided the program manager approves. Special Access Program materials may also be transmitted by U.S. Postal Service Registered Mail (see paragraph 8-200a for packaging instructions). Transmission of Secret information may be effected by:

a. Any of the means approved for the transmission of Top Secret information except that Secret information may be introduced into the DCS only when the control of such information cannot be otherwise maintained in U.S. custody. This restriction does not apply to SCI and COMSEC information;

b. Appropriately cleared contractor employees within and between the United States and its Territories provided that (1) the designated employees have been briefed in their responsibilities as couriers or escorts for protecting Secret information; (2) the classified information remains under the constant custody and protection of the contractor personnel at all times; and (3) the transmission otherwise meets the requirements specified in DoD 5220.22-R and DoD 5220.22-M (references (e) and (f)). In other areas, appropriately cleared DoD contractor employees may transmit classified material only as prescribed by references (e) and (f).

c. U.S. Postal Service registered mail within and between the United States and its Territories;

d. U.S. Postal Service registered mail through Army, Navy, or Air Force Postal Service facilities outside the United States and its Territories, provided that the information does not at any time pass out of U.S. citizen control and does not pass through a foreign postal system or any foreign inspection;

e. U.S. Postal Service and Canadian registered mail with registered mail receipt between U.S. Government and Canadian Government installations in the United States and Canada;

f. Carriers authorized to transport Secret information by way of a Protective Security Service (PSS) under the DoD Industrial Security Program. This method is authorized only within the U.S. boundaries and only when the size, bulk, weight, and nature of the shipment, or escort considerations make the use of other methods impractical. Routings for these shipments will be obtained from the Military Traffic Management Command (MTMC);

g. The following carriers under appropriate escort: government and government contract vehicles including aircraft, ship of the U.S. Navy, civil service-operated U.S. Naval ships, and ships of U.S. registry. Appropriately cleared operators of vehicles, officers of ships or pilots of aircraft who are U.S. citizens may be designated as escorts provided the control of the carrier is maintained on a 24-hour basis. The escort shall protect the shipment at all times, through personal observation or authorized storage to prevent inspection, tampering, pilferage, or unauthorized access. However, observation of the shipment is not required during the period it is stored in an aircraft or ship in connection with flight or sea transit, provided the shipment is loaded into a compartment secure, safe-like container that is:

(1) Constructed of solid building material that provides a substantial resistance to forced entry;

(2) Constructed in a manner that precludes surreptitious entry through disassembly or other means, and that attempts at surreptitious entry would be readily discernible through physical evidence of tampering; and

(3) Secured by a numbered cable seal lock affixed to a substantial metal hasp in a manner that precludes surreptitious removal and provides substantial resistance to forced entry.

h. Use of specialized containers aboard aircraft requires that:

(1) Appropriately cleared personnel maintain observation of the material as it is being loaded aboard the aircraft and that observation of the aircraft continues until it is airborne;

(2) Observation by appropriately cleared personnel is maintained at the destination as the material is being off-loaded and at any

intermediate stops. Observation will be continuous until custody of the material is assumed by appropriately cleared personnel.

8-103. Confidential Information

Transmission of Confidential information may be effected by:

a. Means approved for the transmission of Secret information. However, U.S. Postal Service registered mail shall be used for Confidential only as indicated in paragraph b. below;

b. U.S. Postal Service registered mail for:

(1) Confidential information of NATO;

(2) Other Confidential material to and from FPO or APO addressees located outside the United States and its Territories;

(3) Other addressees when the originator is uncertain that their location is within U.S. boundaries. Use of return postal receipts on a case-by-case basis is authorized.

(4) **Material dispatched to and from U.S. activities in Panama.**

(5) **COMSEC information as prescribed by AR 380-40 and TB 380-41 (reference (v)).**

c. U.S. Postal Service first class mail between DoD Component locations anywhere in the United States and its Territories. However, the outer envelope or wrappers of such Confidential material shall be endorsed "POSTMASTER: Address Correction Requested/ Do Not Forward." **This endorsement should be stamped in black ink to facilitate the identification of sensitive mail. The stamped letters should be approximately 1/4 inch in size, or larger than typed text.** Certified or, if appropriate, registered mail shall be used for material directed to DoD contractors and to non-DoD agencies of the Executive Branch. U.S. Postal Service Express Mail Service or **Federal Express Service** may be used between DoD Component locations, between DoD contractors and between DoD Components and DoD contractors.

d. Within U.S. boundaries, commercial carriers that provide a Constant Surveillance Service (CSS). Information concerning commercial carriers that provide CSS may be obtained from the MTMC.

e. In the custody of commanders or masters of ships of U.S. registry who are U.S. citizens. Confidential information shipped on ships of U.S. registry may not pass out of U.S. Government control. The commanders or masters must give and receive classified information receipts and agree to:

(1) Deny access to the Confidential material by unauthorized persons, including customs inspectors, with the understanding that Confidential cargo that would be subject to customs inspection will not be unloaded; and

(2) Maintain control of the cargo until a receipt is obtained from an authorized representative of the consignee.

f. Such alternative or additional methods of transmission as the head of any DoD Component may establish by rule or regulation, provided those methods afford at least an equal degree of security.

8-104. Transmission of classified material to foreign governments

After a determination by designated officials pursuant to DoD Directive 5230.11 (reference oo) that classified information or material may be released to a foreign government, the material shall be transferred between authorized representatives of each government in compliance with the provisions of this Chapter. To assure compliance, each contract, agreement, or other arrangement that involves the release of classified material to foreign entities shall either contain transmission instructions or require that a separate transportation plan be approved by the appropriate DoD security and transportation officials prior to release of the material. (See DoD TS-5105.21-M-3 (reference ddd) for guidance regarding SCI.)

a. Classified material to be released directly to a foreign government representative shall be delivered or transmitted only to a person who has been designated in writing by the recipient government as its officer agent, or employee (hereafter referred to as the designated representative). Foreign governments may designate a freight forwarder as their agent. This written designation shall contain assurances that such person has a security clearance at the appropriate

level and that the person will assume full security responsibility for the material on behalf of the foreign government. The recipient will be required to execute a receipt for the material, regardless of the level of classification.

b. Classified material that is suitable for transfer by courier or postal service, and which cannot be transferred directly to a foreign government's designated representative as specified in paragraph a., above, shall be transmitted by one of the methods specified in subsection 8-101, 8-102, or 8-103 for the designated classification level to:

(1) An embassy, consulate, or other official agency of the recipient government having extraterritorial status in the United States, or to

(2) A U.S. Embassy or a U.S. military organization in the recipient country or in a third-party country, if applicable, for delivery to a designated representative of the intended recipient government. In either case, the assurance in paragraph a., above, and a receipt, must be obtained.

c. The shipment of classified material as freight via truck, rail, aircraft, or ship shall be in compliance with the following:

(1) *Shipments resulting from foreign military sales (FMS)*: DoD officials authorized to approve a FMS transaction that involves the delivery of U.S. classified material to a foreign purchaser shall, at the outset of negotiation or consideration of proposal, consult with DoD transportation authorities (Military Traffic Management Command, Military Sealift Command, Military Airlift Command, or other, as appropriate) to determine whether secure shipment from the CONUS point of origin to the ultimate foreign destination is feasible. Normally, the United States will use the Defense Transportation System (DTS) to deliver classified material to the recipient government. If, in the course of FMS case processing, the foreign purchaser proposes to take delivery and custody of the classified material in the United States and use its own facilities and transportation for onward shipment to its territory, the foreign purchaser or its designated representative shall be required to submit a transportation plan for DoD review and approval. This plan, as a minimum, shall specify the storage facilities, delivery and transfer points, carriers, couriers or escorts, and methods of handling to be from the CONUS point of origin to the final destination and return shipment when applicable. (See Appendix E.) Security officials of the DoD Component that initiates the FMS transaction shall evaluate the transportation plan to determine whether the plan adequately ensures protection of the highest level of classified material involved. Unless the DoD Component initiating the FMS transaction approves the transportation plan as submitted, or it is modified to meet U.S. security standards, shipment by other than DTS shall not be permitted. Transmission instructions or the requirement for an approved transportation plan shall be incorporated into the security requirements of the United States Department of Defense Offer and Acceptance (DD Form 1513).

(2) *Shipments resulting from direct commercial sales*: Classified shipments resulting from direct commercial sales must comply with the same security standards that apply to FMS shipments. Defense contractors, therefore, will consult, as appropriate, with the purchasing government, the DIS Regional Security Office, and the owning Military Department prior to consummation of a commercial contract that will result in the shipment of classified material to obtain approval of the transportation plan.

(3) *Delivery within the United States, its Territories, or possessions*: Delivery of classified material to a foreign government at a point within the United States, its territories, or its possessions, shall be made only to a person identified in writing by the recipient government as its designated representative as specified in paragraph a., above. The only authorized delivery points are:

(a) An embassy, consulate, or other official agency under the control of the recipient government.

(b) Point of origin. When a designated representative of the recipient government accepts delivery of classified U.S. material at the point of origin (for example, a manufacturing facility or depot), the DoD official who transfers custody shall obtain a receipt for the classified material and assure that the recipient is cognizant of

secure means of onward movement of the classified material to its final destination, consistent with the approved transportation plan.

(c) Military or commercial ports of embarkation (POE) that are recognized points of departure from the United States, its territories, or possessions, for onloading aboard a ship, aircraft, or other carrier authorized under subparagraph 5., below. In these cases, the transportation plan shall provide for U.S.-controlled secure shipment to the CONUS transshipment point and the identification of a secure storage facility, government or commercial, at or in proximity to the POE. A DoD official authorized to transfer custody is to supervise or observe the onloading of FMS material being transported via the DTS and other onloading wherein physical and security custody of the material has yet to be transferred formally to the foreign recipient. In the event that transfer of physical and security custody cannot be accomplished promptly, the DoD official shall ensure that the classified material is either returned to a secure storage facility of the U.S. shipper (government or contractor); or segregated and placed under constant surveillance of a duly cleared U.S. security force at the POE; or held in the secure storage facility (government or commercial) designated in the transportation plan.

(d) Freight forwarder facility that is identified by the recipient government as its designated representative and that is cleared in accordance with subparagraph 6., below, to the level of the classified material to be received. In these cases, a person identified as a designated representative must be present to accept delivery of the classified material and receipt for it, to include full acceptance of security responsibility.

(4) *Delivery outside the United States, its Territories, or possessions:*

(a) Delivery within the recipient country. Classified U.S. material to be delivered to a foreign government within the recipient country shall be delivered on arrival in the recipient country to a U.S. Government representative who shall arrange for its transfer to a designated representative of the recipient government. If the shipment is escorted by a U.S. Government official authorized to accomplish the transfer of custody, the material may be delivered directly to the recipient government's designated representative upon arrival.

(b) Delivery within a third country. Classified material to be delivered to a foreign government representative within a third country shall be delivered to an agency or installation of the United States, or of the recipient government, that has extraterritorial status or otherwise is exempt from the jurisdiction of the third country. Unless the material is accompanied by a U.S. Government official authorized to accomplish the transfer of custody, a U.S. Government official shall be designated locally to receive the shipment upon arrival and be vested with authority to effect delivery to the intended recipient government's designated representative.

(5) *Overseas carriers:* Overseas shipments of U.S. classified material shall be made only via ships, aircraft, or other carriers that are: (a) owned or chartered by the U.S. Government or under U.S. registry, (b) owned or chartered by or under the registry of the recipient government, or (c) otherwise expressly authorized by the head of the DoD Component having classification jurisdiction over the material involved. Overseas shipments of classified material shall be escorted, prepared for shipment, packaged, and stored on-board as prescribed elsewhere in this Chapter and in DoD 5220.22-R and DoD 5220.22-M (references (e) and (f)).

(6) *Freight forwarders:* Only freight forwarders that have been granted an appropriate security clearance by the Department of Defense or the recipient government are eligible to receive, process, and store U.S. classified material authorized for release to foreign governments. However, a freight forwarder that does not have access to or custody of the classified material need not be cleared.

8-105. Consignor-consignee responsibility for shipment of bulky material

The consignor of a bulk shipment shall:

a. Normally, select a carrier that will provide a single line service

from the point of origin to destination, when such a service is available;

b. Ship packages weighing less than 200 pounds in closed vehicles only;

c. Notify the consignee, and military transshipping activities, of the nature of the shipment (including level of classification), the means of shipment, the number of seals, if used, and the anticipated time and date of arrival by separate communication at least 24 hours in advance of arrival of the shipment. Advise the first military transshipping activity that, in the event the material does not move on the conveyance originally anticipated, the transshipping activity should so advise the consignee with information of firm transshipping date and estimated time of arrival. Upon receipt of the advance notice of a shipment of classified material, consignees and transshipping activities shall take appropriate steps to receive the classified shipment and to protect it upon arrival.

d. Annotate the bills of lading to require the carrier to notify the consignor immediately by the fastest means if the shipment is unduly delayed enroute. Such annotations shall not under any circumstances disclose the classified nature of the commodity. When seals are used, annotate substantially as follows: DO NOT BREAK SEALS EXCEPT IN EMERGENCY OR UPON AUTHORITY OF CONSIGNOR OR CONSIGNEE. IF BROKEN APPLY CARRIER'S SEALS AS SOON AS POSSIBLE AND IMMEDIATELY NOTIFY CONSIGNOR AND CONSIGNEE.

e. Require the consignee to advise the consignor of any shipment not received more than 48 hours after the estimated time of arrival furnished by the consignor or transshipping activity. Upon receipt of such notice, the consignor shall immediately trace the shipment. If there is evidence that the classified material was subjected to compromise, the procedures set forth in Chapter VI of this Regulation for reporting compromises shall apply.

8-106. Transmission of COMSEC information

COMSEC information shall be transmitted in accordance with National COMSEC Instruction 4005 (reference (v)).

8-107. Transmission of Restricted Data

Restricted Data shall be transmitted in the same manner as other information of the same security classification. The transporting and handling of nuclear weapons or nuclear components shall be in accordance with DoD Directives 4540.1 and 5210.41 (references (qq) and (rr)) and applicable DoD Component directives and regulations.

Section 2

Preparation of Material for Transmission, Shipment, or Conveyance

8-200. Envelopes or containers

a. Whenever classified information is transmitted, it shall be enclosed in two opaque sealed envelopes or similar wrappings when size permits, except as provided below. **As a rule, whenever Special Access Program information is transmitted via U.S. Postal Service, an opaque or cardboard sheet will be inserted in the inner envelope prior to transmission. This requirement applies to Special Access Program packages containing seven pages or less of material.**

b. Whenever classified material is transmitted of a size not suitable for transmission in accordance with paragraph a., above, it shall be enclosed in two opaque sealed containers, such as boxes or heavy wrappings.

(1) If the classified information is an internal component of a packageable item of equipment, the outside shell or body may be considered as the inner enclosure provided it does not reveal classified information.

(2) If the classified material is an inaccessible internal component of a bulky item of equipment that is not reasonably packageable, the outside or body of the item may be considered to be a sufficient enclosure provided the shell or body does not reveal classified information.

(3) If the classified material is an item or equipment that is not reasonably packageable and the shell or body is classified it shall be concealed with an opaque covering that will hide all classified features.

(4) Specialized shipping containers, including closed cargo transporters, may be used instead of the above packaging requirements. In such cases, the container may be considered the outer wrapping or cover.

c. Material used for packaging shall be of such strength and durability as to provide security protection while in transit, prevent items from breaking out of the container, and to facilitate the detection of any tampering with the container. The wrappings shall conceal all classified characteristics.

d. Closed and locked vehicles, compartments, or cars shall be used for shipments of classified information except when another method is authorized by the consignor. Alternative methods authorized by the consignor must provide security equivalent to or better than the methods specified herein. In all instances, individual packages weighing less than 200 pounds gross shall be shipped only in a closed vehicle.

e. To minimize the possibility of compromise of classified material caused by improper or inadequate packaging thereof, responsible officials shall ensure that proper wrappings are used for mailable bulky packages. Responsible officials shall require the inspection of bulky packages to determine whether the material is suitable for mailing or whether it should be transmitted by other approved means.

f. When classified material is handcarried outside an activity, a locked briefcase may serve as the outer wrapper. In such cases, the addressing requirements of paragraph 8-201 d. do not apply; however, the requirements of paragraph 8-201 c. are applicable. **A locked briefcase may not be used as an outer wrapper when classified material is handcarried aboard commercial airline flights.**

8-201. Addressing

a. Classified information shall be addressed to an official government activity or DoD contractor with a facility clearance and not to an individual. This is not intended, however, to prevent use of office code numbers or such phrases in the address as "Attention: Research Department," or similar aids in expediting internal routing, in addition to the organization address.

b. Classified written information shall be folded or packed in such a manner that the text will not be in direct contact with the inner envelope or container. A receipt form shall be attached to or enclosed in the inner envelope or container for all Secret and Top Secret information; Confidential information will require a receipt only if the originator deems it necessary. The mailing of written materials of different classifications in a single package should be avoided. However, when written materials of different classifications are transmitted in one package, they shall be wrapped in a single inner envelope or container. A receipt listing all classified information for which a receipt is requested shall be attached or enclosed. The inner envelope or container shall be marked with the highest classification of the contents.

c. The inner envelope or container shall show the address of the receiving activity, classification, including, where appropriate, the "Restricted Data" marking, and any applicable special instructions. **The sender's return address (to include office symbol) will be shown on inner envelopes or containers.** It shall be carefully sealed to minimize the possibility of access without leaving evidence of tampering.

d. An outer or single envelope or container shall show the complete and correct address and the return address of the sender.

e. An outer cover or single envelope or container shall not bear a classification marking, a listing of the contents divulging classified information, or any other unusual data or marks that might invite special attention to the fact that the contents are classified.

f. Care must be taken to ensure that classified information intended only for U.S. elements of international staffs or other organizations is addressed specifically to those elements. **AR 340-25 contains the following:**

(1) **Addresses of Military Assistance Advisory Groups, Military Liaison Offices, Joint U.S. Military Advisory Groups, and similar activities.**

(2) **Addresses of U.S. Defense Attache Offices.**

(3) **Procedures for protecting material during transmission.**

8-202. Receipt systems

a. Top Secret information shall be transmitted under a chain of receipts covering each individual who gets custody.

b. Secret information shall be covered by a receipt when transmitted to a foreign government (including foreign government embassies located in the United States) and when transmitted between major subordinate elements of DoD Components and other authorized addressees except that a receipt is not required when there is a hand-to-hand transfer between U.S. personnel and the recipient acknowledges responsibility for the Secret information. **A DA Form 3964 will be used as a receipt for Secret material transmitted between Army activities when U.S. Postal Service resources or mailrooms are used. A receipt is not required when the Secret information is handcarried between Army and/or other U.S. Government activities, and the recipient personally acknowledges responsibility for the material. A DA Form 3964 will be obtained in all instances of transfer, either by hand or mail, to defense contractors.**

c. Receipts for Confidential information are not required except when the information is transmitted to a foreign government (including foreign government embassies located in the United States) or upon request. **Within Army, internal receipts for Confidential information are prohibited unless required by a non-Army originator or by other regulations or directives.**

d. Receipts shall be provided by the transmitter of the material and the forms shall be attached to the inner cover.

(1) Postcard receipt forms may be used.

(2) Receipt forms shall be unclassified and contain only such information as is necessary to identify the material being transmitted.

(3) Receipts shall be retained for at least 2 years.

(4) **The addressor, addressee, identity of the document by unclassified or short title, file number (if any), and identification of all Top Secret or Secret enclosures will be entered on the classified document receipt form. Unclassified documents, comments, endorsements, cover letters, enclosures, etc., will not be included on the receipt form. Receipts will be signed immediately by the recipient and returned to the sender. The name of the recipient will be legibly printed, stamped, or typed on the form. When a shipment of material is split because of weight or size, a receipt will accompany each container. Each receipt will list only the portion of the material transmitted in the accompanying container.**

(5) **The following forms will be used as receipts for classified material:**

(a) **DA Form 3964 will be used to acknowledge receipt of a document.**

(b) **SF 153 (COMSEC Material Report) is authorized in place of DA Form 3964 as a receipt for COMSEC material.**

(c) DA Form 3964 or DA Form 455 will be used as an internal receipt for Top Secret and, when authorized, Secret material.

(d) DA Form 1965 (Delivery and Pick Up Service) may be used as a manifest for delivery by courier or messenger of sealed containers of single or several classified documents. The Top Secret and Secret contents will have an attached receipt form to be completed by the recipient and returned to the originator.

(e) ADP cards that provide full identification of the classified material in other than ADP machine-readable language may be used to acknowledge receipt of material.

e. In those instances where a fly-leaf (page check) form is used

with classified publications, the postcard receipt will not be required.

8-203. Exceptions

Exceptions may be authorized to the requirements contained in this Chapter by the head of the Component concerned or designee, provided the exception affords equal protection and accountability to that provided above. Proposed exceptions that do not meet these minimum standards shall be submitted to the DUSD(P) for approval. **The DCSINT approves exceptions within the Army. Requests will be forwarded through command channels to HQDA (DAMI-CIS) WASH DC 20310-1051.**

Section 3 Restrictions, Procedures, and Authorization Concerning Escort or Handcarrying of Classified Information

8-300. General restrictions

Appropriately cleared personnel may be authorized **in writing by the security manager** to escort or handcarry classified material between their duty station and an activity to be visited subject to the following conditions:

a. The storage provisions of Section 1 and subsection 5.206 of Chapter V of this regulation shall apply at all stops enroute to the destination, unless the information is retained in the personal possession and under constant surveillance of the individual at all times. The hand-carrying of classified information on trips that involve an overnight stop is not permissible without advance arrangements for proper overnight storage in a U.S. Government facility or, if in the United States, a cleared contractor's facility that has the requisite storage capability.

b. Classified material shall not be read, studied, displayed, or used in any manner in public conveyances or places.

c. When classified material is carried in a private, public, or government conveyance, it shall not be placed in any detachable storage compartment such as automobile trailers, luggage racks, aircraft travel pods, or drop tanks nor, under any circumstances, left unattended. **Under no circumstances will Army couriers leave classified material unattended in locked vehicles, car trunks, trains, airplanes, etc., during rest or meal stops, overnight, or at any other time whatsoever.**

d. Responsible officials shall provide a written statement to all individuals escorting or carrying classified material aboard commercial passenger aircraft authorizing such transmission. This authorization statement may be included in official travel orders and should ordinarily permit the individual to pass through passenger control points without the need for subjecting the classified material to inspection. Specific procedures for carrying classified documents aboard commercial aircraft are contained in subsection 8-302.

e. Each activity shall list all classified information carried or escorted by traveling personnel. All classified information shall be accounted for.

f. Individuals authorized to hand-carry or escort classified material shall be fully informed of the provisions of this Chapter, and shall sign a statement to that effect prior to the issuance of written authorization or identification media. This statement shall be retained for a minimum of 2 years; it need not be executed on each occasion that the individual is authorized to transport classified information provided a signed statement is on file. **Security managers will retain signed courier statements in local files. The courier statements will be executed prior to issuance of written courier authorization letters, or DD Forms 2501 (Courier Authorization Card). Complete instructions on use of the DD Form 2501 will be issued prior to dissemination of the Card.**

8-301. Restrictions on handcarrying classified information aboard commercial passenger aircraft

Classified information shall not be hand-carried aboard commercial passenger aircraft unless:

a. There is neither time nor means available to move the information in the time required to accomplish operational objectives or contract requirements.

b. The hand-carry has been authorized by an appropriate official in accordance with subsection 8-303.

c. In the case of the hand-carry of classified information across international borders, arrangements have been made to ensure that such information will not be opened by customs, border, postal, or other inspectors, either U.S. or foreign.

d. The hand-carry is accomplished aboard a U.S. carrier. Foreign carriers will be utilized only when no U.S. carrier is available and then the approving official must ensure that the information will remain in the custody and physical control of the U.S. escort at all times.

8-302. Procedure for handcarrying classified information aboard commercial passenger aircraft

a. Basic requirements

(1) Advance and continued coordination by the DoD activity and contractor officials shall be made with departure airline and terminal officials and, when possible, with intermediate transfer terminals to develop mutually satisfactory arrangements within the terms of this issuance and Federal Aviation Administration (FAA) guidance. Specifically, a determination should be made beforehand whether documentation described in paragraph d., below, will be required. Local FAA Security Officers can be of assistance in making this determination. To aid coordination and planning, a listing of FAA field offices is at Appendix D.

(2) The individual designated as courier shall be in possession of either DD Form 2, "Armed (or Uniformed) Services Identification Card" (any color), or other DoD or contractor picture identification card and written authorization to carry classified information.

(3) **The classified material must remain in the personal possession of the courier at all times, unless the provisions of paragraph c, below, apply. Classified material will not be contained in regular checked baggage. Couriers must ensure that "carry-on" containers (for example, packages or briefcases) used for transportation of classified material are within the carrier's allowable size limits for such baggage.**

b. *Procedures for carrying classified information in envelopes.* Persons carrying classified information should process through the airline ticketing and boarding procedure the same as all other passengers except for the following:

(1) The classified information being carried shall contain no metal bindings and shall be contained in sealed envelopes. Should such envelopes be contained in a briefcase or other carry-on luggage, the briefcase or luggage shall be routinely offered for opening for inspection for weapons. The screening officials may check envelopes by X-ray machine, flexing, feel, and weight, without opening the envelopes themselves.

(2) Opening or reading of the classified document by the screening official is not permitted.

c. *Procedures for transporting classified information in packages* Classified information in sealed or packaged containers shall be processed as follows:

(1) The government or contractor official who has authorized the transport of the classified information shall notify the appropriate air carrier in advance.

(2) The passenger carrying the information shall report to the affected airline ticket counter before boarding, present his documentation, and the package or cartons to be exempt from screening. The airline representative will review the documentation and description of the containers to be exempt.

(3) If satisfied with the identification of the passenger and his documentation, the official will provide the passenger with an escort to the screening station and authorize the screening personnel to exempt the container from physical or other type inspection.

(4) If the airline official is not satisfied with the identification of the passenger or the authenticity of his documentation, the passenger will not be permitted to board, and not be subject to further screening for boarding purposes.

(5) The actual loading and unloading of the information will be under the supervision of a representative of the air carrier; however, appropriately cleared personnel shall accompany the material and keep it under surveillance during loading and unloading operations. In addition, appropriately cleared personnel must be available to conduct surveillance at any intermediate stops where the cargo compartment is to be opened.

(6) DoD Components and contractor officials shall establish and maintain appropriate liaison with local FAA officials, airline representatives and airport terminal administrative and security officials. Prior notification is emphasized to ensure that the airline representative can make timely arrangements for courier screening.

d. Documentation

(1) When authorized to carry sealed envelopes or containers containing classified information, both government and contractor personnel shall present an identification card carrying a photograph, descriptive data, and signature of the individual. (If the identification card does not contain date of birth, height, weight, and signature, these items must be included in the written authorization.)

(a) DoD personnel shall present an official identification issued by U.S. Government agency.

(b) Contractor personnel shall present identification issued by the contractor or the U.S. Government. Contractors' identification cards shall carry the name of the employing contractor, or otherwise be marked to denote "contractor."

(c) The courier shall have the original of the authorization letter. A reproduced copy is not acceptable; however, the traveler shall have sufficient authenticated copies to provide a copy to each airline involved. The letter shall be prepared on letterhead stationery of the agency or contractor authorizing the carrying of classified material. In addition, the letter shall:

(1) Give the full name of the individual and his employing agency or company;

(2) Describe the type of identification the individual will present (for example, Naval Research Laboratory Identification Card, No. 1234; ABC Corporation Identification Card No. 1234);

(3) Describe the material being carried (for example, three sealed packages, 9" x 8" x 24", addressee and addressor);

(4) Identify the point of departure, destination, and known transfer points;

(5) Carry a date of issue and an expiration date;

(6) Carry the name, title, and signature of the official issuing the letter. Each package or carton to be exempt shall be signed on its face by the official who signed the letter; and

(7) Carry the name of the government agency designated to confirm the letter of authorization, and its telephone number. The telephone number of the agency designated shall be an official U.S. Government number.

(2) Information relating to the issuance of DoD identification cards is contained in DoD Instruction 1000.13 (reference (ss)). The green, gray, and red DD Forms 2 and other DoD and contractor picture ID card are acceptable to FAA.

(3) The Director, DIS, shall establish standards for the issuance of identification cards when required by contractor employees selected as couriers or whose duties will involve hand-carrying of classified material.

8-303. Authority to approve escort or handcarry of classified information aboard commercial passenger aircraft

a. Within the United States, its Territories, and Canada

(1) DoD Component officials who have been authorized to approve travel orders and designate couriers may approve the escort or hand-carry of classified information within the United States, its Territories, and Canada.

(2) The Director, DIS, may authorize contractor personnel to handcarry classified material in emergency or time-sensitive situations subject to adherence with the procedures and limitations specified in this Section.

b. Outside the United States, its Territories, and Canada The

head of a DoD Component, or single designee at the headquarters or major command level, may authorize the escort or hand-carrying of classified information outside the area encompassed by the boundaries of United States, its Territories, and Canada. **As an exception to policy, the DUSD(P) has authorized DA to extend authority to approve handcarrying of classified information aboard commercial aircraft outside the United States to the DCSI, G-2, or S-2 at the MACOM or Army Staff level, 0-6 and above. Persons acting in the absence of this official may also approve such actions. Authority may not be further delegated. Requests may be considered upon certification by the requestor that:**

(1) The material is not present at the destination;

(2) The material is needed urgently for a specified official purpose; and

(3) There is a specified reason that the material could not be transmitted by other approved means to the destination in sufficient time for the stated purpose.

(4) **Local records are retained which specify:**

(a) **Name, position title, rank or grade, and social security number of the courier.**

(b) **Classification of the material to be handcarried.**

(c) **Nature of the material to be handcarried (document titles or other identifying data, and number of copies).**

(d) **Justification, to include circumstances precluding transmission by other approved means, adverse effect on mission accomplishment if the request is denied, and so forth.**

(e) **Additional justification (separate from subparagraph d, above) if the material is to be handcarried on the return trip.**

(f) **Itinerary: departure and arrival times, dates, and places for all commercial flights traveling outside the United States, its territories, and Canada; names of carriers and flight numbers.**

(g) **Storage arrangements in transit (when required) and at the temporary duty location upon arrival.**

Chapter IX Disposal and Destruction

9-100. Policy

Documentary record information originated or received by a DoD Component in connection with the transaction of public business, and preserved as evidence of the organization, functions, policies, operations, decisions, procedures, or other activities of any U.S. Government department or agency or because of the informational value of the data contained therein, may be disposed of or destroyed only in accordance with DoD Component record management regulations. Nonrecord classified information, and other material of similar temporary nature, shall be destroyed when no longer needed under procedures established by the head of the cognizant DoD Component. These procedures shall incorporate means of verifying the destruction of classified information and material and be consistent with the following requirements.

9-101. Methods of destruction

Classified documents and material shall be destroyed by burning or, with the approval of the cognizant DoD Component head or designee, by melting, chemical decomposition, pulping, pulverizing, cross-cut shredding, or mutilation sufficient to preclude recognition or reconstruction of the classified information. **In all cases, burning is the preferred method of destroying classified information. Small amounts of classified waste should be destroyed in this manner.** (Strip shredders purchased prior to the effective date of this Regulation may continue to be used but only in circumstances where reconstruction of the residue is precluded. Shredding significant amounts of unclassified material together with classified material normally will meet this requirement.) **Standards for destruction equipment used by the U.S. Army are in appendix K. All new and modified equipment will meet these standards. Technical assistance and other guidance may be obtained by**

writing directly to the Chief, Intelligence Materiel Activity, ATTN: AMXIM-PS, Ft.Meade, MD 20755-5313.

9-102. Destruction procedures

a. Procedures shall be instituted that ensure all classified information intended for destruction actually is destroyed. Destruction records and imposition of a two-person rule, that is, having two cleared persons involved in the entire destruction process, will satisfy this requirement for Top Secret information. Imposition of a two-person rule, without destruction records, will satisfy this requirement for Secret information, as will use of destruction records without imposition of the two-person rule. Only one cleared person needs to be involved in the destruction process for Confidential information.

b. When burn bags are used for the collection of classified material that is to be destroyed at central destruction facilities, such bags shall be controlled in a manner designed to minimize the possibility of their unauthorized removal and the unauthorized removal of their classified contents prior to actual destruction. When filled, burn bags shall be sealed in a manner that will facilitate the detection of any tampering with the bag.

c. Procedures to ensure that all classified information intended for destruction actually is destroyed, other than those in paragraphs a. and b., above, shall be submitted to the DoD Component's senior official (subsections 13-301 and 13-302) for approval. **Methods other than those prescribed herein will not be used by Army activities unless approved by HQDA. Requests will be forwarded through channels to HQDA (DAMI-CIS) WASH DC 20310-1051, with full justification and a description of the alternate method of ensuring destruction.**

9-103. Records of destruction

a. Records of destruction are required for Top Secret information. The record shall be dated and signed at the time of destruction by two persons cleared for access to Top Secret information. However, in the case of Top Secret information placed in burn bags for central disposal, the destruction record may be signed by the officials when the information is so placed and the bags are sealed. Top Secret burn bags shall be numbered serially and a record kept of all subsequent handling of the bags until they are destroyed. This record may be in lieu of actual burn bag receipts and shall be maintained for a minimum of 2 years. **Completion of the "custodian" or "Destruction Official" block and the "Witnessing Official" blocks of DA Form 3964 satisfies the two-person witness requirements for Top Secret information. Destruction certificates for Secret material, when only one person is involved in the destruction process, require only one signature.**

b. Records of destruction of Secret and Confidential information are not required except for NATO Secret and some limited categories of specially controlled Secret information. When records of destruction are used for Secret information, only one cleared person has to sign such records. (DoD Directive 5100.55 (reference (z)) provides guidance on the destruction of NATO classified material.) **Unless required by other Army regulations (such as AR 380-40, TB 380-41 (reference (v)), and AR 380-15 (reference (z)) or directives, and only one person is involved in destruction of Secret information, records of destruction are not required for Secret material.**

(1) **The signature of the destruction and witnessing official on the record of destruction indicates one of the following:**

(a) **Actual destruction of the material. (The destruction official must examine the final residue to ensure that the documents are completely destroyed.)**

(b) **The material has been placed in a classified burn bag for later disposal as classified waste by one of the methods authorized in paragraph 9-101, above. Local procedures will include numbering, and protection of classified burn bags equal to the highest level of classified material in the bags until actual destruction takes place.**

(2) **The DA Form 3964 will normally be used as the record of destruction.**

(3) **Forms used for destruction of Top Secret material will be serially numbered in calendar year series. The serial number and date of destruction record will be noted on Top Secret registers to indicate that the material has been destroyed.**

(4) **Accountability records not formatted to contain a destruction certificate may be used as a certificate of destruction if annotated substantially as follows:**

DESTRUCTION CERTIFICATE

(Check appropriate block)

Material described here has been:

Destroyed Placed in a classified burn bag/container
Date _____

Destruction/Certifying Official _____

Witnessing Official _____

(5) **All accountable documents and enclosures to them will be identified on the destruction certificate. The witnessing official, when used, will initial all alterations.**

(6) **If destruction by the custodian is impractical because of the volume of material, or because only limited facilities for destruction are available, the responsible commander will appoint, in writing, a properly cleared destruction official to destroy or to witness the destruction.**

c. Records of destruction shall be maintained for 2 years. (Refer to AR 340-2 (reference (mmm)) or AR 340-18-1.)

9-104. Classified waste

Waste material, such as handwritten notes, carbon paper, typewriter ribbons, and working papers that contains classified information must be protected to prevent unauthorized disclosure of the information. Classified waste shall be destroyed when no longer needed by a method described in subsection 9-101. Destruction records are not required.

9-105. Classified document retention

a. Classified documents that are not permanently valuable records of the government shall not be retained more than 5 years from the date of origin, unless such retention is authorized by and in accordance with DoD Component record disposition schedules.

b. Throughout the Department of Defense, the head of each activity shall establish at least one clean-out day each year where a portion of the work performed in every office with classified information stored is devoted to the destruction of unneeded classified holdings. **MACOMs and Staff Headquarters elements will report the date(s) during which activitywide annual cleanouts were conducted to HQDA (DAMI-CIS) WASH DC 20310-1051 by the end of each fiscal year. The annual cleanout certification may be forwarded along with the annual SF 311, Information Security Program Data Report (see paragraph 13-400).**

Chapter X Security Education

10-100. Responsibility and objectives

Heads of DoD Components shall establish security education programs for their personnel. Such programs shall stress the objectives of improving the protection of information that requires it. They shall also place emphasis on the balance between the need to release the maximum information appropriate under the Freedom of Information Act (DoD Directive 5400.7, reference (k)) and the interest of the Government in protecting the national security.

10-101. Scope and principles

The security education program shall include all personnel authorized or expected to be authorized access to classified information. Each DoD Component shall design its program to fit the requirements of different groups of personnel. Care must be exercised to

assure that the program does not evolve into a perfunctory compliance with formal requirements without achieving the real goals of the program. The program shall, as a minimum, be designed to:

a. Advise personnel of the adverse effects to the national security that could result from unauthorized disclosure and of their personal, moral, and legal responsibility to protect classified information within their knowledge, possession, or control;

b. Indoctrinate personnel in the principles, criteria, and procedures for the classification, downgrading, declassification, marking, control and accountability, storage, destruction, and transmission of classified information and material, as prescribed in this Regulation, and alert them to the strict prohibitions against improper use and abuse of the classification system;

c. Familiarize personnel with procedures for challenging classification decisions believed to be improper;

d. Familiarize personnel with the security requirements of their particular assignment;

e. Inform personnel of the techniques employed by foreign intelligence activities in attempting to obtain classified information, and their responsibility to report such attempts;

f. Advise personnel of the penalties for engaging in espionage activities;

g. Advise personnel of the strict prohibition against discussing classified information over an unsecure telephone or in any other manner that permits interception by unauthorized persons;

h. Inform personnel of the penalties for violation or disregard of the provisions of this Regulation (see paragraph 14-101 b.);

i. Instruct personnel that individuals having knowledge, possession, or control of classified information must determine, before disseminating such information, that the prospective recipient has been cleared for access by competent authority; needs the information in order to perform his or her official duties; and can properly protect (or store) the information.

j. Advise personnel of the requirements to report such matters as:

- (1) Deficiencies in physical security.
 - (2) Possible loss or compromise of classified material.
 - (3) Information that could reflect adversely on the trustworthiness of an individual who has access to classified information.
- k. Inform personnel of the proper methods and channels for reporting matters of security interest.

l. For persons who will have access to classified intelligence information, explain in general terms the intelligence mission of the US. Army and the reasons why intelligence information is sensitive.

m. Inform personnel of—

- (1) The objectives of the Operations Security (OPSEC) Program.(Refer to AR 530-1 (reference (eee))).
- (2) The need for and means of applying OPSEC principles in their particular situations.

10-102. Initial briefings

DoD personnel granted a security clearance (see subsection 7-100) shall not be permitted to have access to classified information until they have received an initial security briefing and have signed Standard Form 189, "classified Information Nondisclosure Agreement." DoD 5200.1-PH-I (reference (xx)) provides a sample briefing and additional information regarding Standard Form 189. Cleared personnel employed prior to the effective date of this Regulation must sign Standard Form 189 as soon as practicable but not later than 28 February 1990. **Security managers will refer to the Army Implementing Instructions for the Classified Information Nondisclosure Agreement, SF 189, contained in DA Circular 380-85-1. Military and civilian personnel will be given a security indoctrination prior to being granted access to classified information, upon transfer of or within a duty station (i.e., upon job change). Use of the SF 189 minimum briefing contained in the circular alone, does not satisfy this requirement. The indoctrination must specifically address the security aspects of the new assignment and take into account the experience level of the**

personnel to determine their knowledge of the requirements for safeguarding classified information (see AR 604-5 (reference (II))).

10-103. Refresher briefings

Programs shall be established to provide, at a minimum, annual security training for personnel having continued access to classified information. The elements outlined in subsection 10-101 shall be tailored to fit the needs of experienced personnel. **Annual attendance of personnel at a security education presentation will not, in itself, be considered fulfillment of the requirements of this chapter. Programs must provide effective education of activity personnel in the subjects listed in paragraph 10-101, tailored to suit the nature of their particular involvement with the Information Security Program.**

10-104. Foreign travel briefings

a. Personnel who have had access to classified information shall be given a foreign travel briefing, before travel, to alert them to their possible exploitation under the following conditions:

- (1) Travel to or through communist-controlled countries; and
- (2) Attendance at international scientific, technical, engineering or other professional meetings in the United States or in any country outside the United States where it can be anticipated that representatives of Communist-controlled countries will participate or be in attendance. (See also DoD Directive 5240.6(reference (bb)).

b. Individuals who travel frequently, or attend or host meetings of foreign visitors as described in a.2., above, need not be briefed for each occasion, but shall be provided a thorough briefing at least once every 6 months and a general reminder of security responsibilities before each such activity.

10-105. Termination briefings

a. Upon termination of employment, administrative withdrawal of security clearance, or contemplated absence from duty or employment for 60 days or more, DoD military personnel and civilian employees shall be given a termination briefing, return all classified material, and execute a Security Termination Statement. **DA Form 2962 (Security Termination Statement and Debriefing Certificate) will be used. Except as provided in subparagraph e, below, DA Form 2962 is required only in the above situations and when personnel have had their security clearances revoked under AR 604-5 (reference (II)). An oral debriefing will be accomplished before the DA Form 2962 is completed. If they have not already done so, personnel departing the activity who have had access to classified information will be asked to execute the SF 189, Classified Information Nondisclosure Agreement. The executed SF 189s for departing personnel will be processed as described in DA Circular 380-85-1. This statement shall include:**

- (1) An acknowledgment that the individual has read the appropriate provisions of the Espionage Act (reference (tt)), other criminal statutes, DoD regulations applicable to the safeguarding of classified information to which the individual has had access, and understands the implications thereof;
- (2) A declaration that the individual no longer has any documents or material containing classified information in his or her possession;
- (3) An acknowledgement that the individual will not communicate or transmit classified information to any unauthorized person or agency; and
- (4) An acknowledgement that the individual will report without delay to the FBI or the DoD Component concerned any attempt by any unauthorized person to solicit classified information.

b. When an individual refuses to execute a Security Termination Statement, that fact shall be reported immediately to the security manager of the cognizant organization concerned. In any such case, the individual involved shall be debriefed orally. The fact of a refusal to sign a Security Termination Statement shall be reported to the Director, Defense Investigative Service who shall assure that it is recorded in the Defense Central Index of Investigations.

(1) Upon an individual's refusal to execute a termination statement, the security manager will:

- (a) Provide an oral termination briefing.
- (b) Annotate the fact that an oral termination briefing was given, and the date, on the DA Form 2962.
- (c) Note on the form the circumstances and reasons (if given) for the individual's refusal to execute the DA 2962.
- (d) Advise the person that refusal to complete the termination statement could adversely affect his/her gaining future security clearance.
- (e) Send a copy of the DA Form 2962 to the Director, Defense Investigative Service, Personnel Investigations Center, P.O. Box 1211, Baltimore, MD 21203-1211.

(2) Should an individual who has had access to classified information refuse to execute the SF 189 when outprocessing an Army activity, the security manager will advise the gaining activity security manager of this fact, and complete the outprocessing of the individual. (Upon receipt of notification, the gaining security manager has the option of considering the date the individual refused to execute the SF 189 form during outprocessing as the beginning of the 30-day "cooling off" period; or the security manager may commence the 30-day period if the person continues to refuse when inprocessing the new activity.)

(3) Individuals retiring or resigning who refuse to execute the SF 189 prior to leaving the facility cannot be compelled to do so. In such cases, the security manager will note the refusal and the date of the refusal on the DA Form 2962, and forward a copy of the DA Form 2962 to the Director, Defense Investigative Service for notation in the Defense Central Index of Investigations. The refusal to execute the SF 189 should be noted on the DA Form 2962 even if the individual signs the termination statement.

c. The security termination statement shall be retained by the DoD Component that authorized the individual access to classified information for the period specified in the Component's record retention schedules, but for a minimum of 2 years after the individual is given a termination briefing.

d. The termination briefing will include, if appropriate, a reminder of the risks associated with certain foreign travel and hazardous activities.

e. DA Form 2543 (Briefing/Rebriefing/ Debriefing Certificate) normally will be used to show and acknowledge receipt of NATO security briefings. (See AR 380-15 (reference (z)). A record of debriefing may be shown on the DA Form 2962.

f. For information regarding termination briefings of general officers and senior civilian officials (GS-16 and above), see AR 604-5 (reference (ll)).

10-106. Other requirements

a. Requiring individuals to read and certify by signature their understanding of security regulations, does not satisfy any of the training requirements of this chapter. This practice may be included as a part of security education programs, but it will not be used as a substitute for other methods of training.

b. Special briefings are required in addition to those listed above:

(1) When an individual is authorized to handcarry or escort classified material, whether locally, within, or outside the United States.

(2) When an employee is granted access to sensitive compartmented information (SCI) and/or special access program (SAP) information.

(3) When an official is approved as an Original Classification Authority (OCA).

(4) To ensure that supervisors are familiar with their responsibilities in matters pertaining to personnel security (see AR 604-5).

Chapter XI Foreign Government Information

Section 1 Classification

11-100. Classification

a. Foreign government information classified by a foreign government or international organization of governments shall retain its original classification designation or be assigned a U.S. classification designation that will ensure a degree of protection equivalent to that required by the government or organization that furnished the information. Original classification authority is not required for this purpose.

b. Foreign government information that was not classified by a foreign entity but was provided with the expectation, expressed or implied, that the information, the source of the information, or both, are to be held in confidence must be classified by an original classification authority. The two-step procedure for classification prescribed in subsection 2-202 does not apply to the classification of such foreign government information because E. O. 12356 (reference (b)) states a presumption of damage to the national security in the event of unauthorized disclosure of such information. Therefore, foreign government information shall be classified at least Confidential, but higher whenever the damage criteria of subsections 1-501 or 1-502 are determined to be met.

11-101. Duration of classification

a. Foreign government information shall not be assigned a date or event for automatic declassification unless specified or agreed to by the foreign entity.

b. Foreign government information classified by the Department of Defense under this or previous Regulations shall be protected for an indefinite period (see subsection 11-304).

Section 2 Declassification

11-200. Policy

In considering the possibility of declassification of foreign government information, officials shall respect the intent of this Regulation to protect foreign government information and confidential foreign sources.

11-201. Systematic review

When documents containing foreign government information are encountered during the systematic review process they shall be referred to the originating agency for a declassification determination. Consultation with the foreign originator through appropriate channels may be necessary before final action can be taken.

11-202. Mandatory review

Requests for mandatory review for declassification of foreign government information shall be processed and acted upon in accordance with the provisions of section 3 of Chapter III, except that foreign government information will be declassified only in accordance with the guidelines developed for such purpose and after necessary consultation with other DoD Components or government agencies with subject matter interest. When these guidelines cannot be applied to the foreign government information requested, or in the absence of such guidelines, consultation with the foreign originator through appropriate channels normally should be effected prior to final action taken on the request. When the responsible DoD Component is knowledgeable of the foreign originator's view toward declassification or continued classification of the types of information requested, consultation with the foreign originator may not be necessary.

Section 3 Marking

11-300. Equivalent U.S. classification designations

Except for the foreign security classification designation RESTRICTED, foreign classification designations, including those of international organizations of governments, that is, NATO, generally parallel U.S. classification designations. A table of equivalents is contained in Appendix A.

11-301. Marking NATO documents

Classified documents originated by NATO, if not already marked with the appropriate classification in English, shall be so marked. Markings required under subsection 4-402 shall not be placed on documents originated by NATO. Documents originated by NATO that are marked RESTRICTED shall be marked with the following additional notation: "To be safeguarded in accordance with USSAN Instruction 1-69" (see DoD Directive 5100.55 (reference(z))).

11-302. Marking other foreign government documents

a. If the security classification designation of foreign government documents is shown in English, no other classification marking shall be applied. If the foreign classification designation is not shown in English, the equivalent overall U.S. classification designation (see Appendix A) shall be marked conspicuously on the document. When foreign government documents are marked with a classification designation having no U.S. equivalent, as in the last column of Appendix A, such documents shall be marked in accordance with paragraph b., below.

b. Certain foreign governments use a fourth classification designation as shown in the last column of Appendix A. Such designations equate to the foreign classification RESTRICTED. If foreign government documents are marked with any of the classification designations listed in the last column of Appendix A, no other classification marking shall be applied. In all such cases, the notation, "This classified material is to be safeguarded in accordance with DoD 5200.1-R or DoD 5220.22-M," shall be shown on the face of the document.

c. Other marking requirements prescribed by this Regulation for U.S. classified documents are not applicable to documents of foreign governments or international organizations of governments.

11-303. Marking of DoD classification determinations

Foreign documents containing foreign government information not classified by the foreign government but provided to the Department of Defense in confidence shall be classified as prescribed in paragraph 11-100 b. and marked with the appropriate U.S. classification.

11-304. Marking of foreign government information in DoD documents

a. Except where such markings would reveal that information is foreign government information when that fact must be concealed, or reveal a confidential source or relationship not otherwise evident in the document or information, foreign government information incorporated in DoD documents shall be identified in a manner that ensures that such information is not declassified prematurely or made accessible to nationals of a third country without consent of the originator. This requirement may be satisfied by marking the face of the document "FOREIGN GOVERNMENT INFORMATION," or with another marking that otherwise indicates that the information is foreign government information, and by including the appropriate identification in the portion or paragraph classification markings, for example, (NS) or (U.K.-C). All other markings prescribed by subsection 4-103 are applicable to the documents. In addition, DoD classified documents that contain extracts of NATO classified information shall bear a marking substantially as follows on the cover or first page: "THIS DOCUMENT CONTAINS NATO CLASSIFIED INFORMATION."

b. When foreign RESTRICTED or NATO RESTRICTED information is included in an otherwise unclassified DoD document, the DoD document shall be marked CONFIDENTIAL. All requirements

of subsection 4-103 apply to such documents. Portion markings on such a document include, for example "(U)," "(NR)," and "(FRG-R)." In addition, the appropriate caveat from paragraph a., above, shall be included on the face of the document.

c. The "Classified by" line of DoD documents containing only foreign government information normally shall be completed with the identity of the foreign government or international organization involved, for example, "Classified by Government of Australia" or "classified by NATO," provided that other requirements of subsection 4-104 do not pertain to such documents.

d. The "Declassify on" line of DoD documents containing foreign government information normally shall be completed with the notation "Originating Agency's Determination Required" or "OADR" (see subsections 4-600 and 11-101).

Section 4 Protective Measures

11-400. NATO classified information

NATO classified information shall be safeguarded in accordance with the provisions of DoD Directive 5100.55 (reference(z)).

11-401. Other foreign government information

a. Classified foreign government information other than NATO information shall be protected as is prescribed by this Regulation for U.S. classified information of a comparable classification.

b. Foreign government information, unless it is NATO information, that is marked under paragraphs 11-302 b. or 11-304 b. shall be protected as U.S. CONFIDENTIAL, except that such information may be stored in locked filing cabinets, desks, or other similar closed spaces that will prevent access by unauthorized persons. **Foreign Restricted information will be transmitted and destroyed under procedures governing Confidential information.**

Chapter XII Special Access Programs

12-100. Policy

It is the policy of the Department of Defense to use the security classification categories and the applicable sections of E.O. 12356 (reference (b)) and its implementing ISOO Directive (reference (c)), to limit access to classified information on a "need-to-know" basis to personnel who have been determined to be trustworthy. It is further policy to apply the "need-to-know" principle in the regular system so that there will be no need to resort to formal Special Access Programs. In this context, Special Access Programs may be created or continued only on a specific showing that:

a. Normal management and safeguarding procedures are not sufficient to limit "need-to-know" or access; and

b. The number of persons who will need access will be reasonably small and commensurate with the objective of providing extra protection for the information involved. **No person will receive access to a Special Access Program simply because of rank, title, or position.**

(1) **Favorable consideration for access will be based on a need-to know determination that access clearly benefits the Special Access Program activity.**

(2) **Army employees officially charged with ensuring legal, fiscal, investigate, or operational oversight of Special Access Programs will be deemed to have a need to know sufficient for access to those programs for which they are responsible.**

12-101. Establishment of Special Access Programs

Army programs meeting the criteria above will be submitted to the Chief, Technology Management Office (TMO), HQDA (DACS-DMP), WASH DC 20310-0200, for approval as Special Access Programs by the Secretary of the Army. Army Special Access Programs are governed by the provisions of AR 380-381, DA Pamphlet 380-381 (reference (aaaa)), and this regulation. All

Army activities involved in Special Access Programs will follow the guidance contained in these publications for managing such programs.

a. Procedures for the establishment of Special Access Programs involving NATO classified information are based on international treaty requirements (see DoD Directive 5100.55 (reference (z))).

b. The policies and procedures for access to and dissemination of Restricted Data and Critical Nuclear Weapon Design Information are contained in DoD Directive 5210.2 (reference (y)).

c. Special Access Programs for foreign intelligence information under the cognizance of the Director of Central Intelligence, or those of the National Telecommunications and Information Systems Security Committee originate outside the Department of Defense. **Within Army, such programs are the responsibility of the DCSINT.** However, coordination with the DUSD(P) and the Component's central point of contact is necessary before the establishment or implementation of any such Programs by any DoD Component. The information required by paragraph 12-105a. will be **coordinated, and provided for reporting purposes to the Chief, TMO by the Office of the DCSINT.**

d. Excluding those Programs specified in paragraphs a., b., and c., above, Special Access Programs shall be established within the Military Departments by:

(1) Submitting to the Secretary of the Department of the Army, **through the Chief, TMO, HQDA (DACS-DMP), WASH DC 20310-0200**, the information required under paragraph 12-105 a.;

(2) Obtaining written approval from the Secretary of the Department;

(3) Providing to the DUSD(P) a copy of the approval; and

(4) Maintaining the information and rationale upon which approval was granted within the Military Department's central office. **(The Chief, TMO will maintain necessary records of approved Army Special Access Programs. Approval records for each active Special Access Program will be available for review by appropriate officials during the life of the program and for at least 1 year thereafter.)**

e. Special Access Programs, other than those specified in paragraphs a., b., and c., above, that are desired to be established in any DoD Component other than the Military Departments shall be submitted with the information referred to in paragraph 12-105 a. to the DUSD(P) for approval.

12-102. Review of Special Access Programs

a. Excluding those Programs specified in paragraphs 12-101 a., b., or c., each Special Access Program shall be reviewed annually by the DoD Component responsible for establishment of the Program. **The Chief, TMO will ensure that Army Special Access Programs are reviewed and revalidated annually.** To accommodate such reviews, DoD Components shall institute procedures to ensure the conduct of annual security inspections and regularly scheduled audits by security, contract administration, and audit organizations. **In addition, the Chief, TMO will establish special management procedures to ensure:**

(1) **Security for soliciting, awarding, and administering contracts and purchase requests.**

(2) **Compliance with applicable provisions of laws and regulations.**

(3) **Financial accountability and effective oversight on security vulnerabilities, including a method for Special Access Program personnel to report irregularities.**

(4) **Involvement of authorities (such as cognizant security officials, contracting officers, and procurement officials) in the decisionmaking process for establishment of Special Access Program procedures.**

(5) **Compliance with the applicable requirements of AR 380-35 (DoD C-5105.21-M-1, DoD TS-5105.22-M-2, and DoD TS-5205.21-M-3) (references (ccc), (bbb), and (ddd)) for all Special Access Programs that use, handle, store, or develop SCI.**

(6) **Coordination with the DCSINT, as the Senior Official of the Intelligence Community for the Army, on all Special Access**

Programs involving SCI materiel or requiring participation by the intelligence community.

b. Special Access Programs, excluding those specified in paragraphs 12-101 a., b., or c., or those required by treaty or international agreement, shall terminate automatically every 5 years unless reestablished in accordance with the procedures contained in subsection 12-101.

12-103. Control and administration

a. Each DoD Component shall appoint an official to act as a single point of contact for information concerning the establishment and security administration of all Special Access Programs established by or existing in the Component. **The Chief, TMO is the single point of contact for the establishment and administration of Army Special Access Programs.** Such official shall report to the DUSD(P):

(1) The establishment of a Special Access Program as required by paragraph 12-101 d.3.; and

(2) Changes in Program status as required by paragraphs 12-105 b. or c.

b. Officials serving as single points of contact, as well as members of their respective staffs and other persons providing support to Special Access Programs who require access to multiple sets of particularly sensitive information, shall be subject to a counterintelligence-scope polygraph examination periodically but not less than once every 5 years. Additionally, such testing will be subject to the limitations imposed by Congress. **The DCSINT is the proponent for the Army counter-intelligence scope polygraph program for SAPs.** The program for each DoD Component, as well as requests for waiver, shall be submitted for approval by the DUSD(P). **Army requests will be forwarded to HQDA (DAMI-CIS) WASH DC 20310-1051 for coordination with the Chief, TMO, and submission to the DUSD(P).**

12-104. Codewords and nicknames

Excluding those Programs specified in paragraphs 12-101 a., b., and c., each Special Access Program will be assigned a codeword, a nickname, or both. Codewords and nicknames for Special Access Programs shall be allocated solely by the DUSD(P) through the official appointed under subsection 12-103 **(the Army official for allocation of Special Access Program codewords and nicknames is the Chief, TMO).** DoD Components may request codewords and nicknames individually or in block. If codewords or nicknames are obtained in block, however, the issuing Component shall promptly notify the DUSD(P) upon activation and assignment.

12-105. Reporting of Special Access Programs

a. *Report of establishment.* Reports to the Secretary of the Military Department or the DUSD(P) required under subsection 12-101 for Special Access Programs shall include:

(1) The responsible department, agency, or DoD Component, including office identification;

(2) The codeword and/or nickname of the Program;

(3) The relationship, if any, to other Special Access Programs in the Department of Defense or other government agencies;

(4) The rationale for establishing the Special Access Program including the reason why normal management and safeguarding procedures for classified information are inadequate;

(5) The estimated number of persons granted special access in the responsible DoD Component; other DoD Components; other government agencies; contractors; and the total of such personnel;

(6) A summary statement pertaining to the Program security requirements with particular emphasis upon those personnel security requirements governing access to Program information;

(7) The date of Program establishment;

(8) The estimated number and approximate dollar value, if known, of carve-out contracts that will be or are required to support the Program; and

(9) The DoD Component official who is the point of contact (last name, first name, middle initial; position or title; mailing address; and telephone number).

b. Annual Reports. Annual reports to the DUSD(P) shall be submitted **by the Chief, TMO** not later than 31 January of each year, showing the changes in information provided under paragraph a., above, as well as the date of last review. Annual reports shall reflect *actual* rather than *estimated* numbers of carve-out contracts and persons granted access and shall summarize the results of the inspections and audits required by paragraph 12-102 a. The effective date of information in the annual report shall be 31 December.

c. Termination Reports. The DUSD(P) shall be notified immediately **by the Chief, TMO**, upon termination of a Special Access Program.

12-106. Accounting for Special Access Programs

The DUSD(P) shall maintain a listing of approved Special Access Programs. **Within Army, the Chief, TMO will coordinate approvals for, and maintain a list of, approved Special Access Programs.**

12-107. Limitations on access

Access to data reported under this Chapter shall be limited to the DUSD(P) and the minimum number of properly indoctrinated staff necessary to perform the functions assigned the DUSD(P) herein. Access may not be granted to any other person for any purpose without the approval of the DoD Components sponsoring the Special Access Programs concerned.

12-108. "Carve-out" contracts

a. The Secretaries of the Military Departments and the DUSD(P), or their designees, shall ensure that, in those Special Access Programs involving contractors, special access controls are made applicable by legally binding instruments. **The DD Form 254 (Contract Security Classification Specification), classified if necessary, will be used for this purpose. The Chief, TMO, will ensure that:**

(1) A DD Form 254 is issued for each Special Access Program involving a contractor; each DD Form 254 identifies the specific areas or locations within a contractor's plant that define the extent of the carve-out.

(2) A DD Form 254 is provided to the cognizant Defense Investigative Service (DIS) security office, and if applicable, to the Director, Defense Audit Agency.

(3) Other appropriate notification is conveyed to the Director, Defense Investigative Service, and to the Director, Defense Audit Agency, in those rare instances when an unusual sensitivity surrounds the Special Access Program.

b. To the extent necessary for DIS to execute its security responsibilities with respect to Special Access Programs under its security cognizance, DIS personnel shall have access to all information relating to the administration of these Programs.

c. Excluding those Programs specified in paragraph 12-101 c., the use of "carve-out" contracts that relieve the DIS from inspection responsibility under the Defense Industrial Security Program is prohibited unless:

(1) Such contract supports a Special Access Program approved and administered under subsection 12-101;

(2) Mere knowledge of the existence of a contract or of its affiliation with the Special Access Program is classified information **(the fact that a classified contract is part of an approved Special Access Program is not sufficient justification for carve-out status);** and

(3) Carve-out status is approved for each contract by the Secretary of a Military Department, the Director, NSA, the DUSD(P), or their designees. **A determination on carve-out status will be based upon a case-by-case assessment coordinated by the Chief, TMO as follows:**

(a) Contract security administration by the Defense Investigative Service would pose an unacceptable risk to the security of the program.

(b) Contract security may be administered effectively and completely by the Army under DoD standards.

d. Approval to establish a "carve-out" contract must be requested

from the Secretary of a Military Department, or designee(s), the Director, NSA, or designee(s) or in the case of other DoD Components, from the DUSD(P). **Army activities will submit fully justified requests through the Chief, TMO, HQDA (DACS-DMP) WASH DC 20310-0200 for consideration.** Approved "carve-out" contracts shall be assured the support necessary for the requisite protection of the classified information involved. The support shall be specified through a system of controls that shall provide for:

(1) A written security plan;

(2) Professional security personnel at the sponsoring DoD Component performing security inspections at each contractor's facility which shall be conducted, at a minimum, with the frequency prescribed by paragraph 4-103 of DoD 5220.22-R (reference (e));

(3) "Carve-out" contracting procedures;

(4) A central office of record; and

(5) An official to be the single point of contact for security control and administration. DoD Components other than the Military Departments and NSA shall submit such appropriate rationale and security plan along with requests for approval to the DUSD(P).

e. An annual inventory of carve-out contracts shall be conducted by each DoD Component which participates in Special Access Programs. **HQDA (DACS-DMP) will conduct the annual carve-out inventory and submit reports to DUSD(P), as necessary.**

f. This subsection relates back to the date of execution for each contract to which carve-out contracting techniques are applied. The carve-out status of any contract expires upon termination of the Special Access Program which it supports.

12-109. Oversight reviews

a. The DUSD(P) shall conduct oversight reviews, as required, to determine compliance with this Chapter. **The Chief, TMO will coordinate the annual DUSD(P) reviews of Army Special Access Programs.**

b. Pursuant to statutory authority, the Inspector General, Department of Defense, shall conduct oversight of Special Access Programs.

Chapter XIII Program Management

Section 1

Executive Branch Oversight and Policy Direction

13-100. National Security Council

Pursuant to the provisions of E.O. 12356 (reference (b)), the NSC shall provide over-all policy direction for the Information Security Program.

13-101. Administrator of General Services

The Administrator of General Services is responsible for implementing and monitoring the Information Security Program established under reference (b). In accordance with reference (b), the Administrator delegates the implementation and monitorship functions of the Program to the Director of the ISOO.

13-102. Information Security Oversight Office

a. Composition. The ISOO has a full-time director appointed by the Administrator of General Services with approval of the President. The Director has the authority to appoint a staff for the office.

b. Functions. The Director of the ISOO is charged with the following principal functions that pertain to the Department of Defense.

(1) Oversee DoD actions to ensure compliance with reference (b) and implementing directives, for example, the ISOO Directive No. 1 (reference (c)) and this Regulation;

(2) Consider and take action on complaints and suggestions from persons within or outside the government with respect to the administration of the Information Security Program;

(3) Report annually to the President through the NSC on the implementation of reference (b);

(4) Review this Regulation and DoD guidelines for systematic declassification review; and

(5) Conduct on-site reviews of the Information Security Program of each DoD Component that generates or handles classified information.

c. Information requests. The Director of the ISOO is authorized to request information or material concerning the Department of Defense, as needed by the ISOO in carrying out its functions.

d. Coordination. Heads of DoD Components shall ensure that any significant requirements levied directly on the Component by the ISOO are brought to the attention of the Director of Security Plans and Programs, ODUSD(P). **Notification of any direct taskings will be forwarded through command channels to HQDA (DAMI-CIS) WASH DC 20310-1051. DAMI-CIS will provide notification to ODUSD(P).**

Section 2 Department of Defense

13-200. Management responsibility

a. The DUSD(P) is the senior DoD official having DoD-wide authority and responsibility to ensure effective and uniform compliance with and implementation of E.O. 12356 and its implementing ISOO Directive No. 1 (references (b) and (c)). As such, the DUSD(P) shall have primary responsibility for providing guidance, oversight and approval of policy and procedures governing the DoD Information Security Program. The DUSD(P) or his designee may approve waivers or exceptions to the provisions of this Regulation to the extent such action is consistent with references (b) and (c).

b. The heads of DoD Components may approve waivers to the provisions of this Regulation only as specifically provided for herein. **Requests for waivers or exceptions will be forwarded through command channels to HQDA (DAMI-CIS) WASH DC 20310-1051.**

c. The Director, NSA/Chief, Central Security Service, under DoD Directive 5200.1 (reference (a)), is authorized to impose special requirements with respect to the marking, reproduction, distribution, accounting, and protection of and access to classified cryptologic information. In this regard, the Director, NSA, may approve waivers or exceptions to these special requirements. Except as provided in subsection 1-205, the authority to lower any COMSEC security standards rests with the Secretary of Defense. Requests for approval of such waivers or exceptions to established COMSEC security standards which, if adopted, will have the effect of lowering such standards, shall be submitted to the DUSD(P) for approval by the Secretary of Defense. **Requests for waivers or exceptions will be submitted through command channels to HQDA(DAMI-CIS) WASH DC 20310-1051.**

Section 3 DoD Components

13-300. General

The head of each DoD Component shall establish and maintain an Information Security Program designed to ensure compliance with the provisions of this Regulation throughout the Component.

13-301. Military departments

In accordance with DoD Directive 5200.1 (reference(a)), the Secretary of each Military Department shall designate a senior official who shall be responsible for complying with the implementing this Regulation with the Department. **The Chief of Staff, U.S. Army, under the direction of the Secretary of the Army, exercises control over Army policies relating to the DoD Information Security Program. The DCSINT has general staff responsibility for the implementation of, and compliance with, the program**

throughout the Army, and is the "senior official" designated under this subsection.

13-302. Other components

In accordance with DoD Directive 5200.1 (reference(a)), the head of each other DoD Component shall designate a senior official who shall be responsible for complying with and implementing this Regulation within their respective Component.

13-303. Program monitorship

The senior officials designated under subsections 13-301 and 13-302 are responsible within their respective jurisdictions for monitoring, inspecting with or without prior announcement, and reporting on the status of administration of the DoD Information Security Program at all levels of activity under their cognizance. **Information security officials from HQDA (DAMI-CIS) will conduct periodic visits to each MACOM and to selected installations, activities, and agencies to monitor and inspect the administration of the Army Information Security Program. The DCSINT will ensure funding for this purpose.**

13-304. Field program management

a. Throughout the Department of Defense, the head of each activity shall appoint, in writing, an official to serve as security manager for the activity. This official shall be responsible for the administration of an effective Information Security Program in that activity with particular emphasis on security education and training, assignment of proper classifications, downgrading and declassification, safeguarding, and monitorship, to include sampling classified documents for the purpose of assuring compliance with this Regulation.

(1) **In addition to the specific areas listed below, Army commanders are responsible for the maintenance of an effective security posture within their activities. Each Army commander and agency head will:**

(a) **Designate in writing a properly cleared, professional commissioned officer (0-3), warrant officer, or DA civilian in the 080 series, whose job is already classified at grade GS-12 or above, as security manager for the MACOM or ARSTAF activity. (Commanders of subordinate MACOM/ARSTAF elements may appoint security managers at lesser grade/rank than that specified above.)**

(b) **Establish local information security policies and procedures which comply with this regulation.**

(c) **Initiate and supervise measures or instructions necessary to ensure continual control of classified material.**

(d) **Ensure that persons who require access to classified information are properly cleared and have a need to know.**

(e) **Continually assess the individual trustworthiness of personnel who possess a security clearance.**

(f) **Ensure adequate funding and manpower to allow security personnel to manage applicable information security program requirements.**

(g) **Prioritize security management assets to ensure that information security program requirements are met.**

(h) **Ensure integration of the information security program with mission requirements of the activity.**

(2) **A commander may delegate authority to perform local security functions, but not the responsibility to do so. Security, including proper classification and timely declassification, is a responsibility of the commander. Therefore, it is incumbent upon local commanders to ensure that individuals delegated security responsibilities possess the personal maturity, good judgment, and professional caliber to maintain a good security posture within the activity.**

b. Activity heads shall ensure that officials appointed as security managers either possess, or obtain within a reasonable time after appointment, knowledge of and training in the Information Security Program commensurate with the needs of their positions. The Director of Security Plans and Programs, ODUSD(P) shall, with the

assistance of the Director, Defense Security Institute, develop minimum standards for training of activity security managers. Such training should result in appropriate certifications to be recorded in the personnel files of the individuals involved. HQDA (DAMI-CIS) will coordinate minimum training requirements for Army security manager certification with ODUSD(P) and the Defense Security Institute.

c. Activity heads shall ensure that officials appointed as security managers are authorized direct and ready access to the appointing official on matters concerning the Information Security Program. They also shall provide sufficient resources of time, staff, and funds to permit accomplishment of the security manager's responsibilities, to include meaningful oversight of the Information Security Program at all levels of the activity.

(1) **Designated Army security managers will:**

(a) **Advise and represent the commander on matters related to the classification, downgrading, declassification, and safeguarding of national security information.**

(b) **Establish, implement, and maintain an effective security education program. (Security managers who delegate this responsibility in whole or in part to subordinate security personnel, staff element security points of contact, etc., remain responsible for overseeing activity compliance with Chapter X of this regulation.)**

(c) **Establish procedures for ensuring that all persons handling classified material are properly cleared and have a need to know. The clearance status of each individual must be recorded and accessible for verification.**

(d) **Advise and assist officials on classification problems and the development of classification guidance.**

(e) **Ensure that classification guides for classified plans, programs, and projects are created early and reviewed and updated when required.**

(f) **Conduct periodic reviews of classifications assigned within the activity to ensure that such decisions are proper.**

(g) **Ensure the review and continual reduction of classified information within the activity by declassification, destruction, or retirement. Oversee activity annual cleanout days.**

(h) **Oversee the conduct of announced and unannounced security inspections for compliance with this regulation and other security directives. Notify the commander of the results of such inspections.**

(i) **Assist and advise the commander in matters pertaining to the enforcement of regulations on the dissemination, reproduction, transmission, protection, and destruction of classified material.**

(j) **Make recommendations regarding requests for visits by foreign nationals.**

(k) **Ensure the protection of classified information presented during meetings, symposiums, and/or conferences sponsored by the activity.**

1. **Act as single point of contact for coordinating, challenging, and resolving classification and declassification problems.**

2. **Requests to waive the minimum rank/grade requirements for designation as a HQDA agency or MACOM security manager (See paragraph a, above) will be forwarded HQDA (DAMI-CIS) WASH DC 20310-1051.**

Section 4 Information Requirements

13-400. Information requirements

DoD Components shall submit on a fiscal year basis a consolidated report concerning the Information Security Program of the Component on SF 311, "Agency Information Security Program Data," to reach the ODUSD(P) by October 20 of each year. SF 311 shall be completed in accordance with the instructions thereon and augmenting instructions issued by the ODUSD(P). The ODUSD(P) shall submit the DoD report (SF 311) to the ISOO by October 31 of each year. Interagency Report Control Number 0230-GSA-AN applies to

this information collection system as well as to that contained in subsection 1-602. **MACOM and HQDA agency security managers will submit a consolidated report on SF 311 to reach HQDA (DAMI-CIS) WASH DC 20310-1051 by 11 October each year. Information reported will be as of 30 September. USAR units are exempt from this requirement. DAMI-CIS will submit a consolidated report to ODUSD(P).**

Section 5 Defense Information Security Committee

13-500. Purpose

The Defense Information Security Committee (DISC) is established to advise and assist the DUSD(P) and the Director, Security Plans and Programs, ODUSD(P) in the formulation of DoD Information Security Program policy and procedures.

13-501. Direction and membership

The DISC shall meet at the call of the DUSD(P) or the Director, Security Plans and Programs. It is comprised of the DUSD(P) as Chairman; the Director, Security Plans and Programs, as Vice Chairman; and the senior officials (designated in accordance with section E.3.a., DoD Directive 5200.1, reference (a)) (or their representatives) responsible for directing and administering the Information Security Program of the OJCS, the Departments of the Army, Navy, and Air Force, the Defense Intelligence Agency, the Defense Nuclear Agency, the National Security Agency, and the Defense Investigative Service. Other DoD Components may be invited to attend meetings of particular interest to them. **The DCSINT is designated as Army representative for the Defense Information Security Committee. The Director of Counterintelligence and Security Countermeasures, DCSINT, is the alternate representative.**

Chapter XIV Administrative Sanctions

14-100. Individual responsibility

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

14-101. 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 (Reference "b"), any implementing issuance's or this regulation,

(2) Knowingly, willfully or negligently disclose to unauthorized persons information properly classified under Reference "b" or prior orders, or

(3) Knowingly and willfully violate any other provision of Reference "b", any implementing issuance or this regulation.

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 regulation prohibits or limits action under the Uniform Code of Military Justice (Reference "uu") based upon violations of that code.

(1) Actions against military personnel may include those recognized by the manual for courts-martial (US), 1969 (Revised), Paragraph 128c, or provided by regulation. If none of these measures is clearly adequate, a commander should consider whether punitive action under the UCMJ is warranted.

(2) Administrative action against civilian personnel may be pursued under U.S. Army civilian personnel regulations.

14-102. Correction 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 Paragraph 14-1-1a, occurs or repeated administrative discrepancies or repeated disregard of requirements of this regulation occur (See Subsection 14-103). 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 regulation and other pertinent DoD issuance

14-103. 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 regulation that pertain to dissemination, storage, accountability and destruction. And that are determined not to constitute a violation under Paragraph 14-101a, may be grounds for adverse administrative action, including warning, admonition, reprimand or termination of classification authority as determined appropriate under applicable policies and procedures.

14-104. Reporting violations

a. Whenever a violation under Paragraph 14-101a, 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 regulation, the sanctions imposed and the corrective action taken. Whenever a violation under Subparagraph 14-101a, 1, or 3 occurs, the Director of Security Plans and Programs, ODUSD (P) shall be provided the same information. Notification of such violations shall be furnished to the Director of the ISOO in accordance with Section 5.4(d) of E.O. 12356 (Reference “b”) by the ODUSD (P). MACOM commanders and HQDA agency heads will report incidents involving the knowing and willful violation of this regulation as specified in Paragraphs 14-101a, 1 and 14-101a, 1 or 3 to HQDA (DAMI-CIS) Washington, DC 20310-1051. DAMI-CIS will forward the required reports to 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 (Reference “kk”) and DoD Instruction 5240.4 (Reference “jj”).

c. Any action reported under Paragraph “b”)above, 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 to have been responsible for repeated security violations over a period of a year, for appropriate evaluation, including re-adjudication of the employee’s security clearance. Reports of such individuals will be made through channels to HQDA (DAMI-CIS) Washington, DC 20310-1051, with a copy to the U.S. Army Central Personnel Security Clearance Facility (CCF), Attn: PCCF-A, Fort Meade, MD 20755-5250.

Chapter XV Safeguarding Joint Chiefs of Staff Papers

Section 1 General

15-100. Purpose

This chapter prescribes responsibilities and establishes procedures to secure and distribute JCS papers within the Army.

15-101. References

- a.* AR 380-10, Department of the Army Policy for Foreign Disclosure of Military Information to Foreign Governments.
- b.* JCS Policy Memorandum 39, Release Procedures for JCS Papers.
- c.* SF 135, Records Transmittal and Receipt.

15-102. Responsibilities

a. In accordance with JCS Memorandum of Policy, the Chief of Staff (CSA), Army will distribute JCS papers or extracts of these papers-

- (1) Within Department of the Army (DA).
- (2) To those agencies operating under the JCS for whom the Army is executive agent.

b. The Deputy Chief of Staff for Operations and Plans (DCSOPS) will ensure that the Joint Action Control Office, Office of the Deputy Chief of Staff for Operations and Plans (ODCSOPS) performs the following functions:

- (1) Control and distribution of JCS papers within DA.
- (2) Response to inquiries regarding distribution of JCS documents from-
 - (*a.*) Agencies or commands.
 - (*b.*) Organizations for which the Army is executive agent.
 - (*c.*) MACOM commanders and heads of headquarters staff agencies will ensure that-
 1. JCS papers are properly safeguarded.
 2. Requests for JCS papers are forwarded to HDQA (DMO-ZJC), Washington, DC 20310-0421.

Section 2 Requirements

15-200. Policies

a. JCS papers, including extractions from such papers, will be safeguarded in accordance with this regulation.

b. JCS papers will be safeguarded to ensure that release is not granted recipients not authorized as outlines in Section 3.

15-201. Access to JCS papers

Access to JCS papers will be limited to persons who have-

- a.* Appropriate security clearances, and
- b.* Official duties that require knowledge or possession of the JCS papers (i.e., need to know).

15-202. Familiarization requirements

a. The following personnel will become familiar with the provisions of this chapter:

(1) Those assigned to or employed by DA or any organization for which the Army is executive agent.

(2) Those who have access to JCS papers.

b. Personnel will be briefed on their responsibilities regarding JCS papers at the time of initial assignment and annually thereafter.

Section 3 Procedures

15-300. Distribution of JCS documents

a. JCS papers will be distributed only within the Army staff and to commanders of Army field and component commands and agencies. No other distribution will be made unless approval has been

granted by the Joint Secretariat, Organization of the Joint Chiefs of Staff.

b. Other Army activities that require information from JCS papers will be furnished abstracts when possible rather than complete documents. Such information will be phrased so that it can be clearly understood. For example, a decision of JCS should be referred to by such phrases as "On August 20 19___, the Joint Chiefs of Staff approved (or requested or directed) _____."

c. JCS papers that require a decision by the JCS will not be distributed outside the Army staff until a decision has been published.

d. JCS papers that must be approved by the President or Secretary of Defense will not be distributed outside the Army staff until approval is obtained. After these papers have been approved, the Joint Chief Secretariat and OJCS will officially notify the holders.

15-301. Release and distribution of Joint Strategic Planning System (JSPS) documents

Release and distribution of JSPS documents will be the same as for other JCS papers except for release to service schools and colleges. However, JSPS documents are subject to the following additional controls:

a. The Joint Action Control Office, ODCSOPS, will request a semiannual sighting report on JSPS documents. The report will include outstanding copies or sections of the current edition of separately bound portions classified secret or above.

b. Sections or extracts of JSPS documents may be reproduced or distributed to Army activities that require this information. Information should be issued in this form when possible, rather than in the form of entire documents.

c. A continuous chain of receipts will account for JSPS documents.

d. The CSA may distribute JSPS documents, except Joint Strategic Capabilities Plan (HSCP), to service schools and colleges for the following purposes:

- (1) To support the curriculum through controlled classroom use.
- (2) For use in curriculum-related, directed research by U.S. personnel from organizations responsive to the JCS or agencies that have received the documents.

e. JSPS documents may not be reproduced or automatically distributed to faculty or students of service schools and colleges. Access to the JSCP and Joint Strategic Planning Document Supporting Analyses (JSPDSA) will be further restricted to those members of the faculty and U.S. student body with an official duty requirement. Faculty or students in service schools and colleges conducting independent work (not in response to a JCS tasking) are not considered to have an official duty requirement.

15-302. Release and distribution of Joint Operation Planning System (JOPS) documents

Release and distribution of JOPS documents will be as follows:

a. Distribution or circulation will be limited to Army agencies directly concerned in supporting-

- (1) Operations plans prepared by the commanders of unified and specified commands.
- (2) Plans written to support these commands.

b. Distribution will not be made to Army service schools for-

- (1) Current and superseded operations plan.
- (2) Related documents prepared by supported, supporting and subordinate commanders.

15-303. Release of JCS information to Army Service schools

a. JCS papers are not normally distributed to schools. However, documents may be requested on a case-by-case basis-

- (1) To support the curriculum of U.S. students (controlled classroom use).
- (2) For use in directed-institutional research.

b. Fully justified requests for release of information will be submitted through command channels to HQDA (DAMO-ZCJ), Washington, DC 20310-0421.

c. Documents or information furnished to the schools will be controlled to ensure that access is limited to U.S. personnel with proper security clearances and need to know. Foreign nationals attending the schools may require access. If so, this fact will be specified in the request for release along with full justification as outlined in AR 380-10 (Reference "uuu").

d. Release of JSPS and JOPS documents will be as outlined in Paragraphs 15-301 and 15-302, above.

15-304. Release of information to organizations outside DA

JCS papers or extracts thereof will not be distributed outside of DA. Exceptions to this policy will be processed as follows:

a. Release of JCS documents or information extracted therefrom must be approved beforehand by JCS.

b. Each request will be considered on a case-by-case basis.

c. Requesting organizations will submit full justification to-

- (1) The Army agency with which they normally maintain contact.
- (2) The nearest Army area command or agency, or
- (3) The cognizance Army staff agency for validation.

d. These requests will be forwarded with recommendations to HQDA (DAMO-ZCJ), Washington, DC 20310-0421 for action.

e. The numbers of JCS green papers (JCS 0000/000) less than ten years old will not be referenced in the text of any extract for release to agencies outside DA

f. Non-concurrent JCS documents inter-filed in non-concurrent DA records may be transferred to records centers according to established requirements. In this case, SF 135 (Records Transmittal and Receipt) will stipulate that access to JCS documents attached by individuals or agencies not under the jurisdiction of the JCS or DA will be permitted only with the approval of the JCS.

15-305. Reproduction of JCS documents

JCS documents will not be reproduced except as authorized under Paragraph 15-301b.

Appendix A
 Equivalent Foreign and International Pact
 Organization Security Classifications

APPENDIX A
 Equivalent Foreign and International Pact Organization Security Classifications

Country	TOP SECRET	SECRET	CONFIDENTIAL	
Argentina	ESTRICTAMENTE SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
Australia	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Austria	STRENG GEHEIM	GEHEIM	VERSCHLUSS	
Belgium (French)	TRES SECRET	SECRET	CONFIDENTIEL	DIFFUSION
(Flemish)	ZEER GEHEIM	GEHEIM	VERTROUWELIJK	RESTREINT'S BEPERKTE VERSPREIDING
Bolivia	SUPERSECRETO or MUY SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
Brazil	ULTRA SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
Cambodia	TRES SECRET	SECRET	SECRET/CONFIDENTIEL	
Canada	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Chile	SECRETO	SECRETO	RESERVADO	RESERVADO
Columbia	ULTRASECRETO	SECRETO	RESERVADO	CONFIDENCIAL RESTRINGIDO
Costa Rica	ALTO SECRETO	SECRETO	CONFIDENCIAL	
Denmark	YDERST HEMMELIGT	HEMMELIGT	FORTROLIGT	TIL TJENESTEBRUG
Ecuador	SECRETISIMO	SECRETO	CONFIDENCIAL	RESERVADO

Figure A-1.

Country	TOP SECRET	SECRET	CONFIDENTIAL
El Salvador	ULTRA SECRETO	SECRETO	CONFIDENCIAL
Ethiopia	YEMLAZ BIRTOU MISTIR	MISTIR	KILKIL
Finland	ERITTAIM SALAINEN	SALAINEN	
France	TRES SECRET	SECRET DEFENSE	CONFIDENTIEL DEFENSE
Germany	STRENG GEHEIM	GEHEIM	VS-VERTRAULICH
Greece	AKPHE AIOPHTON	AIOPHTON	EMPHIYETIKON
Guatemala	ALTO SECRETO	SPCRETO	CONFIDENCIAL
Haiti		SECRET	CONFIDENTIAL
Honduras	SUPER SECRETO	SECRETO	CONFIDENCIAL
Hong Kong	TOP SECRET	SECRET	CONFIDENTIAL
Hungary	SZIGORJAN TITKOS	TITKOS	BIZALMAS
India	TOP SECRET	SECRET	CONFIDENTIAL
Indonesia	SANGAT RAHASIA	RAHASIA	TERBATAS
Iran	BEKOLI SERRI بکلی سری	SERRI سری	KHEILI MAHRAMANEH خیلی محرمانه
Iraq	سری مطلقه (Absolutely secret)	سری (Secret)	محرمانه محدود (Limited)
Iceland	ALGJORTI	TRUNADARMAL	

Figure A-2.

Country	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Ireland Gaelic	TOP SECRET AN-SICREIDEACH	SECRET SICREIDEACH	CONFIDENTIAL RUNDA	RESTRICTED SRLANTA
Israel	SODI BEYOTER סודי ביותר	SODI סודי	SHAMUR שמור	MUGBAL מגבל
Italy	SEGRETISSIMO	SEGRETO	RISERVATISSIMO	RISERVATO
Japan	KIMITSU 機密	GOKUHI 極密	HI 秘	TORIATSUKAICHUI 取扱注意 BUGAIHI 部外秘
JORDAN	MAKTUM JIDDAN مكتوم جدا	MAKTUM مكتوم	SIRRI سر	MAHDUD محدود
Korea	I KUP PI MIL I급 비밀	II KUP PI MIL II급 비밀	III KUP PI MIL III급 비밀	SECRET/CONFIDENTIAL
Laos	TRES SECRET	SECRET	SECRET/CONFIDENTIAL	DIFFUSION RESERVEINTE
Lebanon	TRES SECRET	SECRET	CONFIDENTIAL	
Mexico	ALTO SECRETO	SECRETO	CONFIDENCIAL	RESTRINGIDO
Netherlands	ZIEER GEHEIM	GEHEIM	CONFIDENTIEEL of VERTROUWELIJK	DIENSTGEHEIM
New Zealand	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Nicaragua	ALTO SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
Norway	STRENGT HEMLIG	HEMLIG	KONFIDENSIELL	BEGRENSET
Pakistan	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Paraguay	SECRETO	SECRETO	CONFIDENTIAL	RESERVADO

Figure A-3.

Country	TOP SECRET	SECRET	CONFIDENTIAL
Peru	ESTRICTAMENTE SECRETO	SECRETO	CONFIDENTIAL
Philippines	TOP SECRET	SECRET	CONFIDENTIAL
Portugal	MUITO SECRETO	SECRETO	CONFIDENTIAL
SAUDI ARABIA	SAUDI TOP SECRET	SAUDI VERY SECRET	SAUDI SECRET
Spain	MAXIMO SECRETO	SECRETO	CONFIDENTIAL
Sveden (Red Borders)	HEMIGIG	HEMIGIG	
Switzerland	(Three languages. TOP SECRET has a registration number to distinguish from SECRET and CONFIDENTIAL.)		
French	TRES SECRET	SECRET DEFENSE	CONFIDENTIEL DEFENSE
German	STRENG GEHEIM	GEHEIM	VERTRAULICH
Italian	SEGRETISSIMO	SECRETO	RISERVATISSIMO
Taiwan	絕對機密	極機密	機密
Thailand	LUP TISUD สุนทร	LUP MAAG สุนทร	LUP อู่
Turkey	ÇOK GİZLİ	GİZLİ	ÖZEL
Union of South Africa English	TOP SECRET	SECRET	CONFIDENTIAL
Afrikaans	UITERS GEHEIM	GEHEIM	VERTROULIK
United Arab Republic (EGYPT)	سري للغاية TOP SECRET	سري جدا VERY SECRET	سري SECRET
			RESTRICTED
			BEFERK
			OFFICIAL
			POK PID ၂၀၁၈
			HIZMET ÖZEL
			RESTRICTED
			BEFERK
			OFFICIAL

Figure A-4.

Country	'TOP SECRET'	'SECRET'	CONFIDENTIAL
United Kingdom	TOP SECRET	SECRET	RESTRICTED
Uruguay	ULTRA SECRETO	SECRETO	RESERVADO
USSR	СОВЕРШЕННО СЕКРЕТНО	СЕКРЕТНО	НЕ ПОДЛЕЖАЩИЙ ОГЛАШЕНИЮ ДЛЯ СЛУЖЕБНОГО ПОЛЬЗОВАНИЯ
Viet Nam	TRES SECRET	SECRET DEFENSE	DIFFUSION RESTREINTE
French	ТРИ СЕКРЕТ	МÂТ	TU MÂT
Vietnamese	ТÔI-МÂТ	МÂТ	KIN
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.

Figure A-5.

Appendix B
General Accounting Office Officials Authorized to
Certify Security Clearances

(See Paragraph 7-105c)

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, 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 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 Assistant 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, DC

Appendix C Instructions Governing Use of Code Words, Nicknames and Exercise Terms

(See Subsection 7-209)

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.* Word selected from those listed in Joint Army, Navy and Air Force Publication (JANAP) 299 (Reference "aa") 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) *Cancelled.* 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 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) The Joint Chiefs of Staff shall maintain a permanent record of all code words.

(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 two 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.

(3) The Deputy Chief of Staff for Operations and Plans (DCSOPS), HQDA will control and allot blocks of code words from JANAP 299 to MACOMs and U.S. Army commands on request. Commands are authorized to make assignments from these code word blocks, subject to rules in this regulation. The DCSOPS will allocate code words to HQDA agencies, as needed. Requirements will be submitted in writing to HQDA (DAMO-ODS), Washington, DC 20310-0440.

(b) Nicknames

(1) Nicknames may be assigned to actual events, projects, movement of forces or other non-exercise 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 (Reference "aa") or ACP 110 (Reference "vv"). 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 (Reference "aa") and later volumes.)

b. Combination of words including word "project," "exercise," or "operation."

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 and 4a above.

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

c. All requests for and changes in nicknames, including assignments, meanings, changes to meanings, cancellations, deletions and possible compromises will be submitted in writing to HQDA (DAMO-ODS), Washington, DC 20310-0440.

(c) Exercise term

(1) 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. The exercise term, 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 designed to simulate actual use of DoD code words and must be employed using identical security procedures throughout the planning, preparation, and execution of the test, drill or exercise to ensure realism.

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

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

c. Exercise terms will be reported as specified in Paragraph b5 above. All requests for and changes in exercise terms, including assignments, meanings, changes to meanings, cancellations, deletions and possible compromises, will be submitted in writing to HQDA (DAMO-ODS), Washington, DC 20310-0440 in accordance with AR 525-1 and JCS Publication 6, Volume II.

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 3b and 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 3b, 1 and 2 above.

(c) The using component shall assign to a code word a specific meaning classified Top Secret, Secret or Confidential, commensurate with military security requirements. Code words shall not be used to cover unclassified meanings. The assigned meaning need not in all cases be classified as high as the classification assigned to the plan or operation as a whole.

(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 should 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. MACOMs, Army Staff agencies and Field Operating Agencies will notify HQDA (DAMO-ODS), Washington, DC 20310-0440, of all code word transactions as specified above.

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

(1) Dissemination of the code word and its meaning to other DoD agencies will be made by ODCSOPS at the request of the assigning authority.

(2) The assigning authority is responsible for disseminating code words and their meanings to activities within its jurisdiction.

(3) When a MACOM or HQDA Agency receives classified meanings and related code words from an agency outside DA, the receiving activity will provide this information to activities under its jurisdiction when needed for security reasons.

(4) A MACOM that receives a code word and its classified meaning from an agency outside of the U.S. Army, for which there is no required action, will retain that information in the office responsible for maintaining records of code words. No internal distribution of the meaning will be made without approval from the original using agency.

(5) If MACOMs or HQDA agencies receive documents or messages that contain code words but do not have the associated meaning, that information may be requested in writing, from the DCSOPS if officially needed. Requests for the classified meaning will contain justification for the need.

(6) When a non-DoD Government agency furnishes a word that has a special meaning for use within DoD, recipients will be informed that it originated outside the department and is not subject to the department's code word policy. Words of this type will be safeguarded if required by the classification assigned by the originator.

(c) The using component is responsible for notifying the Joint Chiefs of Staff of cancelled code words. This cancellation report is considered final action, and no further reporting or accounting of the status of the cancelled 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. 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 two 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 two 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 addressees who may or may not have knowledge of the meaning. If the context of a document contains detailed instructions 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. 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 two years after the code words were placed in the former categories of "inactive," "Obsolete," or "canceled."

**Appendix D
Federal Aviation Administration Air Transportation
Security Field Offices**

(See Paragraph 8-302a.1)

Table D

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 (LaGuardia)	New York
Philadelphia	Pennsylvania
Pittsburgh	Pennsylvania
Portland	Oregon
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 Transportation Plan

(See Subsection 8-104)

The provisions of Subsection 8-104 of this regulation require that transmission instruction or a separate transportation plan is 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 Chapter VIII, 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 en route 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.

Appendix F Program Evaluation Guide

(Note: This appendix lists questions designed to assist Army activities in their monitor-ship responsibilities under the Information Security Program. This is not an all-inclusive checklist, but can form the basis for locally developed inspection checklists or self-evaluation guides.)

F-1. Assign authority to classify

a. Is original classification authority limited to the minimum number of officials whose duties involve the origination and evaluation of material requiring protection in the interest of national security?

b. Is original classification authority exercised only by officials authorized by the Deputy Chief of Staff for Intelligence?

c. Are listings of original classification authorities reviewed at least annually to ensure listed officials have demonstrated a continuing need for such authority?

d. Are changes to the original classification authority list forwarded to HQDA (DAMI-CIS) as they occur?

e. Are desk-side briefings given all approved original classification authorities before they exercise such authority?

F-2. Originally or derivatively classify information

a. Is information only within authorized categories classified?

b. Are classified guides developed for all Army classified projects/programs?

c. Is newly created material classified as reflected in the approved project/program classification guide?

d. If no classification guide exists, has the material been reviewed for classification by an original classification authority?

e. If no information is extracted from a classified source document, are all markings carried forward on newly created material?

f. Are classification decisions challenged when material appears to be unnecessarily classified?

g. Is unclassified material that may be classified referred to an original classification authority for review?

F-3. Perform Downgrading and declassification

a. Has a particular date or event been determined for the downgrading or declassification of classified material?

b. Is material marked OADR only when a specific date for downgrading/declassification cannot be determined?

(1) If declassification action is taken sooner than originally scheduled, or if duration of classification is extended, are all holders of the material promptly notified?

(2) Is the material remarked promptly according to the instructions provided by the originator?

(3) Are permanently valuable classified documents reviewed and remarked as necessary prior to transfer to record centers?

(4) Are requests for declassification and/or release of classified information reviewed by the originating agency?

(1) Does the proponent review program/project classification guides every two years?

(2) After the review, are all holders of guides advised in writing of changes in classification or that the guide is still current?

F-4. Properly marked classified material

a. Do all newly created classified documents contain the following mandatory markings:

(1) Highest overall classification (Top Secret, Secret, Confidential) on the front cover or face, title and first page of the document?

(2) Agency and office of origin?

(3) Date of document?

(4) Position title of the original classification authority on "classified By" line? Or other source of classification such as the title of an approved classification guides?

(5) Specific date or event for downgrading or declassification(as appropriate)?

(6) If "5" above cannot be determined, OADR?

(7) If the document is classified by "multiple sources," a list of all such sources on the record file copy of the document?

(8) If information is derived from a source document classified by "multiple sources," the title of the source document in the "classified By" line of the new document?

(9) Additional warning notices/caveats, (e.g., Restricted Data)when reflected on source document(s)?

b. Is every internal paragraph, part, section, portion, subparagraph, drawing, graph and illustration, etc., of each document marked with its individual classification (TS), (S) or (C)as appropriate?

c. Are unclassified portions also individually marked (U) as appropriate?

(1) Are the markings (TS), (S), (C) or (U) following, and to the right of the document subject or title (e.g., The Information Security Program (U))?

(2) Are unclassified short titles used in lieu of classified document titles to expedite administrative handling?

(3) Is each interior page of each classified document marked top and bottom with the highest overall classification of the material contained on that page, front and back?

(4) For published documents, in lieu of marking each page according to its individual classification, is each page of the published classified document marked top and bottom, front and back, with the highest overall classification of the entire document?

(5) Are major components of a complex document, e.g., the bibliography, index or glossary, which are likely to be separated and used individually, marked as separate documents?

(6) If a chapter of a classified document is unclassified in its entirety, does the first page of the chapter contain a statement reflecting this fact?

(7) Do electronically transmitted messages contain proper overall and portion markings?

(8) Do record copies of messages reflect the source of original or derivative classification?

(9) Are markings applied to special types of classified materials, such as charts, maps, drawings, photographs, films, recordings, transparencies and slides, microforms and microfiche, etc.?

(10) Does the first page of an unclassified transmittal document, such as a cover letter, reflect the highest classification, classified by line, downgrading instructions and special caveats/markings contained on the enclosed classified document?

(11) Does the unclassified transmittal document also contain a notation advising that the cover letter is unclassified when the classified enclosure is removed?

F-5. Transmit classified information properly

a. Is Top Secret information transmitted by courier service(DCS) or an appropriately cleared courier?

b. Does U.S. Postal Service; Registered Mail or an appropriately cleared courier transmits Secret information?

c. Is confidential information transmitted between government entities via U.S. Postal Service, First Class mail or Express mail?

d. Is confidential information forwarded to or from defense contractors transmitted via U.S. Postal Service Certified mail or Express mail?

e. Is Federal Express used for overnight delivery of confidential information within the United States only?

f. Is U.S. Postal Service Registered mail used to forward:

(1) All NATO Confidential materials?

(2) All Confidential to and from APO/FPO addresses?

(3) All Confidential material dispatched to and from U.S.-activities in Panama?

(4) All Confidential COMSEC materials?

g. Is classified information hand-carried only when absolutely necessary?

h. Are records kept of all classified material being hand-carried?

i. Is the hand-carrying of classified material outside the U.S. and on board commercial aircraft-

(1) Limited to emergency situations when the material is not available at the destination?

(2) Approved only by a MACOM or ARSTAF G2 or Director of Security and authorized in writing?

(3) Limited to hand carrying to the destination whenever possible, material mailed back?

j. Are couriers for classified information:

(1) Cleared to the level of material to be hand-carried?

(2) Briefed by the security manager concerning their duties and procedures to be followed?

(3) Designated in writing by the security manager?

k. Is the courier designation limited to a specific event or period?

l. Are all term courier designations reviewed and re-certified annually to ensure that a bona fide need?

m. Is the hand-carried material reconciled with office records to ensure all information has been returned?

n. Have arrangements been made for authorized storage for classified material upon arrival at the destination?

o. Is classified information transmitted to a foreign government:

1. After release to the specific government involved has been approved by HQDA (DAMI-CIT)?

(2) Only through approved government-to-government channels?

(3) Released to an embassy, official agency or representative of the recipient government?

(4) Via direct on loading by ship, aircraft or other carrier designated by the recipient government provided a recipient government representative is present at the point of departure?

p. Is all classified material to be hand-carried or forwarded through the U.S. Mail:

(1) Enclosed in two opaque sealed envelopes or other double package?

(2) Addressed on the outer envelope to an official government or DoD contractor with a facility clearance, not to an individual, and the sender's return address?

(3) Addressed on the inner envelope as in "2" above and marked with the highest classification of the package contents as well as applicable caveats/markings?

q. Has a classified document receipt (DA Form 3964) been included in secret packages sent through a mailroom or the U.S. Postal Service?

r. Did the receiving command retain one copy of the (DA Form 3964) as its record of receipt of Secret material in addition to forwarding one copy back to the sending activity?

s. Is a receipt also obtained for all Secret material hand-carried or forwarded by mail to a contractor?

t. Has a classified material receipt been obtained for all Top Secret information, whether transmitted by courier or ARFCOS?

u. Are all DA Forms 3964 and 969s retained for two years?

F-6. Classified information access, dissemination and accountability

a. Does the government individual desiring access to classified information-

(1) Have an official reason for requiring access to classified material?

(2) Need access to the classified information to accomplish a bona fide job requirement (need to know)?

(3) Possess a security clearance at an appropriate level, verify by his/her security manager?

(4) Have a courier authorization if material is to be released?

b. Does the defense contractor desiring access to classified information:

(1) Have a current Army or other government contract requiring access to the material?

(2) Have a written certification of need-to-know for the material from the Government Contracting officer?

(3) Have an approved visit request on file from his/her security

manager with security clearance certification at the appropriate level?

c. Have arrangements and approvals been obtained in advance prior to release of classified information to contractors?

d. Does the contractor possess a written courier authorization from the security manager?

e. Has a receipt been obtained for all classified information released to contractors?

f. Have proper procedures been established for the dissemination of classified material?

g. Are security clearances revoked for cause when necessary?

h. Have proper procedures been established for the dissemination of classified material?

i. Is classified information released to foreign nationals only when authorized under the provisions of the National Disclosure Policy?

j. Are special restrictions on dissemination of intelligence information, e.g., Originator Controller (ORCON), No Contractor Release (NOCONTRACT), etc., observed?

k. Is consent of the originator or higher authority obtained before reproduction of Top Secret material?

l. Have officials been designated by position title to approve the reproduction of Top Secret and Secret information?

m. Is copying of classified information kept to the absolute minimum?

n. Are operators assigned to classified reproduction machines wherever possible?

o. Has specific reproduction equipment been designated for copying classified materials?

p. Have the rules for reproduction of classified material been posted with designated reproduction equipment?

q. Are notices prohibited classified reproduction posted on equipment used only for reproduction of unclassified materials?

r. Are copies of classified documents subjected to the same controls as the originals?

s. Are top secret accountability registers and access rosters maintained?

t. Are Top Secret documents inventories annually and excess material destroyed?

u. Are only mission essential Top Secret documents retained?

v. Are Secret and Confidential documents reviewed annually and excess materials destroyed?

w. Are classified documents, which cannot be destroyed, re-evaluated for possible downgrading or declassification?

x. Is a continuous chain of receipts established for all Top Secret documents?

y. Are all Top Secret documents numbered serially?

z. Have procedures been established to protect incoming mail until a determination is made as to whether it contains classified information?

aa. Are working papers accounted for and controlled in the same manner as a finished document of the same classification under the conditions specified in Paragraph 7-304a5?

ab. Is the two-person rule followed in areas where Top Secret and Special Access Program (SAP) information is stored and accessible?

ac. Are individuals prohibited from working alone after hours in areas where Top Secret and SAP information is stored and accessible?

ad. Has an exception to policy been submitted and approved for Top Secret and SAP areas where the two-person rule cannot be implemented?

F-7. Ensure security of meetings and conferences

a. Have all personnel been advised of the procedures for obtaining approval to sponsor a classified meeting, conference or symposium?

b. Are all classified meetings, non in-house, sponsored by an Army activity, which accepts responsibility for meeting the security requirements of Paragraph 5-205?

c. Has a request for sponsorship approval been submitted to

HQDA (DAMI-CIT) no later than 120 days prior to the planned conference date?

d. Is the classified conference to be held in a government or cleared contractor facility?

e. If the answer to "4" above is no, has a request for exception to policy been submitted to HQDA (DAMI-CIS) no later than 120 days prior to the conference date?

f. Have authorized foreign industry representatives been included in all acquisition-related classified meetings?

g. Has approval been obtained from HQDA (DAMI-CIT) for attendance by foreign representatives?

h. Has approval to sponsor the classified meeting been obtained from HQDA (DAMI-CIT) prior to making any public announcements or issuing invitations?

i. Has a security manager for the conference been appointed?

j. Have security measures/access procedures for the conference been developed?

k. Does the meeting site meet the physical security requirements for control, storage and protection of the classified information to be presented?

l. Are GSA-approved safes available for overnight storage of classified notes, papers, etc.?

m. Is access to classified sessions limited to government persons and defense contractors whose security clearance and need-to-know have been positively established by a written visit request furnished in advance?

n. In addition, do all contractors' visit requests contain:

(1) The contract numbers project or program, which pertains to the subject matter of the classified meeting?

(2) The level of classified access authorized under the contract?

(3) The purpose/justification for attendance?

(4) The government contracting officers' certification of the person's needed to attend?

o. Has approval been obtained from HQDA (DAMI-CIT) for disclosure of classified information to representatives of the foreign countries expected to attend?

p. Are only foreign nationals approved by HQDA (DAMI-CIT) allowed to enter classified sessions?

q. Are all cleared/certified personnel meeting the need-to-know requirements included on the conference-accessing roster?

r. Is proper identification, driver's license, ID card, etc., shown by each person to establish their identity before entering classified sessions?

s. Are all announcements, invitations, etc. reviewed and approved by security in advance of issuance to ensure they are unclassified?

t. Is the loss or compromise of classified information at conferences or symposia promptly reported by message to HQDA (DAMI-CIS) and investigated?

u. Are classified symposia conducted by contractors approved in advance by the Army proponent for the discussion topics?

v. Do contractor requests include the names of proposed attendees who are not U.S. citizens?

w. Does the request for sponsorship of a classified meeting, addressed to HQDA (DAMI-CIT) include:

(1) Subject of meeting, topical outline and classification of each topic?

(2) Date and location?

(3) Identity of sponsoring Army activity?

(4) Name, grade and telephone number of activity point of contact?

(5) Foreign countries the sponsor desires to invite or a fully justified proposal to exclude foreign nationals)?

x. If non-government associations, such as ADPA, AUSA, etc., are involved in the conduct of a classified meeting:

(1) Has HQDA (DAMI-CIT) been notified of the non-government organization involved?

(2) Has HQDA approved the non-government association's participation?

y. If a non-government association is involved, did the Army

activity's request for sponsorship sent to HQDA (DAMI-CIT) include:

(1) A summary of subjects, levels and source of classified information?

(2) The name of the association holding the meeting?

(3) Location of the meeting, including a physical security certification for the site?

(4) The name, addresses and phone number of the point of contact at the Army sponsoring activity?

(5) The reason for having the classified meeting, conference or symposium?

F-8. Prevention compromise of classified information

a. Are persons aware of their responsibilities in the event of an actual or possible compromise?

b. Once reported, is a preliminary inquiry immediately conducted into the circumstances of the incident?

c. Does the preliminary inquiry report include:

(1) Where and when the violation occurred?

(2) Who reported the violation, to whom and when?

(3) A summary of the incident, identity of the document or material and its classification?

(4) An estimate of the cause of the violation, including contributing factors and identity of the person(s) responsible if known?

(5) A summary of corrective and/or disciplinary action taken or anticipated, if applicable?

(6) A recommendation on the need for further investigation, if further investigation would reasonably reveal the cause(s), responsibility and/or compromise aspects of the case?

d. Does the preliminary inquiry report establish one of the following findings:

(1) Compromise did not occur?

(2) Compromise did occur?

(3) Probability of compromise is remote?

(4) Probability of compromise is not remote?

e. If a compromise is positively established, or the probability of compromise is not remote:

(1) Has an estimate of the damage to the national security been made?

(2) Has the proponent for the compromised information been advised?

(3) Has a damage assessment been conducted of the compromised material?

(4) Has mitigating action been taken as a result of the compromised?

f. Is a formal investigation initiated whenever the preliminary inquiry is insufficient or if otherwise required?

g. Are formal investigation reports reviewed, approved and closed by a final approval authority?

h. Has one copy of the completed report of investigation involving compromise of Top Secret and/or Secret material been forwarded through command channels to HQDA (DAMI-CIS)?

i. Are persons aware that they must report unauthorized disclosures of classified information in newspapers, magazines, etc., to the commander or security manager?

j. Once notified, is HQDA (DAMI-CIS) promptly advised of the unauthorized disclosure?

k. Does the report of unauthorized disclosure by HQDA include:

(1) Identification of the classified information involved?

(2) The nature and circumstances of the incident?

(3) The exact identification of the publication or public broadcast in which the information appeared?

l. If the reporting activity is the proponent of the information does the report also include:

(1) An assessment of the accuracy of the information?

(2) The level and source of classification of the information?

(3) A preliminary estimate of the nature and degree of damage to the national security caused by the disclosure?

(4) Any available information regarding the probable source of the leak document, briefing, etc., and the extent to which the material was disseminated?

(5) Any available information concerning individuals who may have been responsible for the disclosure?

m. Has the unauthorized disclosure report been classified to prevent further dissemination of the information leaked?

n. Has a classification re-evaluation of the disclosed information been accomplished by the proponent?

o. Are all damage assessments developed as a result of probable or actual compromise, and/or the unauthorized disclosure of classified information, retained by the proponent?

F-9. Disposal and destruction of classified information

a. Are all personnel aware that classified material must be destroyed by burning, shredding or other authorized methods?

b. Has the facility established procedures for the pick up and destruction of classified waste?

c. Do all personnel follow local procedures for disposal of classified waste?

d. Is non-record classified information and other material of similar temporary nature destroyed when no longer needed?

e. Is classified material destroyed in the presence of two witnesses for Top Secret information and one witness for Secret?

f. Do those witnessing classified destruction ensure the method used precludes later recognition or reconstruction of the material?

g. Are records of destruction prepared when required?

h. Are records of destruction retained for two years?

i. Are waste materials such as handwritten notes, carbon paper and working papers containing classified information also destroyed by authorized methods?

F-10. Safekeeping and storage of classified information

a. Do containers, vaults, alarm systems and associated security devices used for storage and protection of classified material meet GSA standards?

b. Is information and material afforded protection equal to the level of classification assigned?

c. Are surveys made of on-hand security storage equipment and classified records before procurement of new storage equipment?

d. Are exemptions obtained from HQDA (DAMI-CIS) before procurement of security containers not listed in the GSA Federal Supply Schedule?

e. Are combinations to security containers changed at least annually and as otherwise required?

f. Are records of combinations assigned a security classification equal to the highest category of information stored in the containers?

g. Are combinations to security containers disseminated on a need-to-know basis?

h. When taken out of service, are built-in combination locks reset to a standard combination of 50-25-50 and combination padlocks reset to a standard combination of 10-20-30?

i. Do local procedures provide for only cleared or continuously escorted persons to neutralize lockouts or repair damage to a container authorized to store classified information?

j. Do custodians of classified material understand their responsibilities and carry them out?

k. Are procedures established for controlling the removal of classified information from the facility?

l. Has a briefcase inspection program been established at the facility and has the policy on the program been prominently posted?

m. Have all personnel been advised in writing of the intent of the briefcase inspection policy?

n. Have inspectors been trained in procedures to follow should individuals attempt to remove classified material without authorization?

o. When inspections are conducted after normal duty hours, weekends and holidays, are they conducted at all entry/exit points?

p. Have courier authorizations been issued to individuals who have a legitimate need to remove classified material?

q. Have procedures for end-of-day security checks been established in all offices handling classified material?

r. Have emergency destruction plans been developed and tested?

s. Is security practiced in telephone conversations on non-secure telephones?

t. Are classified documents removed from storage kept under constant surveillance and/or covered?

u. Are preliminary drafts, carbon sheets, work sheets, stencils, etc., protected according to their content? Are they destroyed after they have served their purpose?

v. Are appropriate measures taken to protect classified information located in foreign countries?

F-11. Provide security education

a. Has a security education program been established?

b. As a minimum, are all personnel familiar with:

(1) The adverse effects caused by unauthorized disclosure of classified material and their responsibilities for protecting it?

(2) The principles, criteria and procedures for the classification, downgrading, declassification, marking and dissemination of information?

(3) Procedures for challenging classification decisions?

(4) The specific security requirements of their particular job?

(5) The techniques employed by hostile intelligence to obtain classified information?

(6) The penalties for engaging in espionage activities?

(7) The strict prohibition against discussing classified information over an unsecured telephone?

(8) The penalties for violation of this regulation?

(9) The requirement to determine a person's need-to-know and security clearance prior to allowing them access to classified information?

(10) The channels for reporting matters of security interest?

(11) The reasons why intelligence information is especially sensitive?

(12) The objectives of the Army's Operation Security (OPSEC) Program?

c. Are all personnel aware they must report to their security manager-

(1) Physical security deficiencies?

(2) The possible or actual loss of classified material?

(3) Adverse information concerning other individuals who possess a security clearance?

(4) Unauthorized disclosures to the public media?

d. Are foreign travel briefings given to personnel before travel to alert them to possible exploitation?

e. Are termination briefings given to employees separating from the Army, or upon termination of employment?

f. Is a Security Termination Statement executed?

g. Are Security Termination Statements retained for two years?

h. Have all classified materials in the individual's possession been recovered?

i. Is CCF notified if an individual refuses to sign a Security Termination Statement?

j. Are special in-depth briefings given to personnel who must:

(1) Act as couriers for classified material?

(2) Hand-carry classified material outside the U.S. on commercial aircraft?

(3) Have access to SCI or SAP materials?

(4) Act as Original Classification Authorities (OCAs)?

F-12. Monitor and manage information security program

a. Have all Army activity commanders and agency heads-

(1) Designated a properly cleared professional commissioned officer (0-3), warrant officer or DA civilian (GS-080-9 or above) as the MACOM or ARSTAF security manager? (Note: Subordinate element security managers may be of lesser rank/grade than above.)

(2) Established security policy and procedures which comply with this regulation?

(3) Allocated resources to manage information security program requirements?

(4) Integrated the security program with mission requirements of the activity?

b. Have all designated security managers-

(1) Established an activity Information Security Program?

(2) Established an activity program to train employees in the proper handling, marking, storage, classification, declassification, upgrading and downgrading of classified information?

(3) Established procedures to ensure all personnel with access to classified information are properly cleared with a need-to-know?

(4) Established a program for self-inspections and periodic oversight inspections of subordinate elements?

c. Does the security manager ensure the protection of classified information presented during meetings, symposia, conferences, etc., sponsored by the activity?

d. Does the security manager act as single point of contact for coordinating, challenging and resolving classification and declassification problems?

Appendix G Security Classification Guide Preparation

Section 1 General

G-1.

This appendix discusses preparation of security classification guides. Due to the wide variety of systems, plans and projects for which guides must be published, this appendix provides very general guidance only. The effort must be tailored to fit the specific nature of the guide subject and the classification guidance, which must be provided.

G-2.

This appendix supplements DoD 5200.1-H (Department of Defense Handbook for Writing Security Classification Guidance), which is included as Section II. DoD 5200.1-H has not yet been revised to include new classification criteria and marking requirements of Executive Order 12356. But it still provides useful guidance on preparing classification guides. When DoD 5200.1-H is revised, a change to this regulation will be published; this change will include the revised handbook.

G-3.

The question of classifying guides themselves requires careful consideration.

a. Guides should be published in unclassified form if possible. However, classified guides may be published if necessary. To avoid classifying a guide, it is sometimes possible to include all necessary classified information in a classified supplement. This is also a good method of dealing with Special Access Program Information.

b. Preparing of guides must be careful that descriptions of classified information in the guide do not inadvertently disclose classified information.

c. Like any other classified document, classified guides must be-

(1) Portion marked.

(2) Marked with the identity of the classifier and declassification instructions.

G-4.

The sample format in Section III provides somewhat more detailed guidance than DoD 5200.1-H, Appendix D and has been tailored for use within DA. This format is in the form of selected portions of a hypothetical missile system guide. (Note: Except for Sections 1, 2, 6 and 7, the guide contains only a sampling of topics that normally would be included. Comments are enclosed in parentheses. References are to this regulation.

G-5.

Section IV provides instructions on changing and re-issuing guides.

G-6.

Section V contains instructions for preparing and submitting DD Form 2024. These instructions supplement those found on the reverse of the form and in Paragraph 2-406 of this regulation.

Section II

DoD 5200.1-H Department of Defense Handbook for Writing Security Classification Guidance



**DEPARTMENT OF
DEFENSE HANDBOOK
FOR WRITING
SECURITY
CLASSIFICATION
GUIDANCE**

MARCH 1986



POLICY

THE UNDER SECRETARY OF DEFENSE

WASHINGTON, D.C. 20301

18 March 1986

FOREWORD

This Handbook is issued under the authority of DoD Directive 5200.1, "DoD Information Security Program," June 7, 1982. Its purpose is to assist managers of classified programs, projects, and systems in the development of comprehensive security classification guidance that they are responsible for under Chapter II, Section 4, of DoD 5200.1-R, "Information Security Program Regulation."

DoD 5200.1-H, "Department of Defense Handbook for Writing Security Classification Guidance," October 1980, is hereby canceled.

Users of this Handbook are encouraged to direct comments to the Director of Security Plans and Programs, Office of the Deputy Under Secretary of Defense for Policy, The Pentagon, Washington, D.C. 20301-2200.


Craig Alderman, Jr.
Deputy

Distribution of this Handbook is authorized to U.S. Government Agencies and their contractors (Administrative or Operational Use) (March 18, 1986). Other requests for this document shall be referred to the Security Plans and Programs Directorate, Office of the Deputy Under Secretary for Policy, Washington, D. C. 20301-2000.

REFERENCES

- (a) Executive Order 12356, "National Security Information," April 2, 1982
- (b) Information Security Oversight Office Directive No. 1, "National Security Information," June 23, 1982
- (c) DoD 5200.1-R, "Information Security Program Regulation," August 1982, authorized by DoD Directive 5200.1, June 7, 1982
- (d) DoD 5200.1-I, "Index of Security Classification Guides,"¹ authorized by DoD Directive 5200.1, June 7, 1982
- (e) National Foreign Intelligence Board (NFIB) No. 24.1/18, "Glossary of Intelligence Terms and Definitions," June 15, 1978
- (f) DoD Instruction 5230.22, "Control of Dissemination of Intelligence Information," April 1, 1982

¹Published on a semiannual basis

TABLE OF CONTENTS

	<u>Page</u>
Foreword	i
References	ii
Table of Contents	iii
CHAPTER 1 - INTRODUCTION	1-1
CHAPTER 2 - CLASSIFICATION AND DECLASSIFICATION	
2-1 General	2-1
2-2 Classification	2-1
2-3 Declassification	2-2
2-4 Downgrading	2-3
2-5 Marking	2-3
CHAPTER 3 - A PLAN OF ACTION FOR WRITING CLASSIFICATION GUIDES	
3-1 Step 1. Consider Related Current Guidance	3-1
3-2 Step 2. Determine State of Art Status	3-1
3-3 Step 3. Identify Advantage Factors	3-2
3-4 Step 4. Make Initial Classification Determinations	3-2
3-5 Step 5. Identify Specific Items of Information That Require Classification	3-3
3-6 Step 6. Determine How Long Classification Must Continue	3-3
3-7 Step 7. Writing the Guide	3-4
CHAPTER 4 - CLASSIFYING HARDWARE ITEMS	
4-1 General	4-1
4-2 Hardware Classification Considerations	4-1
4-3 User Considerations	4-2
CHAPTER 5 - CLASSIFYING MILITARY OPERATIONS INFORMATION	
5-1 General	5-1
5-2 Military Operations Information	5-1
5-3 Definitions of Military Operations Terms	5-1
5-4 Military Operations Classification Considerations	5-2
5-5 Downgrading and Declassification Instructions	5-3
5-6 Items to be Considered for Classification	5-3
CHAPTER 6 - CLASSIFYING INTELLIGENCE INFORMATION	
6-1 General	6-1
6-2 Intelligence Information	6-1
6-3 Intelligence Classification Considerations	6-2
6-4 Intelligence Dissemination and Declassification Considerations	6-5
6-5 Special Markings	6-5
6-6 Classification Guide Illustrations	6-6

CHAPTER 7 - CLASSIFYING FOREIGN RELATIONS INFORMATION

7-1	General	7-1
7-2	Foreign Relations Information	7-1
7-3	Foreign Relations Classification Considerations	7-1
7-4	Classification Guide Illustrations	7-3

APPENDICES

A	Initial Classification Determinations	A-1
B	Classifying Details - Considerations	B-1
C	Classifying Details - Items of Information	C-1
D	Recommended Format for a Security Classification Guide	D-1
E	Format Variations	E-1

CHAPTER 1

INTRODUCTION

Good security classification practice in an organization as large and wide-spread as the Department of Defense, calls for the timely issuance of comprehensive guidance regarding security classification of information concerning any system, program, project, plan, operation, equipment or item; the unauthorized disclosure of which reasonably could be expected to cause damage to National security. Precise classification guidance is prerequisite to effective and efficient information security, and can do much to assure that security resources are expended to protect only that which truly warrants protection in the interest of national security. Executive Order 12356 (reference (a)) and its implementing Information Security Oversight Office Directive No. 1 (reference (b)) provide general requirements and standards concerning the issuance of security classification guides.

Information is what is classified for protection. Therefore it is essential that a classification guide be concerned primarily with identifying the specific items of information requiring protection against unauthorized disclosure, specifying the level of protection afforded those items, and establishing the time period when the protection must be continued.

Paragraph 2-400a. of DoD 5200.1-R (reference (c)) requires that a classification guide be issued as early as practical before the initial funding or implementation of each classified system, program, project, or plan. Any uncertainty in application of the policies and requirements of DoD 5200.1-R will result in a less than satisfactory security classification guide. Accordingly, the requirements of DoD 5200.1-R regarding classification, declassification, downgrading, marking, and security classification guides should be reviewed and understood before proceeding with the task of writing a security classification guide.

This Handbook deals with writing security classification guidance applicable to military weapon systems and hardware, military operations, intelligence, and foreign relations information.

CHAPTER 2

CLASSIFICATION AND DECLASSIFICATION

2-1 GENERAL

Since the primary purpose of this Handbook is to provide assistance to those who are responsible for the writing of a security classification guide, some discussion of classification and declassification principles is warranted.

2-2 CLASSIFICATION

Let's start with the question "How do I go about classifying information?"

a. Basically, information is classified in one of two ways, either derivatively or originally. Derivative classification occurs when the information under consideration fits the description of information already known to be classified. Original classification occurs when information is developed which intrinsically meets the criteria for classification under Executive Order 12356, (reference (a)) and such classification cannot reasonably be derived from a previous classification still in force involving in substance the same or closely related information. A security classification guide is, in effect, the written record of an original classification decision or series of decisions regarding a system, plan, program, or project. Some specific examples of original classification criteria are as follows:

(1) The information provides the United States national defense a scientific, engineering, technological, operational, intelligence, strategic, or tactical advantage over other nations.

(2) Disclosure of the information would weaken the international position of the United States, create or increase international tensions contrary to United States interests, result in a break in diplomatic relations, or lead to hostile economic, political, or military action against the United States or its allies, thereby adversely affecting national security.

(3) Disclosure of the information would weaken the ability of the United States to wage war or defend itself successfully, limit the effectiveness of the Armed Forces, or make the United States vulnerable to attack.

(4) There is sound reason to believe that other nations do not know that the United States has, or is capable of obtaining, certain information or material that is important to the international posture or national defense of the United States compared with those nations.

(5) There is sound reason to believe that the information involved is unique, is of singular importance, and is vital to national security.

(6) The information represents a significant breakthrough in basic research that has a direct military application potential in a new field, or a radical change in an existing field.

(7) There is sound reason to believe that knowledge of the information would:

(a) Provide a foreign nation insight into the war potential, the war defense plans, or posture of the United States.

(b) Allow a foreign nation to develop, improve, or refine a similar item of war potential.

(c) Provide a foreign nation a base upon which to develop effective countermeasures.

(d) Weaken or nullify the effectiveness of a defense or military plan, operation, project, or activity that is vital to the national defense.

b. An original classification authority is confronted with the need to decide whether certain information should be classified. To make this determination there are a number of steps to go through. These steps may be laid out as a series of questions.

(1) Does the information fall within one of the several categories of information that is classifiable in accordance with subsection 2-202 of DoD 5200.1-R (reference (c)), (for example, military plans, weapons, or operations; foreign government information; or intelligence activities, sources or methods)?

(2) If the answer to the foregoing question is "no," the information cannot be classified. If answered "yes," then the next question - Can the unauthorized disclosure of the information reasonably be expected to cause damage to national security?

(3) Again, if the answer to the second question is "no," the information cannot be classified. If answered "yes," then the third question - What is the degree of damage to national security that is expected in the event of an unauthorized disclosure of the information?

(4) If the answer to the final question is just "damage," you have arrived at a decision to classify the information Confidential ("C") (see subsection 1-503 of reference (c)). If the answer is "serious damage," you have arrived at a decision to classify the information Secret ("S") (see subsection 1-502 of reference (c)). If the answer is "exceptionally grave damage," you have arrived at a decision to classify the information Top Secret ("TS") (see subsection 1-501 of reference (c)).

2-3 DECLASSIFICATION

The declassification decision determines duration of protection, and is as important as the original classification determination. Therefore, having arrived at the decision to classify certain information, it is now necessary to determine how long the information shall remain classified.

a. Those authorized to make original "C," "S," or "TS" classification determinations must set a date or event for declassification if such a date or event can be predetermined at the time the original classification decision

is made. Only when a declassification date or event cannot be predetermined may original classification authorities provide for indefinite duration of classification. When this is done, the information will be marked "Originating Agency's Determination or Required" or "OADR."

b. The determination as to when information should be declassified shall not be made on the basis of the level of classification originally assigned, but rather on the expected perishability and loss of sensitivity of the information with the passage of time. In a somewhat predictable way, classified information loses its sensitivity with the passage of time. The designation of a time for declassification can be predicated on certain knowledge, a reasonable judgment, or experience. Alternatively, the designation of a particular event certain to occur can be made when circumstances could effectively eliminate the need for classification.

c. A forecast time for declassification shall be determined in light of any one or a combination of the following considerations: state-of-the-art advances that bring about obsolescence; the occurrence of a particular anticipated event; the loss of sensitivity due to the passage of time; the expectation of compromise of information or material due to wide dissemination or use of it; the expectation of official public release; anticipated changes in international political climate; future change in emphasis or reliance on an intelligence source, method, equipment, or defense plan; or an anticipated action that will overcome a vulnerability of a program, project, or system. You may also find that other declassification considerations pertain to your effort.

2-4 DOWNGRADING

Executive Order 12356 (reference (a)) does not provide an automatic downgrading system. It does, however, allow the original classifier to provide for downgrading of classification to a lower level at predetermined points in time, or upon the occurrence of specified events. You are encouraged to specify in your guide, downgrading to a lower level of classification when the lower level will provide adequate protection. However, do consider the utility of downgrading at some future date or event in connection with each determination to classify (other than at the "C" level), particularly when information is originally classified at the "TS" level.

2-5 MARKING

When writing a security classification guide, you are in effect providing direction to others on how to mark information with its proper security classification. Knowing how classified information in documentary or hardware form is marked, will assist in the writing of a security classification guide that will leave no doubt as to how you want information marked and, therefore, adequately protected.

CHAPTER 3

A PLAN OF ACTION FOR WRITING CLASSIFICATION GUIDES

3-1 Step 1. CONSIDER RELATED CURRENT GUIDANCE

Before the actual writing of a security classification guide begins, it is necessary to find out what, if any, classification guidance already issued is applicable to items of information concerning the plan, program, project, system, item, or operation for which the classification guide is being constructed. Any existing guidance may affect your effort, and should be considered carefully. Uniformity and consistency in the exercise of classification authority, especially in the form of a security classification guide, are essential. Be alert to conflicts between the guide you will be developing and any already approved guide.

In some fields of interest guides have been issued that apply to a broad spectrum of activities. Such guides often are issued as DoD Instructions through the DoD Directives System. DoD 5200.1-I (reference (d)) provides a listing of most guides issued within the Department of Defense. Many of the listed guides are available from the Defense Technical Information Center. Always check reference (d)), but be aware that some classification guides are too sensitive to be identified in reference (d). In addition, there may be other classification guides issued along functional lines by activities outside the Department of Defense that could have a bearing on your effort. Seek the advice of those who have knowledge of classification in the subject area under consideration or in closely related fields. Engage the assistance of the information security specialist in your activity to find out what other classification guides may be available. Obtain and analyze all available classification guidance in the field of interest to see how it may govern, fit, or adapt to the particular system or item for which your guide is being developed. While it is not always wise to merely parrot security classification guidance issued for another system or item of the same type or class as your own, neither is it desirable to "re-invent the wheel."

3-2 Step 2. DETERMINE STATE-OF-THE-ART STATUS

Reasonable classification determinations cannot be made in the scientific and technical field without analysis of what has been accomplished, and what is being attempted and by whom. Make use of scientific and information services; consult technical and intelligence specialists; obtain whatever assistance is available from any proper source. Learn about the state-of-the-art, the state of development and attainment in the field of work, and what is known and openly published about it, including:

- a. The known or published status, foreign and domestic.
- b. The known but unpublished (probably classified) status in the United States.
- c. The foreign status in friendly and unfriendly countries.

d. The extent of foreign knowledge of the unpublished status in the United States.

3-3 Step 3. IDENTIFY ADVANTAGE FACTORS

The subject matter of your guide must be looked at as a totality. Decide what it does or seeks to accomplish that will result in a net national advantage. Cover all the values, direct and indirect, accruing or expected to accrue to the United States. In the final analysis, the decision to classify will be related to one or more of the following factors, producing directly or indirectly the actual or expected net national advantage:

- a. Fact of interest by the U. S. Government in the particular effort as a whole or in specific parts that are being considered or emphasized.
- b. Fact of possession by the United States.
- c. Capabilities of the resulting product in terms of quality, quantity, and location.
- d. Performance, including operational performance, as it relates to capability.
- e. Vulnerabilities, countermeasures, and counteractions;
- f. Weaknesses, counter-countermeasures.
- g. Uniqueness, exclusive knowledge by the United States.
- h. Lead time, which is related to the state-of-the-art.
- i. Surprise, which is related to possession and capability to use.
- j. Specifications, which may be indicative of goals, aims, or achievements.
- k. Manufacturing technology.
- l. Associations with other data or activities.

3-4 Step 4. MAKE INITIAL CLASSIFICATION DETERMINATIONS

Making the analyses outlined in sections 3-2 and 3-3 above, will lead to conclusions on the ways the effort will result in net national advantage, and hence, what it is that requires classification to protect that advantage. Although at this stage of the guide's preparation you are concerned primarily with information relating to the overall effort, consideration must be given to some of the more particular information or data such as that covering performance, capabilities, and possible vulnerabilities and weaknesses. Appendix A has been designed to help in that consideration.

3-5 Step 5. IDENTIFY SPECIFIC ITEMS OF INFORMATION THAT REQUIRE CLASSIFICATION

a. The real heart of a classification guide is the identification and enunciation of the specific details of information warranting security protection. Regardless of the size or complexity of the undertaking that the guide applies to, or the level where the classification guide is issued, there are certain identifiable features of the undertaking that create or contribute to actual or expected national security advantage. There also may be certain critical elements of the undertaking that need to be protected to prevent or make it more difficult for hostile forces to develop or apply timely and effective countermeasures. The problem is to identify and state those special features or critical elements that require protection, and to decide how and why they are related to the net national advantage. Several substeps to this problem of identification of classifiable details are laid out in appendices B and C. The important thing is that the statements of classification in the guide are clear and specific enough to be applied easily and readily in determining which documentation and hardware involved in every phase of the effort, reveals the information requiring protection. Statements as to what information is classified must be as specific as possible to minimize the probability of error by those who will use the classification guide. (See chapter 4 for a complete discussion on classifying hardware items.)

b. It is equally important that you specify precisely and clearly the level of classification to be applied to each item of information identified in the guide. Broad guidance such as "U-S" meaning Unclassified to Secret does not provide sufficient instruction to users of the guide, unless you also delineate the exact circumstances under which each level of classification should be applied. The exact circumstances may be supplied in amplifying comments, for example, "Unclassified ("U") when X is not revealed"; "Confidential when X is revealed;" and "Secret when X and Y are revealed." Failure to do so requires, in effect, that users of the guide make original classification decisions as they attempt to apply your guidance. Keep in mind that you want users of the guide to classify things your way, not their's, and that most users of your guide will not have original classification authority.

3-6 Step 6. DETERMINE HOW LONG CLASSIFICATION MUST CONTINUE

a. Equally important to determinations to classify, are the conclusions as to how long the classification should remain in effect. When a classification determination is made, it is necessary to determine how long the classification shall last. At the conceptual stage of a new effort there may be good reason to classify more information about the effort than will be necessary in later phases. Typically, information loses its sensitivity and importance in terms of creating or contributing to the national advantage. At certain stages in production, or deployment, it may not be practical or possible to protect certain items of information from disclosure. Of course, official public releases have a direct affect on the duration of classification. With these factors, and the content of section 2-3 in mind, proceed with the determination of a declassification date or event for each item of classified information. If such a date or event cannot be determined for a particular item of information, that information will be marked "Originating Agency's Determination Required" or "OADR." State the determinations in direct connection with the item of information to which they pertain. Possibilities include: declassifying on occurrence of an event such as roll-out or the commencement of an operation;

declassifying on a date, e.g., 4 (or 7 or 26) years from the time information originally is classified; or declassifying on "OADR."

b. Use of "Originating Agency Determination Required" or "OADR" must be held to a minimum.

c. Always look at the possibility of providing for automatic downgrading of the classification that is assigned. Future downgrading is an option that is always open when information is originally classified at "S" or "TS" levels. Consider it carefully in every instance, and provide for downgrading at fixed future points in time, or upon the occurrence of specified events when the damage that is expected to result from an unauthorized disclosure will be reduced to a level prescribed for lower classification.

3-7 Step 7. WRITING THE GUIDE

a. Having determined exactly what warrants security classification, it is then necessary to set down in clear, precise language, statements describing which items of information require classification. It is also advisable to include items of information that are unclassified in the particular effort. This is done to assure users of the guide that this information is, in fact, unclassified and was not inadvertently omitted. While there is no mandatory DoD-wide format for security classification guides, the one illustrated in appendix D will be adequate in many applications; consider it first. (Also see appendix E for some format variations.) Place significant words of the guide's title first, for example, "F-5B Aircraft Security Classification Guide."

b. There are a number of administrative requirements for security classification guides. Bear in mind that the security classification guide you are writing must:

(1) State precisely the specific information elements to be protected.

(2) Point out the classification levels "TS," "S," or "C" and any additional markings such as Restricted Data (RD) or Formerly Restricted Data (FRD), that apply to each element of information, or when it will serve a useful purpose, specify that the element of information is unclassified.

(3) Specify the duration of classification of each element of information (except RD and FRD) in terms of declassification indicating a fixed date or foreseeable future event, or, as a last resort, "OADR."

(4) State any downgrading action that is to occur, and when such action is to take place.

(5) Identify the original classification authority who PERSONALLY approved the guide in writing, and who has program or supervisory responsibility over the information addressed in the guide.

c. It is often very useful to include amplifying comments to explain the exact application of classification instructions (see section 3-5.) The comments may be placed in a "Remarks" column opposite the item of information discussed, or they may appear as numbered notes at the end of the guide,

and referenced in the "Remarks" column. The latter method is especially useful when a comment applies to more than one element of information. Quite often, a combination of these two methods will be found best. See appendix D for examples.

d. Finally, bear in mind that your guide may have application to information not yet created. Commonly, guidance is written for application to information already existing. For example, the damaging effects of an electromagnetic pulse (EMP) on an electronic device are known through laboratory testing, and that information is classified because knowledge of it could be used to nullify the electronic system's battlefield effectiveness. However, the EMP effects on a system that has not yet been prototyped may not be known because testing of the system in its vehicle will not take place for at least another 2 years. Nevertheless, classification guidance can be written today for application to this unknown information. Rather than stating declassification in terms of a specific future date, state it in terms of an occurrence of an event, for example, "Declassify 15 years after initial operational capability."

CHAPTER 4

CLASSIFYING HARDWARE ITEMS

4-1 GENERAL

A piece of hardware conveys information about itself or the system of which it is a part just as readily as words printed upon a page. Which is more important to protect, blue prints to a fuse, or the fuse itself?

4-2 HARDWARE CLASSIFICATION CONSIDERATIONS

Hardware items are classified because of the information revealed by the items or obtained from them. The following are some basic considerations.

a. An item of hardware does not necessarily need to be classified simply because it is part of a classified product or effort.

b. Unclassified off-the-shelf items, unless modified in some particular way to make them perform differently, can never be classified even though they constitute a critical element, become an integral part of a classified end product, or produce a properly classified effect. However, the association of otherwise unclassified hardware with a particular effort or product may reveal something classified about that effort or product. Common integrated circuits that control frequencies are notable examples. In such cases it is the association with the effort or product that reveals the classified information, not the circuits themselves. Decisions regarding what aspect of the system to classify may be difficult, but it is necessary to consider the effect of association, and how that association could reveal classified information.

c. Frequently, classified information pertaining to a hardware item can be restricted to the paper work associated with the item. When this is possible, the hardware itself should be unclassified.

d. Unusual, unique, or peculiar uses or modifications of ordinarily available unclassified materials or hardware items may create a classifiable item of information. In another instance, the mere fact of use of a particular material in a particular effort might reveal a classifiable research or development interest. In such cases, it is especially important to accurately identify the classified information in order to determine whether the hardware or material itself reveals this information, or whether it is merely the association or use of the hardware item with a particular effort that reveals it. In the latter case, classification of the hardware itself would not be proper.

e. At some stage in a production effort, production and engineering plans are drawn. Usually a family tree-type diagram is prepared to assist in determining what components, parts, and materials will be required. This diagram supplies a good basis to determine where and when classified information will be involved in the production effort.

f. Another usual step in production engineering is the development of drawings for all the individual elements that go into the final product. These drawings show design data, functions, and specifications, all of which are closely tied in with the items of information that may be classified. From these drawings it is possible to determine exactly which elements of the final product will reveal classified information. It is also possible to determine associations between hardware items that reveal classified information. It is necessary, of course, to determine the classifications, if any, to be assigned to each drawing. Accordingly, a classification team should take part in the production engineering phase to assist in identifying and isolating classification situations.

4-3 USER CONSIDERATIONS

Awareness of the users, and responsiveness to problems are essential in the guide. The following are some considerations.

a. Usually management and staff supervisory personnel need to have a fairly broad knowledge of classification requirements. Farther down the line however, foremen, and other first-line supervisors and below, usually need to know only which hardware items are classified, the appropriate levels of classification, and which items are unclassified. Therefore, as soon as possible in the production planning process, make a listing of all classified hardware items according to part number or other identifier, and when necessary for understanding, a listing of unclassified items. Such a listing will be valuable also to procurement and logistics (shipping, handling, and storage) personnel. The listing should preferably be unclassified, but should be reviewed carefully to ensure that classified information is not revealed by the listing itself, particularly through associations.

b. When planning a production line, careful attention is needed to delay as long as possible the insertion of classified hardware items.

c. Test equipment by itself frequently embodies no classified information, and therefore, requires no classification. When such equipment is used to test tolerances, specifications, performance, and other details that are classified, the equipment would still be unclassified unless it was calibrated or set in such a way as to reveal the classified information pertaining to the item being tested. This is one example of a situation where it may be possible to limit the classified information to the paper work involved and to the test operator's personal knowledge, precluding the necessity for classifying the test equipment itself.

CHAPTER 5

CLASSIFYING MILITARY OPERATIONS INFORMATION

5-1 GENERAL

The security classification of military operations information is subject to many of the considerations described in chapter 3 and appendix C of this Handbook. While there are no hard and fast rules for classification of military operations information, and while each Military Service and command may require a unique approach to operations security (OPSEC), there are basic concepts which can be applied. What must be protected are operational concepts and their applications, and the capabilities, vulnerabilities, and weaknesses of the plan. The element of surprise is essential to military effectiveness in both tactical and strategic operations, and requires the continuous concealment of capabilities and intentions. OPSEC is the principal means of achieving that concealment. All commanders must therefore ensure consideration of OPSEC in every phase of their operations. OPSEC is a command responsibility.

5-2 MILITARY OPERATIONS INFORMATION

Military operations information is defined for the purpose of this Handbook as information pertaining to a strategic or tactical military action, including training, movement of troops and equipment, supplies, and other information vital to the success of any battle or campaign.

5-3 DEFINITIONS OF MILITARY OPERATIONS TERMS

- a. Contingency Plan. A plan for major contingencies that can reasonably be anticipated in the principal geographic subareas of the command or area of responsibility.
- b. Operation Order. A directive issued by a commander to subordinate commanders for the purpose of effecting the coordinated execution of an operation.
- c. Operation Plan. A plan for a single or series of connected operations to be carried out simultaneously or in succession. It is usually based upon stated assumptions, and is the form of directive employed by higher authority to permit subordinate commanders to prepare supporting plans and orders.
- d. Operations Security. The process of denying adversaries information about friendly capabilities and intentions by identifying, controlling, and protecting indicators associated with planning and conducting military operations and other activities.
- e. Emergency Relocation Site. A site located, where practical, outside a prime target area, where all or portions of a civilian or military headquarters may be removed. As a minimum, it is manned to provide for the maintenance of the facility, communications, and data base.
- f. Deployment. Act of extending battalions and smaller units in width, in depth, or in both width and depth to increase its readiness for contemplated action. In naval usage, the change from a cruising approach or contact disposition to a disposition for battle. In a strategic sense, the relocation of forces to desired areas of operation.

g. Mission Essential Material. That material which is authorized and available to combat, combat support, combat service support, and combat readiness training forces to accomplish their assigned missions.

h. Operational Intelligence: Intelligence required for planning and executing all types of operations.

i. National Security Information. Information or material, collectively termed "information," that is owned by, produced for or by, or under control of the U.S. Government, and that has been determined under Executive Order 12356 or prior Executive Orders to require protection against unauthorized disclosure and is so designated.

j. Public Release. Includes, but is not limited to news releases, articles, manuscripts, pamphlets, fact sheets, brochures, displays, still and motion pictures, speeches, and responses to queries from representatives of the public media.

k. War Reserve Data.

(1) U.S. requirements or stocks reflecting days of supply, and the total number of days for which required or authorized.

(2) Equipment or personnel densities to be supported when identified with a theater, or contingency or operations plans.

l. Operational Test and Evaluation. The field test, under realistic combat conditions, of any item of (or key component of) weapons, equipment, or munitions for the purpose of determining the effectiveness and suitability of the weapons, equipment, or munitions for use in combat by typical military users; and the evaluation of the results of such test. OT&E may include the comparative evaluation of a new system and its predecessor or similar systems to determine relative gains in effectiveness or inherent weaknesses.

5-4 MILITARY OPERATIONS CLASSIFICATION CONSIDERATIONS

"Loose lips sink ships." The World War II security awareness slogan was to emphasize the importance of protecting our operational plans. That simple slogan is as true today as it was then.

Today, we must prepare to win the first battle of the next war because the first battle could well be the last battle, and international pressures to stop fighting could bring about early cessation of hostilities.

Successful battle operations depend largely upon our ability to assess correctly the capability and intention of enemy forces at each stage of the battle, and to communicate an effective battle doctrine throughout our forces. Classifiable information would include:

- a. The number, type, location, and strengths of opposing units.
- b. The capabilities and vulnerabilities of weapons in enemy hands, and how he normally applies the weapon.
- c. The morale and physical condition of the enemy force.

OPSEC is the art of applying signal security (SIGSEC), physical security, information security, and deception to deny the enemy knowledge of our operations and activities. OPSEC must be considered both before and during the battle to conceal potentially revealing training, logistical, personnel, and other administrative and support activities. It also includes communications security (COMSEC) and electronic security (ELSEC), avoidance of stereotyped activity patterns, strict control of classified information, and the correct use of camouflage, noise, light, and other countersurveillance techniques.

Counterintelligence and OPSEC must be coordinated and executed concurrently with combat operations. All sources of intelligence must be marshalled to support a mission. For operations security to be its best, it must support the commanders' requirements, and it must be event oriented.

Tactical counterintelligence exists to defeat the enemies' intelligence by shielding our intentions and actions. The enemies' "intentions" must be considered along with their capabilities and probable actions. Operations security supported by tactical counterintelligence is vital for economy of force and for surprise.

Information related to operational plans (whether executed or not, presented in whole or in part), that if disclosed could be expected to cause damage to the United States, must be protected. For example, premature news releases, though innocently conceived, can be very dangerous, and must be avoided. In a hypothetical case, an announcement is made during a large exercise that the Air Force would participate, and that there would be 200-300 aircraft taking part. This alone would be releasable. Because of public concern that an accident could occur however, it was also announced that none of the aircraft would be carrying bombs. The intent was to assure the public that there was no danger to them, and to relieve their minds, but in reality this was vital information to an enemy preparing for a surprise attack.

In considering classification guidance for operations, there may be good reason to classify more information about the operation in the beginning than will be necessary later. Certain elements of information such as troop movements may no longer require protection after a certain date or event. When this point is reached, downgrading or even declassification should be considered.

5-5 DOWNGRADING AND DECLASSIFICATION INSTRUCTIONS

A classification guide should clearly identify the elements of information pertaining to the operational plan for which classification guidance is required. Classification shall continue only so long as unauthorized disclosure would result in damage to national security, which may be an indefinite period of time in the case of unexecuted long range plans.

5-6 ITEMS TO BE CONSIDERED FOR CLASSIFICATION

The following are only examples, and are not valid guidance for any effort. The original classification authority is the classifier.

<u>TOPIC</u>	<u>CLASS.</u>	<u>DECLASS.</u>	<u>REMARKS</u>
a. Overall operational plans.	"S"	OADR	
b. System operational deployment or employment.	"C"	After deployment or employment	
c. Initial Operational Capability (IOC) Date.	"C"	After IOC date	
d. Planned location of operational units.	"S"	After arrival on site	
e. Equippage dates, readiness dates, operational employment dates.	"S"	After these events	
f. Total manpower or personnel requirements for total operational force.	"C"	After operation	
g. Coordinates of selected operational sites.	"S"	After site activation	
h. Specific operational performance data which relates to the effectiveness of the control of forces and data on specific vulnerabilities and weaknesses.	"S"	OADR	
i. Existing OPSEC and COMSEC procedures, projections, and techniques.	"S"	OADR	
j. Target characteristics.	"S"	OADR	

CHAPTER 6

CLASSIFYING INTELLIGENCE INFORMATION

6-1 GENERAL

Intelligence is knowledge. When such knowledge contains or reveals information that, if disclosed, could reasonably be expected to cause damage to national security, the elements are classifiable. To the extent that these elements of knowledge can be identified, defined, categorized, and utilized, they are susceptible to security classification guidance.

6-2 INTELLIGENCE INFORMATION

Intelligence may be divided generally into two categories-counterintelligence and foreign intelligence.

a. Counterintelligence is information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, persons, or international terrorist activities, but not including personnel, physical, document, or communications security programs.

b. Foreign intelligence is information relating to the capabilities, intentions, and activities of foreign powers, organizations, or persons, but not including counterintelligence except for information on international terrorist activities. In other words, it is simply being aware of all the things that one should know in advance of initiating a course of action. Thus, combat intelligence, for example, in anticipation of a military operation, furnishes the commander with all available knowledge on the strength and deployment of the enemy, and on the physical attributes of the battlefield to be. The primary objective is that the commander should know what he will be up against before going into battle.

There are many types of intelligence. Basic, strategic, technical, economic, and political are a few. Some types of intelligence are source-oriented, e.g., human intelligence and signals intelligence; some form oriented as in raw or unfinished intelligence; some system oriented as in electronic or telemetric; some subject oriented as in medical or economic; and some use oriented as in military or tactical.

The intelligence community uses a lexicon that is unique to its field of interest. (See reference (e)). For convenience, definitions of "intelligence source" and "intelligence method" are provided below:

a. Intelligence Source. A person or technical means providing intelligence.

b. Intelligence Method. Any process, mode of analysis, means of gathering data, or processing system or equipment used to produce intelligence.

6-3 INTELLIGENCE CLASSIFICATION CONSIDERATIONS

As long as timing and surprise are essential aspects of policy and strategy, there must be secrecy. For example, a quarterback who inadvertently reveals the play, or a pitcher who cannot conceal the pitch is likely not to be the winner. However, security classification should not become an end in itself. Classification may be likened to armor, one can pile on the armor until the man inside is absolutely safe--and absolutely useless. Producers of intelligence must be wary of applying so much security that they are unable to provide a useful product to their consumer. Consequently, an intelligence product should be classified only when its disclosure could reasonably be expected to cause some degree of damage to national security. The following are some basic considerations, but they should not be construed as being all-inclusive:

a. In general, resource information should not be classified unless it reveals some aspect of the intelligence mission, and its revelation would jeopardize the effectiveness of a particular function. An example of classifiable resource information is the intelligence contingency fund.

b. Intelligence concerning foreign weapons systems may be classified based on what is generally known about a particular system or its components. Normally, the less that is publicly known about a particular system or component, the higher its level of classification.

c. Intelligence identifying a sensitive source or method is classified, as well as the evaluation of the particular source or method.

d. Intelligence which does not identify or reveal a sensitive source or method is usually not classified unless the information contains other classified information such as intelligence activities including intelligence plans, policies, or operations.

e. Intelligence that reveals the identity of a conventional source or method normally does not require classification. However, if the information is communicated to the Department of Defense by a foreign government under a government-to-government agreement, it must be protected at the level and for the length of time the transmitting government desires. If the information is obtained from a conventional source or method, and the information is provided freely without any agreement or other restriction, expressed or implied, the classification, if any, should be based solely on the content of the information provided.

f. Intelligence that reveals the identification of all known and possible enemy capabilities to collect and exploit information from a given or similar operation is classified. This threat would include known enemy intelligence collection and analysis capabilities, efforts, and successes. An integral part of these data is an assessment of enemy human intelligence, signals intelligence, and reconnaissance satellite capabilities.

-
- g. Security classification assigned to intelligence received from non-Defense sources must be respected by Defense users.
- h. An intelligence estimate is normally classified since it contains sensitive sources, methods, or raw or evaluated intelligence.
- i. An intelligence requirement is classified when it reveals what is not known, what is necessary to know, and why. Moreover, the requirement may recommend a sensitive source or method, other military intelligence required, or contain technical and operational characteristics of classified weapons systems.
- j. The classification of relationships with foreign intelligence organizations is related to the following considerations:
- (1) Normally, the fact of broad, general intelligence cooperation with foreign countries or groups of countries with which the United States maintains formal military alliances or agreements (e.g. NATO) is not classified.
 - (2) The fact of intelligence cooperation between the United States and a specific governmental component in an allied country, or general description of the nature of intelligence cooperation between the United States and any allied country may be classified. The fact of intelligence cooperation between the United States and specifically named countries or their governmental components with which the United States is NOT allied is always classified.
 - (3) Details of or specifics concerning any intelligence exchange agreement are classified. In some instances, the mere fact of such an agreement may be classified.
 - (4) The identities of foreign governmental or military personnel who provide intelligence under such agreements or liaison relationships may be classified.
- k. Information that reveals counterintelligence activities, identities of undercover personnel or units or clandestine human agents, methods of operations and analytical techniques for the interpretation of intelligence data is classified.
- l. Cryptologic information (including cryptologic sources and methods) is classified.
- m. Information concerning electronics intelligence, telemetry intelligence, and electronic warfare is usually classified.
- n. The intelligence community normally considers the following categories of information to be classified:
- (1) Cryptologic, cryptographic, signals intelligence, or imagery intelligence.
 - (2) Counterintelligence.
-

-
- (3) Special access programs.
 - (4) Information which identifies clandestine organizations, agents, sources, or methods.
 - (5) Information on personnel under official or nonofficial cover, or revelation of a cover arrangement.
 - (6) Covertly obtained intelligence reports and the derivative information which would divulge intelligence sources or methods.
 - (7) Methods or procedures used to acquire, produce, or support intelligence activities.
 - (8) Intelligence organizational structure, size, installations, security, objectives, and budget.
 - (9) Information that would divulge intelligence interests, value, or extent of knowledge on a subject.
 - (10) Training provided to or by an intelligence organization which would indicate its capability or identify personnel.
 - (11) Personnel recruiting, hiring, training, assignment, and evaluation policies.
 - (12) Information that could lead to foreign political, economic, or military action against the United States or its allies.
 - (13) Events leading to international tension that would affect U.S. foreign policy.
 - (14) Diplomatic or economic activities affecting national security or international security negotiations.
 - (15) Information affecting U.S. plans to meet diplomatic contingencies affecting national security.
 - (16) Nonattributable activities conducted abroad in support of U.S. foreign policy.
 - (17) U.S. surreptitious collection in a foreign nation that would affect relations with the country.
 - (18) Covert relationships with international organizations or foreign governments.
 - (19) Information related to political or economic instabilities in a foreign country threatening American lives and installations there.
 - (20) Information divulging U.S. intelligence and assessment capabilities.
-

-
- (21) United States and allies' defense plans and capabilities that enable a foreign entity to develop countermeasures.
 - (22) Information disclosing U.S. systems and weapons capabilities or deployment.
 - (23) Information on research, development, and engineering that enables the United States to maintain an advantage of value to national security.
 - (24) Information on technical systems for collection and production of intelligence.
 - (25) U.S. nuclear programs and facilities.
 - (26) Foreign nuclear programs, facilities, and intentions.
 - (27) Contractual relationships that reveal the specific interest and expertise of an intelligence organization.
 - (28) Information that could result in action placing an individual in jeopardy.
 - (29) Information on secret writing when it relates to specific chemicals, reagents, developing, and microdots.
 - (30) U.S. Military space programs.

6-4 INTELLIGENCE DISSEMINATION AND DECLASSIFICATION CONSIDERATIONS

Intelligence often must be classified for the required period of time to protect the source which would be rendered useless if revealed. Nevertheless, intelligence that is critical to an understanding of our national policy should be disseminated as soon as national security permits, and in as much detail as feasible, while not compromising our collection capability. Careful consideration should be given to the question: To what extent could public knowledge and international sharing of information gathered benefit our national objectives? Don't automatically presume that intelligence requires such special treatment that it is exempt from the rules that govern ALL classified information. Normally, intelligence will remain classified for a longer duration than other types of classified information, but still only as long as is necessary to protect a certain source or method. The outline in section 3-6 of this Handbook on determining how long classification must continue is equally applicable to all information, including intelligence.

6-5 SPECIAL MARKINGS

Reference (f) prescribes special control markings to be used only for intelligence information under certain circumstances. Other control system markings are authorized.

6-6 CLASSIFICATION GUIDE ILLUSTRATIONS

The treatment of Classifying Details (appendix B) and Recommended Format for a Security Classification Guide (appendix D) are applicable to the development of an intelligence guide. Regarding intelligence information, the following example contains security classification guidance on Human Intelligence (HUMINT). (Remember, it is only an example, and is not valid guidance for any effort.)

<u>TOPIC</u>	<u>CLASS.</u>	<u>DECLASS.</u>	<u>REMARKS</u>
<u>HUMINT Collection Operations</u>			
a. Biographic information taken exclusively from open sources, and where no intelligence connection is shown.	"U"		
b. Positive identification of an individual as a potential source to a U.S. intelligence agency.	"S"	OADR	"TS" if identified as an actual source
c. Identity of a target installation or target personality when not linked to a specific collection operation.	"S"	OADR	"TS" when linked to an actual source or specific collection operation
d. Interest in specific events for collection exploitation, including specific areas of technology.	"S"	OADR	
e. Names of collection agency case officers in conjunction with a specific collection operation.	"C"	OADR	
f. Information on collection agency HUMINT policy plans, resources methods or accomplishments.	"S"	OADR	

CHAPTER 7
CLASSIFYING FOREIGN RELATIONS INFORMATION

7-1 GENERAL

The singular problem in writing classification guidance for foreign relations information arises from the everchanging politics between nations. These relationships have a profound influence on classification determinations. Rapid dramatic changes in foreign relations are often accompanied by rapid dramatic changes in the classification of elements of information. Nevertheless, there are consistent standards that can and should be applied.

7-2 FOREIGN RELATIONS INFORMATION

a. Foreign relations are the connections between nations. International relations consist of that information which pertains to the political, military, and economic relationships between countries and international organizations. Foreign affairs refers to matters having to do with international relations. For the purpose of this Handbook, all shall be considered "foreign relations."

b. In the context of foreign relations information, foreign government information can have an impact on the development of security classification guidance. Foreign government information consists of:

1. Documents or material provided by a foreign government or governments, international organization of governments, or any element thereof in the expectation, expressed or implied, that the document, material, or the information contained therein is to be held in confidence.

2. Documents or material originated by the United States that contain classified information provided, in any manner, to the United States by foreign governments, international organizations of governments, or elements thereof, with the expectation, expressed or implied, that the information will be held in confidence.

3. Classified information or material produced by the United States under or as a result of, a joint arrangement, evidenced by an exchange of letters, memorandum of understanding, or other written record, with a foreign government or organization of governments requiring that the information, the arrangement, or both be kept in confidence.

7-3 FOREIGN RELATIONS CLASSIFICATION CONSIDERATIONS

a. Although standards of what is harmful to national security vary with the international situation and are responsive to changes in foreign policy, classification guidance cannot be shifted and changed with the sleight of a shell man's hand--now you see it; now you don't. The mechanisms involved in foreign relations most often effect gradual, not sudden change. Normally, there are too many people and too many institutions involved for sudden, drastic shifts.

b. The Department of State (DoS) is the agency responsible primarily for the development and execution of the foreign policy of the United States. Also, it is the agency that has the primary responsibility for security classification of foreign relations information. For this reason, most Defense classification determinations in the area of foreign relations will be derivative in nature. Nevertheless, many Defense projects and programs involve foreign relations information for which security classification guidance must be developed.

c. The following are some of the types of information or material involving foreign relations that warrant classification consideration:

1. All material that reveals or recommends U.S. Government positions or options in a negotiation with a foreign government or group of governments, or that comments on the merits of foreign government positions in such negotiations.

2. All material that comments on the quality, character, or attitude of a serving foreign government official, whether elected or appointed, and regardless of whether the comment is favorable or critical. Illustrations of the types of information covered in this category are records revealing:

(a) A foreign official speaking in a highly critical manner of his own government's policy.

(b) A foreign official suggesting how pressure might effectively be brought to bear on another part of his own government.

(c) A foreign official acting in unusually close concert with U.S. officials where public knowledge of this might be harmful to that foreign official.

(d) A foreign official whose professional advancement would be beneficial to U.S. interests, especially if any implication has been made of U.S. efforts to further his advancement, or if public knowledge of this might place the person or his career in jeopardy.

3. All unpublished, adverse comments by U.S. officials on the competence, character, attitudes, or activities of a serving foreign government official.

4. All material which constitutes or reveals unpublished correspondence between heads of state or heads of government.

5. Statements of U.S. intent to defend, or not to defend, identifiable areas, or along identifiable lines, in any foreign country or region.

6. Statements of U.S. intent to attack militarily in stated contingencies, identifiable areas in any foreign country or region.

7. Statements of U.S. policies or initiatives within collective security organizations, e.g., NATO.

8. Agreements with foreign countries for the use of, or access to, military or naval facilities.

9. Contingency plans insofar as they involve other countries, the use of foreign bases, territory, or airspace; or the use of chemical, biological, or nuclear weapons.

10. Defense surveys of foreign territories for purposes of basing or using in contingencies.

11. Statements relating to any use of foreign bases not authorized under bilateral agreements.

d. DoD officials, when involved with the kind of information or material described in paragraphs 1. through 11., above, may find coordination with the DoS's Classification/Declassification Center in the Bureau of Administration useful before issuance of a DoD security classification guide.

e. Unless the foreign government or international organization of governments specifies or agrees to an earlier date for declassification, classified information would be declassified upon notice by the foreign government or international organization of governments (OADR).

7-4 CLASSIFICATION GUIDE ILLUSTRATIONS

The treatment of Classifying Details (Appendix B) and Recommended Format for a Security Classification Guide (Appendix D) are applicable to the development of a foreign relations security classification guide. In the context of foreign relations information, let's see how foreign government information can have an impact on the development of classification guidance.

a. A DoD Component is involved in negotiating some arrangement with country "X." In the process of the negotiations, the foreign counterpart states that his country does not want discussion on the subject to become public knowledge. At the same time, the foreign official makes it clear that his country has announced publicly its intention to seek U.S. views on the subject of the discussions.

b. The nature of business being discussed is such that the United States would not require protecting the discussions from public disclosure. Moreover, the subject matter is one that would not be ordinarily classified. The DoD Component however, does classify the notes and transcripts pertaining to the discussion because of the expressed wishes of the foreign government. The information fits the definition of foreign government information. Thus, a classification guide on the subject might contain the following topics:

(Remember, the following are only examples, and are not valid guidance for any effort.)

<u>TOPIC</u>	<u>CLASS</u>	<u>DECLASS.</u>	<u>REMARKS</u>
1. Apple orchard negotiations with country "X."	"U"		Mere fact of negotiations only, any elaborations may be classified; see Topic 2.
2. Transcripts of apple orchard negotiations and substantive notes pertaining to them.	"C"	OADR	Classified at request of country "X."

c. The foregoing scenario illustrates a brief classification guide involving the foreign relations of the United States as well as foreign government information. The guide could not have been written until after the opening of the negotiations at which point the foreign official made known the two critical elements of information. In anticipation that the negotiations will involve a large number of personnel from several U.S. agencies and will last several years, a classification guide such as this one, brief as it is, can serve a very useful purpose.

d. To illustrate a scenario with military implications, let's presume that two countries in Europe have secretly granted the United States permission to fly over their territory, but only at high (50,000 feet) altitudes. One of the countries ("Y") indicated that serious damage would occur to our relations if the information became public while the other ("Z") indicated that it did not want the information to be in the public domain. A classification guide topic might read as follows:

(Remember, the following are only examples and are not valid guidance for any effort.)

<u>TOPIC</u>	<u>CLASS</u>	<u>DECLASS.</u>	<u>REMARKS</u>
3. (U) Fact of U.S. over-flights - Europe			
a. (S) Country "Y"	"S"	OADR	(S) Must be at least 50,000 feet altitude; lower flights not permitted in "Y" and "Z."
b. (C) Country "Z"	"C"	OADR	
c. (U) Other European Countries	"U"		

e. Note that in the context of our example, the above guidance would be classified as indicated.

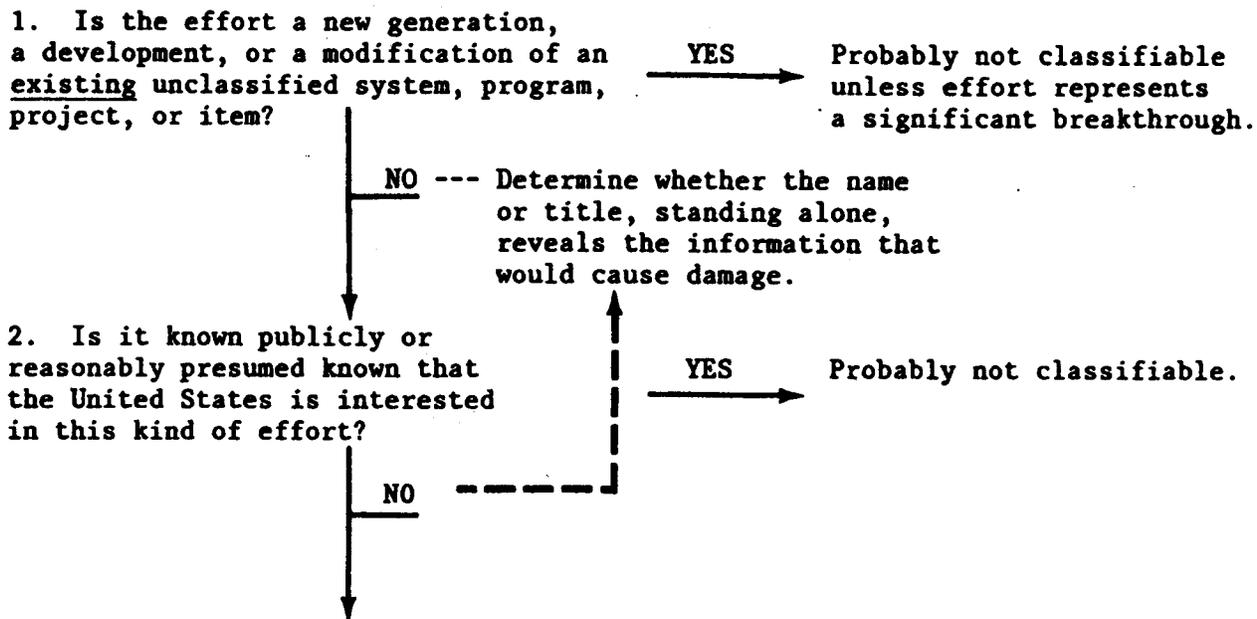
APPENDIX A
INITIAL CLASSIFICATION DETERMINATIONS
(See section 3-4.)

STEP ONE
(appendix A) In making the initial classification determinations broadly pertaining to the overall effort, certain factors should be considered. Such factors are whether the effort is an outgrowth of a classified or an unclassified previous effort, whether U.S. interest in the effort is publicly known, and whether knowledge of U.S. interest in the effort would adversely affect our national security in some way.

STEP TWO
(appendix B) Regardless of whether you determine in Step One that your overall effort is classified, you should consider also classifying certain specific details of the effort. Specific details include such things as performance, capability, uniqueness, lead time, vulnerability, specifications, and manufacturing technology.

STEP THREE After the first two steps are accomplished and determinations made that certain aspects of the overall effort or specific details are classified, the final step is to consider whether the information can be effectively protected and for how long.

The following questions, answers, and potential actions will assist in systematically reviewing the fundamental considerations of Step One in deciding whether certain broad aspects of the overall effort warrant security classification.



3. Is the exact extent of U.S. interest known or reasonably surmised from openly available information?

YES

Probably not classifiable.

NO---Determine what information would reveal the degree of attainment by the U.S. in the particular field, and how that would be of value to a foreign interest in planning actions detrimental to national security.

4. Is the REASON for U.S. interest known or reasonably surmised from openly available information?

YES

Probably not classifiable.

NO---Determine what information would reveal purpose, goal, or mission of the effort that would cause the actual damage.

5. Would knowledge of U.S. interest in this effort cause or worsen foreign political, economic, or military tensions to the detriment of U.S. national security?

YES

Classifiable. The level of classification would be based on the degree of damage to national security.

NO---Not classifiable.

6. Would unauthorized knowledge, magnitude, or mere fact of the overall effort have a detrimental effect on U.S. national security?

YES

Classifiable. The level of classification would be based on the degree of damage to national security.

NO---Not classifiable.

7. Would the fact of U.S. interest or accomplishment in the effort:

(a) Spur foreign interests in a similar effort that would be detrimental to the United States?

(b) Spur foreign interests to develop countermeasures which could diminish U.S. advantage?

(c) Spur foreign interests in military or political action against the United States or an ally?

(d) Provide foreign interests with propaganda capable of damaging U.S. national security?

(e) Eliminate or significantly diminish required lead time or a valuable element of surprise related to national security?

(f) Indicate to foreign interests a lag or failure by the United States to pursue or attain a necessary or expected competence in a particular field related to national security?

YES

Classifiable. The level of classification would be based on the degree of damage to national security.

NO---Not classifiable.

NOW CONSIDER CLASSIFYING SPECIFIC DETAILS OF THE EFFORT (APPENDIX B).

APPENDIX B
CLASSIFYING DETAILS--CONSIDERATIONS*
(See section 3-5.)

Having considered the factors involved in making classification determinations broadly concerning the overall effort, it is now necessary to take the second step and consider the classification of certain specific details of the effort. Providing answers to the following questions will assist in systematically reviewing the details of the effort in deciding whether or not certain specific aspects of the effort warrant security classification. A listing identifying specific items of information to consider is contained in appendix C.

B-1 PERFORMANCE OR CAPABILITY

- a. What will this do (actual or planned) that is more, better, faster, or cheaper (in terms of all kinds of resources) than anything like it?
- b. How does this degree or kind of performance contribute to or create a national security advantage? How much of an advantage?
- c. How long can this data be protected? The advantage?
- d. How would knowledge of these performance details help an enemy, or damage the success of this effort?
- e. Would statement of a particular degree of ATTAINED performance or capability be of value to hostile intelligence in assessing U.S. capabilities? In spurring a foreign nation to similar effort, or in developing or planning countermeasures or counteraction?

B-2 UNIQUENESS

- a. What information pertaining to this effort is known or believed to be the exclusive knowledge of the United States?
- b. Is it known or reasonable to believe that other nations have achieved a comparable degree of success or attainment?
- c. What information, if disclosed, would result in or assist other nations in developing a similar item or arriving at a similar level of achievement?
- d. In what way or ways does the uniqueness of this item contribute to a national security advantage?
- e. In what way or ways has the end product of this effort or any of its parts been modified, developed, or applied so as to be unique to this kind of effort? How unique is this?

*Not prioritized

f. Is the method of adaptation or application of the end product or any of its parts the source of the uniqueness and a national security advantage? In what way or ways? Is it in itself a unique adaptation or application in this kind of effort?

B-3 TECHNOLOGICAL LEAD TIME

- a. How long did it take to reach this level of performance or achievement?
- b. How much time and effort have been expended? Was this a special concerted effort, or only a gradual developmental type of activity?
- c. If all or some of the details involved in reaching this stage of development or achievement were known, how much sooner could this goal have been reached? WHICH details would contribute materially to a shortening of the time for reaching this goal? Can these details be protected? For how long?
- d. Have other nations reached this level of development or achievement?
- e. Do other nations know how far we have advanced in this kind of effort?
- f. Would knowledge of this degree of development or achievement spur a foreign nation to accelerate its efforts to diminish our lead in this field? What details of knowledge would be likely to cause such acceleration?
- g. How important, in terms of anticipated results, is the lead time we think we have gained?
- h. What national security advantage actually results from this lead time?
- i. How long is it practical to believe that this lead time will represent an actual advantage?
- j. How long is it practical to expect to be able to protect this lead time?

B-4 SURPRISE

- a. Do other nations know we have reached this level of development or achievement?
- b. Will operational use of the end item of this effort give us an immediate advantage that would be less or lost if it were known that we have achieved this particular goal?
- c. What is the nature of the advantage resulting from surprise use of this end item?
- d. When will this element of surprise be lost?

B-5 VULNERABILITIES AND WEAKNESSES

- a. What are the weak spots in this effort that make it vulnerable to failure? What is the rate or effect of this failure?

b. How will failure of the effort in whole or in part affect the national security advantage expected upon completion of this effort, or use of the resulting end item?

c. What elements of this effort are subject to countermeasures or counteraction?

d. How would knowledge of these vulnerable elements assist in planning or carrying out countermeasures or counteraction?

e. Can information concerning these weak or vulnerable elements be protected from unauthorized disclosure? Or are they inherent in the system?

f. Can these weaknesses or vulnerabilities be exploited to reduce or defeat the success of this effort? How could this be done?

g. What measures are planned or have been taken to offset these weaknesses or vulnerabilities?

h. Are the counter-countermeasures obvious? Special? Unique? Unknown to outsiders or other nations?

i. How would knowledge of these counter-countermeasures assist in carrying out or planning new countering efforts?

j. Would knowledge of specific performance capabilities assist in developing or applying specific countermeasures or counteractions? How? What would be the effect on the expected national security advantage?

B-6 SPECIFICATIONS

a. What details of specifications would reveal:

(1) A special or unusual interest that contributes to the resulting or expected national security advantage?

(2) Special or unique composition that contributes to the resulting or expected national security advantage?

(3) Special or unique levels of performance that are indicative of a classifiable level of achievement or goal?

(4) Special, or unique use of certain materials that reveals or suggests the source of a national security advantage?

(5) Special or unique size, weight, or shape that contributes to the resulting or expected national security advantage?

b. Are any specification details in themselves contributory to the resulting or expected national security advantage? How?

c. Can details of specifications be protected? For how long?

B-7 CRITICAL ELEMENTS

- a. What are the things that really make this effort work?
- b. Which of these critical elements contribute to the resulting or expected national security advantage? How? To what extent?
- c. Are these critical elements the source of weakness or vulnerability to countermeasures or counteraction?
- d. What details of information pertaining to these critical elements disclose or reveal the national security advantage? Weakness or vulnerability to countermeasures or counteraction?
- e. Can details of information pertaining to these critical elements be protected by classification? For how long?

B-8 MANUFACTURING TECHNOLOGY

- a. What manufacturing methods, techniques, or modes of operation were developed to meet the requirements of this effort? To make the desired end product?
- b. Which of these manufacturing innovations are unique to this effort or this product? Are they generally known or suspected?
- c. Are these manufacturing innovations essential to successful production of the product?
- d. Could the desired result be obtained without these innovations?
- e. What kind of lead time results from these innovations?

B-9 ASSOCIATIONS

- a. Are there any associations between this effort and others that raise classification questions?
- b. Are there associations between information in this effort, and already publicly available information (unclassified), that raise classification problems?
- c. Is it necessary or possible to classify items of information in this effort because their association with other unclassified or classified information would diminish or lose a national security advantage?

B-10 PROTECTABILITY

- a. Can the information effectively be protected from unauthorized disclosure by classification? For how long?
- b. If not, what alternative means can be used to ensure protection?

APPENDIX C
CLASSIFYING DETAILS - ITEMS OF INFORMATION
(See section 3-5.)

The following are items of information that may disclose present or future strategic or tactical capabilities and vulnerabilities. The need for classification of the kinds of information listed during a particular phase or time period should be considered when preparing classification guidance. The listing is not all inclusive nor completely applicable in every instance.

PERFORMANCE AND CAPABILITIES

Accuracy	Payload
Alert time	Penetration
Altitude	Range (range scales)
Maximum	Rate of fire
Optimum	Reaction time
Ballistics	Reliability/failure rate data
Initial	Resolution
Terminal	Response time
Control	Sensitivity
Countermeasures (proven, unproven)	Sequence of events
Counter-Countermeasures	Signature characteristics
Decoys	Acceptance
Electronic	Analysis
Penetration aids	Distinguishment
Shield materials	Identification
Depth/height (also of burst)	Speed/velocity
Maximum	Acceleration/deceleration
Optimum	Cruise
Duration (flight)	Intercept
Effectiveness	Landing
Frequencies (bands, specific, command, operating, infrared, microwave, radio, comsec)	Maximum
	Minimum
	Optimum
Heating	Stability
Impulse	Target data
Intercept	Details
Lethality/critical effects	Identification
Lift	Illumination
Limitations	Impact predicted
Maneuverability	Preliminary
Military Strength	Priority
Actual	Range determination
Planned, predicted, anticipated	Thresholds
Miss distance	Thrust
Noise figure	Toxicity
Operational readiness time cycle	

SPECIFICATIONS
(Detailed, Basic, Subsidiary)

Balance	Loading/loads
Burn rate	Mass factor (propellant)
Capacity (system)	Moment of inertia
Center of gravity	On-station time
Codes	Output data
Composition	Payload
Configuration/contour	Power requirements
Consumption	Purity
Energy requirements	Size, weight, shape
Specific	Stability (static, dynamic)
Total	Strength of members, frames
Filler	Stresses
Fineness	Thickness
Grain configuration	Tolerance
Hardness, degree	Type
Input data	

VULNERABILITY

Countermeasures/counter-countermeasures	Signature characteristics
Dynamic pressure (supersonic)	Acoustic
EMP (radiation)	Electrical
Ground or air shock	Infrared
Jamming	Magnetic
	Pressure
	Radar
	Static overpressure

PROCUREMENT AND PRODUCTION

Completion date or dates	Progress/schedules (milestones)
Numbers	Stock density
(a) Dispersion (numbers per unit of force)	Supply plans and status
(b) On hand--stockpile	Tactical deployment
(c) Planned or programmed (totals scheduled)	
(d) Rate of delivery or production	
(e) Requirements	
(f) Spares	

OPERATIONS

Countdown time	Plans
Deployment data	Command and control
Environment	Results
Location	Analysis, conclusions, reports
Numbers available	Sequence of events
Objectives	Staging techniques
Mission or program	Statement/Concept
Specific or general	Tactical
Tests, broad or detailed	Build-up, units per force, activation dates, personnel

**APPENDIX D
RECOMMENDED FORMAT FOR A SECURITY CLASSIFICATION GUIDE**

This appendix illustrates format for a security classification guide; the balance of the appendix is devoted to that purpose.

(A cover page is recommended showing essentially the following:)

(PROGRAM, PROJECT, SYSTEM, OR STUDY)

SECURITY CLASSIFICATION GUIDE

(If necessary, show a name, program or project number
or some other short form identification, unclassified.)

(DATE)

ISSUED BY: Name and address of issuing office.

APPROVED BY: Original Classification Authority.

(Statement of supersession of any previous guides.)

(Distribution Limitation Statement for Defense Technical Information Center)

PROGRAM, PROJECT, SYSTEM (ETC.) SECURITY CLASSIFICATION GUIDE

Date

SECTION 1

GENERAL INSTRUCTIONS

1. Purpose. To provide instructions and guidance on the classification of information involved in (name, program or project number, study, etc.; using an unclassified identification of the effort covered).
2. Authority. This guide is issued under authority of (state any applicable departmental or agency regulations authorizing or controlling the issuance of guides, such as DoD 5200.1-R, "Information Security Program Regulation"). Classification of information involved in (identification of the effort) is governed by, and is in accordance with, (cite any applicable classification guidance or guides under which this guide is issued). This guide constitutes authority, and may be cited as the basis for classification, regrading, or declassification of information and material involved in (short form identification of the effort). Changes in classification required by application of this guide shall be made immediately. Information identified as classified in this guide is classified by (complete title or position of classifying authority).

Tailor this section to conform to the circumstances of each individual effort.

3. Office of Primary Responsibility (OPR): This guide is issued by, and all inquiries concerning content and interpretation should be addressed to:

(name, code, if any, and mailing
address of issuing office)

(An administrative or security office in the issuing activity may be identified instead. Inclusion of the action officer's name and phone number is desirable.)

4. Classification Recommendations: If the security classifications contained in this guide impose requirements that are impractical, or if current conditions, changes, or progress, scientific, or technological changes in the state-of-the-art, or any other contributory factors indicate a need for changes in this guide, completely documented and justified recommendations should be made through appropriate channels to the OPR. Pending final decision, the items of information involved shall be handled and protected at the higher of the current classifications or the recommended changes. All users of this guide are encouraged to assist in improving and maintaining the currency and adequacy of this guide.
5. Application, Reproductions, and Dissemination: Authority is granted to make reproductions, and take extracts or selected portions of this guide for application by specified groups involved in (identification of the effort), including industrial activities.

NOTE: If it is necessary to classify the guide, you may have to modify this paragraph to express any required limitations. It is important to note that it may be possible to issue unclassified guidance covering parts of the effort, or to select and state classifications without including classified data.

Copies of separate guides issued to operating activities in application of this guide shall be sent to the OPR.

6. **Public Release:** The fact that this guide shows certain details of information to be unclassified does not allow automatic public release of them. Proposed public disclosures of unclassified information regarding (identification of effort) shall be processed through appropriate channels for approval for publication.

NOTE: It may be desirable to indicate the office to which requests for public disclosure are to be channeled.

7. **Foreign Disclosure:** Any disclosure to foreign officials of information classified by this guide shall be in accordance with the procedures set forth in (identify applicable issuances implementing DoD foreign disclosure policy). If a country with which the Department of Defense has entered into a reciprocal procurement memorandum of understanding or offset arrangement expresses an interest in this effort, a foreign disclosure review should be conducted prior to issuance of a solicitation. If it is known that foreign participation cannot be permitted because of the sensitivity of the effort, this fact should be stated.

8. **Definitions:**

NOTE: Include in this paragraph the definitions of any terms for which there may be various meanings to ensure common understanding of the details of information that are covered by the guide.

SECTION 2

OVERALL EFFORT

9. **Identification:** Include in this paragraph any necessary statements explaining the classifications, if any, to be assigned to various statements prescribed for identifying the effort.

10. **Goal, Mission, Purpose:**

NOTE: Include in this paragraph any necessary statements identifying information concerning the purpose of the effort that can be released as unclassified and that must be classified. Take care to ensure that such unclassified statements do not REVEAL classified information.

11. End Item:

NOTE: Include in this paragraph statements of the classifications to be assigned to the end products of the effort, whether paper-work or hardware. In this connection it is important to distinguish between classifications required to protect the fact of the existence of a completed end item, and classifications required because of what the end items contain or reveal. In some instances classified information pertaining to performance, manufacture, or composition of incorporated parts or materials is not ascertainable from mere use of or access to the end item. In others, the classifiable information is that which concerns total performance, capabilities, vulnerabilities, or weaknesses of the end item itself, rather than of any parts or materials.

SECTION 3

PERFORMANCE AND CAPABILITIES

This section includes characteristics of performance and capability of an end item, or an end item's component, part, or material, the performance or capabilities of which require classification. However, such general characteristics that often require classification, such as speed, range, sensitivity, etc., may be unclassified in your effort. The status of these characteristics should be made clear.

NOTE: In this section, provide in sequentially numbered items, statements that express details of performance and capabilities, planned and actual. Include both those elements that warrant classification and those that frequently require classification, but are unclassified in this particular effort. These statements normally would not set forth the numeric values that indicate degree of performance or capability, planned or attained, but merely should identify the specific elements of performance or capability that are covered. When it is necessary to state certain limiting figures above or below which classification is required, the statement itself may warrant classification. For clarity, continuity, or ease of reference it may be desirable to include performance classification data in the sections dealing with the end item or the components or parts to which the performance data apply. Use a "Remarks" column for explanations, limitations, special conditions, associations, etc.

(Remember, the following are only examples, and are not valid guidance for any effort.)

<u>TOPIC</u>	<u>CLASS.</u>	<u>DECLASS.</u>	<u>REMARKS</u>
1. Range			
a. Actual	"S"	15 Jun 95	
b. Planned	"U"		
2. Accuracy/range rate			
a. Predicted	"C"	30 Jan 95	
b. Measured	"C"	30 Jan 95	
3. Altitude--Operational	"C"	30 Jan 95	
Maximum	"C"	30 Jan 95	The statement "in excess of 50,000 feet" is "U."
4. Receiver sensitivity, selectivity, and frequency coverage.	"S"	15 Apr 05	If standard commercial receivers are used, their characteristics are "U" but their application to this effort shall be "S."
5. Resolution--thermal			
a. Maximum attainable	"S"	15 Apr 01	Planned or actual attained thermal resolutions above 0.25 degrees C. are "U."
b. Operational optimum	"S"	15 Apr 01	
c. Operational attainment	"S"	15 Apr 01	
6. Speed			
a. Maximum	"S"	15 Jan 95	Downgrade to "C" upon IOC.
b. Rate of climb	"S"	15 Jan 95	Reference to "supersonic speed" is "U."
c. Intercept	"S"	15 Jan 95	

SECTION 4

SPECIFICATIONS

This section includes items of information describing standards for qualities of materials and parts; methods or modes of construction, manufacture or assembly; and specific dimensions in size, form, shape, and weight, that require classification because they are contributory to the national security advantage resulting from (identification of this effort), or which frequently require classification but are unclassified in (identification of this effort). Classification of specifications pertaining to performance capability are covered in section 3.

NOTE: In this section provide as sequentially numbered items, statements that express details of specifications that warrant classification, and those that frequently are classified, but are unclassified in this effort. In this case, actual figures do not need to be given, merely statements identifying clearly the specific items of information involved. If figures are necessary to establish classification levels, it may be necessary to classify the statements themselves. When necessary for clarity, continuity, or ease of

reference, specification classification data may be included in sections on the end product or components or parts to which the data apply. Use a "Remarks" column for explanations, limitations, special conditions, associations, etc.

(Remember, the following are only examples, and are not valid guidance for any effort):

<u>TOPIC</u>	<u>CLASS.</u>	<u>DECLASS.</u>	<u>REMARKS</u>
1. Burn rate	"C"	17 Sep 93	
2. Power requirement.	"S"	17 Sep 93	Only when associated with advanced model ##; otherwise "U."
3. Chemical composition.	"U"		

SECTION 5

CRITICAL ELEMENTS

This section is used only if there are specific elements that are critical to the successful operation of the end item of this effort, and are unique enough to warrant classification of some data concerning them. Provide in sequentially numbered paragraphs each significant item of information peculiar to these critical elements and the classifications applicable. Also include in this section the classifications to be assigned to information pertaining to components, parts, and materials that are peculiar and critical to the successful operation of the end item of this effort when such items of information are the reason for or contribute to the national security advantage resulting from this effort. Performance data pertaining to such critical elements may be included in this section instead of section 3.

SECTION 6

VULNERABILITIES AND WEAKNESSES

This section is used to specify classifications to be assigned to details of information that disclose inherent weaknesses that could be exploited to defeat or minimize the effectiveness of the end product of this effort. Classifications assigned to details of information on countermeasures and counter-countermeasures should be included in this section.

SECTION 7

ADMINISTRATIVE DATA

This section is used only if particular elements of administrative data, such as program information, procurement schedules, production quantities, schedules, progress, or status of the effort, and data on shipments, deployment, or transportation and manuals (field, training, etc.) warrant classification.

Particular care must be exercised when considering whether there is realistic need for classification of such information. Include in this section items of information relating to the above types of administrative data requiring classification and items that are frequently classified, but are unclassified in the particular effort.

(Remember, the following are only examples, and are not valid guidance for any effort.)

<u>INFORMATION</u> <u>REVEALING</u>	<u>CLASS.</u>	<u>DECLASS.</u>	<u>REMARKS</u>
1. Planned delivery rate.	"C"	13 Mar 90	See item 3, below.
2. Actual routing of delivery of end items.	"C"	See remarks.	Classify upon selection of route, and declassify upon completion of last delivery to site.
3. Shipping dates and times.	"C"	See remarks.	Classify upon decision to ship, and declassify upon arrival at site.

SECTION 8

HARDWARE

The degree of specificity to be included in this section will depend largely upon:

a. The level from which issued. When issued from a headquarters level, probably the only classification to be applied to hardware would be to the end item itself.

b. The channels or hands through which the guidance will travel to the ultimate user. The closer the issuer is to the user, the more detailed the guidance may become. Intermediate levels may be required to expand or elaborate on the guidance, and cover more details concerning materials, parts, components, subassemblies, and assemblies, and the classifications, if any, to be assigned. Any such expansion or elaboration should be fully coordinated with the headquarters issuing the basic guide.

c. The ease of determining when classified information could be revealed by a particular hardware item. Obscure connections and associations that could reveal classified information may require the issuer of the guide to state classifications for certain hardware items. In such cases it probably would be advisable to explain why classifications are necessary.

d. Whether there are factors that require consideration and action at a headquarters level. National or DoD policy, intelligence data, broad operational requirements, extraneous factors, or other matters not ordinarily available below headquarters, or which require high level consideration may result in decisions to classify certain hardware items.

In this section include in serially numbered subsections and paragraphs, classifications that are to be assigned to specifically designated or identified hardware items. The user of a guide issued at a high level should be afforded some latitude in determining classifications to be assigned to particular materials, parts, components, and subassemblies. Such determinations would be original classification decisions, and should be reflected in a supplemental guide.

(Remember, the following are only examples, and are not valid guidance for any effort.)

<u>INFORMATION</u> <u>REVEALING</u>	<u>CLASS.</u>	<u>DECLASS.</u>	<u>REMARKS</u>
1. End item hardware:			External views of the assembled AN/APR-999 are "U."
a. AN/APR-999	"C"	20 Aug 94	
(1) Analyzer unit	"C"	20 Aug 94	
(2) Threat Display unit	"U"		
(3) Preamplifier	"U"		
b. AN/APR-0000	"U"		

APPENDIX E - FORMAT VARIATIONS

This appendix illustrates column headers and arrangements that are different from those used in appendix D. These headers and arrangements may be employed in the construction of your classification guide, and modified to suit your style and needs in a given effort. For example, a column for downgrading action would not be necessary if the guide did not provide for it, or if only one or two items of information are to be downgraded. In the latter case, the downgrading instruction could be placed in a "Remarks" or "Comments" column.

(Example I)

<u>TOPIC</u>	<u>CLASSIFICATION</u>	<u>DECLASSIFY</u>	<u>COMMENTS</u>
1.4.1 System capacity	"S"	30 Jun 2004	Downgrade to "C" Upon IOC.
1.4.1 Signature characteristics	"C"	15 Jun 1995	

(Example II)

<u>DESCRIPTION</u>	<u>CLASSIFIED</u>	<u>UNTIL</u>	<u>REMARKS</u>
1.4.1 System capacity	"S"	30 Jun 2004	Downgrade to "C" Upon IOC.
1.4.2 Signature characteristics	"C"	15 Jun 1995	

(Example III)

<u>INFORMATION REVEALING</u>	<u>CLASSIFICATION/DECLASSIFICATION</u>	<u>REMARKS</u>
1.4.1 System capacity	"S" DCL on 30 Jun 2004	Downgrade to "C" Upon IOC.
1.4.1 Signature characteristics	"C" DCL on 15 Jun 1995	

Section III Sample Format for a Classification Guide

Date: September 20, 1982 (The date of approval.)

Project/Program Number(s): (Enter number(s), if appropriate.)

Supersession(s): XXXXX Security Classification Guide dated May 12, 1976 and Project YYYYY Security Classification Guide dated July 3, 1981. (Use only if appropriate.)

Action Officer: LTC John Doe, (101) 222-2222, AUTOVON 112-2222.

Distribution: DoD and DoD Contractors only. (Enter the correct distribution statement from Paragraph 2-405b.)

(Note: The above information should appear on the title page or first page. If there is a cover on the guide, the distribution statement must appear on the cover.)

Section 1 General Information

1. Purpose:

To provide instructions and guidance on the security classification of information and material pertaining to the XXXXX Missile System.

2. Authority:

This guide is issued under the authority of AR 380-5. It constitutes authority and may be cited as the basis for classification, regarding or declassification of information concerning the XXXXX Missile System. Unless otherwise noted, authority of the approving official classifies information or material identified as classified in this guide identified on the title page.

3. Application:

Changes in classification required by this guide will be made immediately. (Any discussion of retroactive application, if appropriate, should be inserted here.)

4. Questions and Recommendations:

Questions concerning the content and interpretation of this guide should be directed to the issuing activity. If the security classifications imposed by this guide are considered impractical, documented and justified recommendations should be made through appropriate channels to the issuing activity. If current conditions, progress made in this effort, scientific or technological developments, advances in the state of the art, or other factors indicate a need for changes, similar recommendations should be made. Pending a final decision, the information involved will be protected at either the currently specified level or the recommended level, whichever is higher. All users of this guide are encouraged to assist in improving its currency and adequacy. Any over-classification or incorrect classification should be brought to the attention of the issuing activity.

5. Public Release:

The fact that certain details of information are shown to be unclassified does not authorize automatic public release. Proposed public releases of unclassified information must be processed through appropriate channels for approval for publication. Within the Department of the Army, the procedures specified in AR 360-5 (Reference (iii) in AR 380-5) will be followed. Other DoD activities will comply with DoDD 5230.9

(Reference (iii) in AR 380-5) and applicable service regulations. Defense contractors will comply with DoD 5220.22-M (Reference "F" in AR 380-5) and other contractual requirements. (This paragraph should be included in guides as written here. Be careful not to impose unrealistic or impractical clearance requirements.)

6. Definitions:

(Include here, if necessary, definitions of terms, which are unique to the subject of the guide. If there are many definitions, they may be included in an appendix.)

7. Foreign Government Information and Foreign Military Sales:

(This paragraph may be included, when necessary, to provide guidance on marking and protecting foreign government information involved in the project or program, or to make reference to the Military Assistance and Sales Manual.)

(Usually, the best method for organizing the body of a guide is to arrange the information in columns. The first column should identify the item of information involved. The second column, headed "Classification," should indicate the classification of the item ("U," "c," "S," or "TS") and, when appropriate, "RD" for Restricted Data, "FRD" for Formerly Restricted Data, or "N" for CNWDI (Critical Nuclear Weapon Design Information). Other special access designations or dissemination caveats ("NOFORN," "WNINTEL," etc.) should be shown in the "Remarks" column. The third column should be headed "Declassification," and should contain dates or events for declassification (for example, "DECL August 20, 1994" or "DECL on the first firing") or the notation "OADR." If information is to be downgraded, the downgrading instructions should be placed in the "Remarks" column. The fourth column should be headed "Remarks," and should include any comments needed to make the classification instructions clear and specific. There are two methods of using the "Remarks" column. One is to insert brief statements clarifying the classification, noting exceptions, or providing additional information. This should be done when the statement applies to only one or two items in the guide and is relatively short. When a statement is long, or when it applies to several items, it should be included in a separate section, "Notes," at the end of the guide and referenced as appropriate in the "Remarks" column. The sample sections illustrate these suggestions.)

**Section 2
Overall Effort**

Table G-1

	Classification	Declassification or review	Remarks
8. Identification (nomenclatures, part and stock numbers, etc.)		U	
9. Goal, mission, purpose, military application	U		Unless information classified by other portions of this guide is revealed.
10. End Item			
a. External view	U		
b. Internal view	U		
(1) Missile	U		See note 11.
(2) Warhead and guidance package	U		See note 11.
(3) IR seeker assembly	C	DECL 1 Oct 83	See note 11.
(4) Launcher, radar's, and ground support equipment	U		

Notes:

Special Note: Designs, drawings, photographs, reports, test data, and systems specifications will be classified only if they contain or reveal information classified elsewhere in this guide.

**Section 3
Performance and Capabilities**

Table G-2

	Classification	Declassification or review	Remarks
31. Missile			
a. Altitude			
(1) Maximum	C	DECL 10 June 92	
(2) Minimum	U		
b. Range			
(1) Maximum	S	OADR	"In excess of 10 km" is Unclassified.
(2) Minimum	U		
c. Velocity	C	OADR	See note 9.
d. Acceleration	C	OADR	See Note 9.
e. Maneuverability	S	DECL 10 Jun 92	Downgrade to CONFIDENTIAL upon IOC.

**Section 4
Specifications**

(As suggested in DoD 5200.1-H, this section should address the

characteristics of the system and how it operates-not its capabilities or level of performance, which should be covered in Section 3. For example, for our imaginary XXXXX Missile System, ranges, velocities and acceleration are discussed in Section 3. Details of rocket motor functioning, though, are included in this section.)

Table G-3

	Classification	Declassification or review	Remarks
40. Rocket motor			
a. Size, weight, details of construction	U		
b. Fuel			
(1) Components of Mixture	U		
(2) Proportion of Components in Mixture	C	DECL 3 May 93	
c. Burn rate	C	DECL 3 May 93	
d. Thrust Achieved	U	DECL 3 May 93	Thrust, stated alone, is UNCLASSIFIED unless it is the maximum achieved in flight. Thrust in terms of time from ignition or launch if CONFIDENTIAL.

Notes:

(Physical characteristics such as size, weight, power output, transportability, etc., should also be discussed here.)

**Section 5
Critical Elements**

(The identification of “critical elements” of an effort is a matter of judgment. Sometimes, it serves no real purpose. It may be more useful to include classification instructions for information above “critical elements” in other sections (2, 3, 4, 6 or 8) of the guide. In such cases, this section should be included in the guide for the sake of format consistency, but should contain only the words, “NOT APPLICABLE.” If this section is used, the format is similar to that of other sections.)

**Section 6
Vulnerabilities and Weaknesses**

Table G-4

	Classification	Declassification or review	Remarks
54. Operational countermeasures (target tactical employment techniques which degrade system performance)			
a. Identification of techniques	C	OADR	See notes 21, 25.
b. Description of effects of techniques			
(1) Quantitative	S	OADR	
(2) Nonquantitative	C	OADR	See Notes 21, 25.
55. Electronic and electro-optical countermeasures (ECM and EOCM)			
a. Identification of possible ECM and EOCM	U		
b. Description of effects			
(1) Quantitative	S	OADR	
(2) Nonquantitative	C	OADR	See Notes 22, 25.
56. Nuclear hardening and NEMP vulnerability			
a. The Fact that the XXXXX Missile System is nuclear hardened	U		
b. Nuclear hardening techniques employed	S	OADR	
c. Information revealing degree of hardening of NEMP vulnerability	S	OADR	
57. Antiradiation missile (ARM) vulnerability			
a. The fact that ARMs are a recognized threat to the system	U		See Notes 24, 25
b. Any statement revealing the degree of ARM vulnerability	S	OADR	
c. Identification of ARM countermeasures employed	C	OADR	See Note 26.
d. Qualitative or quantitative information revealing effectiveness of countermeasures	S	OADR	
58. Electronic counter-countermeasures (ECCM)			
a. Identification of ECCM inherent in or proposed for application to the system	U		
b. Description of ECCM effectiveness			
(1) Quantitative	S	OADR	
(2) Nonquantitative	C	OADR	See note 23.
c. ECCM design or			See paras 41c and 50.

Notes:

(As with other sections in this sample format, this section should not be interpreted as imposing or suggesting classification requirements for any actual system. It is intended, instead, to indicate the minimum level of detail that should be included. In some cases, even more detailed or specific information may be necessary.)

**Section 7
Administrative Data**

Table G-5

	Classification	Declassification or review	Remarks
61. Research and Development Program			
a. Budget year and prior year dollars and quantities	U		
b. Future years and total dollars and quantities	U		
62. Procurement, Production and Programming			
a. Quantities			
(1) Assets (Worldwide)/Authorized Acquisition Objective (AAO)/Total Program	C	DECL 10 Aug 87	
(2) Assets or programmed quantities by theater or command	C	DECL 10 years from date of information	
(3) Foreign Military Sales (FMS) and Military Assistance Program			See Note 3.
(4) Program quantities for budget year, authorization year and prior years	U		See Note 4.
(5) Future years quantities (FYPD or total program beyond those displayed in Exhibit P-1)	C	DECL 10 Aug 87	See Note 4.
b. Funds			See Note 35.
(1) Budget year, authorization year and prior years dollars	U		
(2) Future years dollars (beyond those displayed in Exhibit P-1)	U		
(3) Total procurement dollars	U		
(4) Unit cost as listed in Exhibit P-1	U		
(5) Program unit cost	C	DECL 10 Aug 87	
(6) Design-to-cost goal and other unit cost estimates	U	See Note 5.	
c. Production and delivery			
(1) Numbers contracted	U		See Note 5.
(2) Production and delivery schedules	U		See Note 5.
(3) Rate of delivery	U		
(4) Production capability, or capacity	C		
(5) Equipment distribution plans	U	OADR	
63. Key Scheduling Dates			
a. Initial Operating Capability (IOC)	U		
b. Developmental milestones other than IOC	U		
c. Individual test/demonstration dates	C	DECL on date of test	See Note 7.
d. Future schedule of test/demonstration dates	C	DECL upon completion of schedule	See Note 7.
e. Theater deployment date	C	DECL when announced by theater commander	
f. Phase-out date	C	DECL when announced	

**Section 8
Hardware**

(This section is appropriate only for guides dealing with systems and equipment. Each item of classified hardware must be identified along with its declassification date or event. In some cases, it may be best to list only classified hardware items. In other situations, it might be necessary to list both classified and unclassified items to avoid confusion. U.S. Army parts numbers and national stock numbers should be included, when possible, but should not

be used as a substitute for item nomenclature. If all hardware is unclassified, a simple statement to that effect should be made here.)

(When writing guides for systems, which use electronic data processing equipment, the classification of software must be included. In such cases, this section should be titled "HARDWARE AND SOFTWARE," with each type of item addressed separately. You must discriminate between programs, data and media. A portion of a section dealing with software is shown below.

Table G-6

	Classification	Declassification or review	Remarks
64. Programs	U		
65. Data files			
a. Stanadard (furnished) files	S		See Note 32.
b. Locally generated files			
(1) TACEMP, CDEP1, CDEP2, TARGDF	S	DECL 3 Aug 95	Classified if classified information concerning target performance data is entered, otherwise UNCLASSIFIED.
(2) TARGID, REL1, REL2			
(3) All others	U		
66. Storage and data entry media			
a. Storage media			
(1) Standard (furnished) tapes	S		See Note 32.
(2) Locally generated tapes			See Note 33.
b. Data entry cards			
(1) Program change and system control cards	U		See Note 34.
(2) File change and parameter cards			

Section 9 Notes

- 3.**
Classify in accordance with Chapter G, Military Assistance and Sales Manual, the classification of the request for assistance from the foreign government involved, or other appropriate guidance.
- 4.**
Information for the budget year and authorization year is declassified upon submission to Congress as a part of the DA FY Procurement Program, the President's Budget (Exhibit P-1) unless the year in question is the last (or "buy-out") year. That year's information would reveal the AAO or total program and must remain classified until the AAO is declassified.
- 5.**
Unclassified only if the information does not reveal and cannot be used to compute the AAO or total program quantities, otherwise Confidential, declassify August 10, 1987.
- 7.**
Classification applies to missile firing tests only, and only when the scheduled date of firing is revealed. Other test schedules are Unclassified.
- 9.**
Applies only to velocities/acceleration attained within system performance envelope. Velocities/acceleration attained at minimum range altitude and below are Unclassified.
- 11.**
External and internal views of the IR modulator assembly are Confidential. Internal views of the missile and warhead/guidance package are Unclassified unless the IR modulator assembly is shown.
- 21.**
The statement that the XXXXX Missile System is "highly effective against high-G maneuvering targets and targets in NOE flight" is Unclassified.
- 22.**
Statements that system performance is "degraded" or "affected" by a particular ECM or EOCM, without further elaboration, are Unclassified.
- 23.**
Statements that ECCM features are "effective" against a specific ECM or EOCM are Unclassified. Any further elaboration of such statements or statements that reveal a lack of ECCM effectiveness are Confidential.
- 24.**
This information is UNCLASSIFIED since it is well known that any radiating system may be targeted by ARMs. Since the XXXXX Missile System includes dedicated target acquisition and tracking radar's, and since the missile itself uses radar and active IR homing devices, ARMs must logically be considered a threat.
- 25.**
Data concerning specific threat capabilities and tactics may be classified at a higher level by the originator. This information will be derivatively classified according to the originator's instructions.
- 26.**
The fact that ARM countermeasures are being applied to the system is UNCLASSIFIED.
- 31.**
No XXXXX Missile System operating program is classified in

them. The following programs access classified files: MIX1, MIX2, REFIRM, SYNC6 and OPORD2.

- 32.**
All standard files furnished to using units will be classified SECRET, since they will contain SECRET range and maneuverability data. Declassification instructions will be provided with each file.
- 33.**
Locally generated tapes will be classified according to the information they contain, as described in Paragraph 65b.
- 34.**
File change and parameter cards will be classified according to the information they contain, as specified in other portions of this guide. Cards furnished, as part of a general system update will be pre-marked by the preparer.
- 35.**
A breakout of UNCLASSIFIED yearly funding or cost estimates which would prejudice negotiations with a contractor and which qualify for exemption from mandatory public disclosure under the provisions of AR 340-17 should be marked "FOR OFFICIAL USE ONLY." If furnished to the Congress of the United States, this information must be marked "NSE" ("Non-Security Exemption").

Section IV Changing Security Classification Guides

- G-9.**
Whenever a security classification involving a guide subject changes that revision or re-issuance of the guide must reflect change. It may also be necessary to clarify or correct information in the guide or provide additional information or instructions.
- G-10.**
The terms "revision" and "re-issuance" have specific meanings which must be understood because they are used differently on DD Form 2024 (DoD Security Classification Guide Data Elements).
 - a.* The term "revision" includes the following three types of actions:
 - (1) A change, which actually modifies some provision(s) of a guide (e.g., a classification, declassification or review date, the description of an item of information, a note).
 - (2) An errata sheet, which corrects an error (typographical or otherwise) in a guide.
 - (3) An addendum, which adds new material to a guide.
 - b.* A single revision may serve more than one of these purposes (e.g., add new material and correct an error). A revision may be titled "change," "errata sheet," or "addendum," but in the interests of clarity the term "revision" is recommended. Each revision should bear an identifying number. Revisions may be pen-and-ink changes or page changes whichever is more efficient. Revisions will show the date of approval.
- G-11.**
The term "re-issuance" applies only to republication of an entire guide to incorporate modifications. The date of the reissued guide will be the date of approval of the re-issuance. The original issue of the guide or the latest prior re-issuance (if any) will be shown under "Super-sessions."
- G-12.**
Revisions and reissued guides must be approved, distributed and reported as required in Paragraphs 2-400d, 2-405 and 2-406 of DoD 5200.1-R.

Section V Instructions for Preparing DD Form 2024(DoD Security Classification Guide Data Elements)

G-13.

Submission of DD Form 2024, required by Paragraph 2-406 of this regulation, allows the listing of a security classification guide (SCG) in DoD 5200.1-1, the DoD Index of Security Classification Guides.

G-14.

DD Form 2024 must be prepared at least in four copies. The original and two copies are forwarded to HQDA (DAMI-CIS), Washington, DC 20310-1051. One copy is to be retained with the record copy of the SCG. In the case of new guides, revisions or re-issuance's, the DD Form 2024 submitted to HQDA should accompany the copies of the SCG or change sent to DAMI-CIS.

G-15.

DD Form 2024 was revised on 1 February 79. The previous edition of 1 July 76 is obsolete and should not be used.

G-16.

The reverse side of DD Form 2024 provides instructions for completing the form. The following guidance supplements and clarifies these instructions.

a. Paragraph B of the instructions defines the meanings of the six blocks in Item 1 of the form.

(1) The "new guide" block should be checked when reporting any of the following:

(a) The issue of a guide covering a subject on which no previous guide has been issued.

(b) Publication of a guide under the circumstances described in paragraph E-18b.

(c) Reissue of a guide which is not currently indexed in DOD 5200.1-I.

(2) Do not check the "new guide" block just because the title of a guide has been changed. The "revision" block should be checked when the form is prepared to reflect a partial change (errata sheet, addendum, page change) to an SCG. The "reissuance" block should be checked when the entire guide is republished to include changes. The "correction" block is used when DD Form 2024 is submitted to correct information entered on a previous DD Form 2024, not to correct information in the SCG itself.

b. Item 2 of the form should show only numbered publications which contain or transmit SCGs (for example, ARs, TBs, LOIs, major command or local regulations). If the guide is separately published, letters of transmittal, etc., should not be listed; "NONE" should be entered in Item 2.

c. Never complete Item 3 by entering "Security Classification Guide for _____." The item or project name should be entered as it appears on the guide; the phrases "Security Classification Guide" or "classification Guidance for" are unnecessary.

d. Item 4 must contain a date as shown in paragraph D on the back of the form. For a new guide, enter the date of its approval. When reporting a reissuance, enter the date of approval of the reissued guide. For other submissions, enter the date of the latest issue of the guide.

e. In Item 7, enter a date two years from the date of issue, reissue, or the last biennial review, whichever is latest.

f. When completing Item 8, enter "NONE" if no revisions to the SCG have been published. Record revisions according to this example: A guide was issued on 5 May 76. A revision was issued on 12 Jul 77; the DD Form 2024 for the revision showed "01770712" in Item 8. A second revision was issued on 20 Nov 78; Item 8 of that DD Form 2024 read "02781120."

g. Item 9, "Subject Matter Index Terms," is an extremely important portion of the form, since the accuracy and validity of these terms determine the usefulness of DOD 5200.1-I. Carefully study the list of index terms found in DOD 5200.1-I and select terms that best apply to the SCG subject. Within the Department of the Army, only

terms listed in the current edition of the index will be used. Other terms may not be used without the permission of the Directorate of Counterintelligence and Security Countermeasures, ODSCINT, (OACSI), HQDA. If none of the current terms is appropriate, submit recommended additions to HQDA(DAMI-CIS), WASH, DC 20310-1051. Insure that the index terms do not disclose classified information about the SCG subject.

h. The index sequence number entered in Item 11 is essential to the accuracy of DOD 5200.1-I. If DD Form 2024 reflects a revision, reissuance, biennial review, cancellation, or correction, the index sequence number following the SCG title in the current edition of DOD 5200.1-I must be entered in Item 11. Two special circumstances deserve mention:

(1) If a guide is to be reissued with a new title (due to a change in equipment nomenclature or project title), the index sequence number of the old guide must be entered in Item 11. The computer program used to compile the index will key on that number, delete the old title, and replace it with the new title. Do not submit a DD Form 2024 to list it under its new title. This might cause the SCG to be deleted from the index entirely.

(2) In a very few cases, a revision or correction to a recently issued SCG which has not yet been listed in DOD 5200.1-I will be issued. In such cases, leave item 11 blank.

i. Item 12, "Remarks," may be used to advise the recipients of DD Form 2024 of any additional information considered appropriate. Information placed in Item 12 will not appear in DOD 5200.1-I. Item 12 may be left blank.

j. DD Form 2024 states that completing Item 14a, "Action Officer," is optional. Within the Department of the Army, an action officer will be indicated in Item 14a each time DD Form 2024 is prepared. The person listed should be the current action officer for the SCG.

G-17.

Sometimes an SCG will be replaced by two or more SCGs dealing with individual projects or items of equipment. For example, an SCG dealing with aircraft survivability equipment was replaced with separate SCGs for each item of equipment. In other cases, two or more SCGs may be combined. For example, SCGs covering two pieces of equipment may be replaced by one SCG for a system in which both items are included. When this occurs, the proponent of each superseded SCG must submit a DD Form 2024 to cancel the old SCG. A statement in Item 12 of the DD Form(s) 2024 for the new SCG(s) will not cancel the superseded SCG(s).

G-18.

When the proponent of a SCG changes due to organizational changes or progress in system development, the following instructions apply:

a. If responsibility is transferred from one U.S. Army element to another, a "correction" or "cancellation" DD Form 2024 will not be submitted. The change of proponent should not be reported until the SCG is revised or reissued by the new proponent.

b. If responsibility is assumed by a U.S. Army element from an agency outside the US Army, the change should be reflected when the gaining activity revises the SCG. The "new guide" block in Item 1 of the DD Form 2024 will be checked; no index sequence number will be entered. Cancelling the old SCG is the responsibility of the former proponent.

c. If responsibility is assumed by a non-Army agency from a U.S. Army element, the losing element should make sure they know when the new proponent republishes the SCG. The losing U.S. Army element is responsible for submitting a "cancellation" DD Form 2024 when, but not before, the gaining agency republishes the SCG.

Appendix H Classified Document and Material Storage Standards and Information

Section I Minimum Class A, B, and C Vault Construction Standards

H-1. Consolidated masonry vault specifications

These specifications are given in table H-1.

H-2. Lightweight alternate Class A vault specifications

Interim lightweight alternate class A and B vault specifications (for use above ground level only). Where building structural design factors preclude the use of a standard class A or B vault design at above ground level locations, a modular vault-ASTM type I, U.L. class-M approved under ANSI/UL Standard 608, dated 27 June 1983 or later, may be used. Until final testing of this product is completed, it will not be used in lieu of the conventional designed vaults, at or below grade. Existing steel lined rooms, built to previously approved specifications, will continue to be approved for use, but further construction of steel liners will be deferred in favor of the above specified ANSI/UL Standard 608 product.

H-3. Doors for both methods of vault construction

The vault will be equipped with an approved vault door of the type presently listed on the Federal Supply Schedule. The Class 5 vault door will be used with reinforced concrete vaults. Where weight of

construction is a factor and a steel-lined vault is used, a Class 6 vault door may be used, if obtainable. Normally, a vault should have only one entrance. When a vault exceeds 1,000 square feet of floor space or has more than eight occupants, it should have a minimum of two exits (one of which will be the entrance) for safety purposes. When more than one entrance is required, each must be equipped with the approved door, but only one door will be used for normal access. The use of a vault door for controlling movement into and out of a facility is not authorized as this continued use will create undue wear on the door and will eventually weaken the locking mechanism and cause malfunctioning. Therefore, a vestibule should be constructed at the entrance with an access door to achieve control when the vault door is open. Where building codes require that the vault entrance meet a specified fire rating, the vestibule and its access door must be of the required fire rating. Where permissible, the vault door optional day gate may be employed as the entrance control in lieu of the above vestibule. There will be no windows in a vault, and all ventilator openings or other access routes into the vault will be properly treated to deny unauthorized access. Sound attenuation will be fully employed and where inadequate, white noise masking will be added to prevent classified discussions from being overheard.

Table H

Class	Approved storage level	Thickness		
		Floors	Walls	Ceiling
A	TOP SECRET	8" RC ¹	8" RC	8" RC
B	SECRET	4" RC	8" ²	4" RC
C	CONFIDENTIAL	4" C ¹	8" ³	4" RC

Notes:

LEGEND RC = Reinforced concrete; C = Concrete without reinforcement

¹ All concrete used in vault construction will be monolithic cast in place, Class A, conforming to US Army Corps of Engineers Specification C.E. 204 (minimum compressive strength of 3000 psi after 28 days of aging). Reinforcing will be by minimum 5/8-inch diameter steel reinforcing bars (rebars) laid a maximum of 6 inches on centers, creating a cross-hatched steel curtain, to be sandwiched at half thickness of the concrete, parallel to the longest surface. Rebars will be anchored or imbedded in all contiguous walls/surfaces.

² Class B vault walls will be constructed of masonry at least 8 inches thick, such as brick or concrete block employing adequate bond. Hollow masonry, only of the vertical cell (load bearing) type, can also be used, but if used, each cell will have from ceiling to floor 1/2-inch diameter or larger rebar inserted, and then be filled with pea gravel and Portland cement grout. Rebars will be anchored in both floor and ceiling to a depth of at least 4 inches. In seismic areas, 6-inch or thicker RC will be required.

³ Class C vault walls will be constructed of thick-shell concrete block or vertical cell clay tile and be not less than 8 inches thick. In seismic areas, 6-inch or thicker RC will be used.

H-4. Additional security safeguards for vaults

All vaults designated Class A or B will have intrusion and fire protection. In addition, when a vault is unattended, the areas contiguous to such vault will be supervised either by frequent routine guard patrols or electronic means so as to increase the depth of security and to allow early detection of trespass. Detection of trespass outside the vault is preferred to detection of vault penetration, since response to the former should preclude the latter. Detection systems that indicate attempted penetration (such as vibration sensors) are acceptable, provided they allow adequate response time before actual barrier violation.

H-5. Security assistance

If requested in writing, additional technical advice and guidance relative to vault security problems, may be obtained from the Commander, Intelligence Material Activity (IMA), ATTN: AMXIM-PS, Fort Meade, MD 20755.

Section II Security Upgrading Via Construction—Buildings, Offices, and Rooms

H-6. Approved standards for security upgrading

The following guidance is offered as a norm against which—

a. To evaluate the adequacy of existing structural security safeguards.

b. To provide security guidance for new construction in areas which will contain activities and material of foreign intelligence interest.

H-7. Hardware

Heavy-duty builder's hardware should be used in construction, and all screws, nuts, bolts, hasps, clamps, bars, 2-inch-square mesh of No. 11 wire, 18-gauge expanded metal screen, hinges, pins, etc., should be securely fastened to preclude surreptitious removal and ensure visual evidence of tampering. Hardware accessible from outside the area should be peened, pinned, brazed, or tack-welded to preclude removal. The term "2-inch-square mesh of No. 11 wire,"

which meets the requirements of Federal Specification RR-F-191d, 17 June 1965, hereinafter shall be referred to as "wire mesh."

H-8. Interior walls

Construction should be plaster, gypsum wallboard, metal panels, hardboard, wood, plywood, or other opaque materials offering similar resistance to, and evidence of, unauthorized entry into the area. If insert-type panels are used, a method should be devised to prevent the removal of such panels without leaving visual evidence of tampering. Area barriers up to a height of 8 feet should be of opaque or translucent construction where visual access is a factor. If visual access is not a factor, the area barrier walls may be of wire mesh or other nonopaque material offering similar resistance to, and evidence of, unauthorized entry into the area.

H-9. Windows

Window openings 18 feet or less from an access point (for example, another window outside the area, roof, ledge, door, and so forth) should be fitted with ½-inch bars (separated by no more than 6 inches), plus crossbars to prevent spreading, or 18-gauge expanded metal screen, or wire mesh securely fastened on the inside. When visual access is a factor, the windows should be kept closed and locked at all times, and also should be made translucent or opaque by any practical method such as painting or covering the inside of the glass. During non-duty hours the windows should be closed and securely fastened to preclude surreptitious removal of classified material.

H-10. Doors

Doors should be substantially constructed of wood or metal. When windows, panels, or similar openings are used in the door, they should be secured with 18-gauge expanded metal screen or wire mesh securely fastened on the inside. If visual access is a factor, the windows should be translucent or opaqued. When doors are used in pairs, a mullion insert anchored top and bottom should be installed between the doors.

H-11. Door louvers or baffle plates

When used, they should be reinforced with 18-gauge expanded metal screen, or wire mesh fastened inside the area.

H-12. Door locking devices

a. Entrance doors should be secured with either a GSA-approved built-in, three-position, dial-type, changeable combination lock; a GSA-approved combination padlock (per paragraph 5-101) as amended and as specified in paragraph 5-102d; a key-operated padlock or locking device with high security cylinder and hasp (see figure H-1) as described in the same paragraph; or a built-in 1-inch throw, deadbolt lock equipped with the GSA-approved high-security cylinder; or preferably a combination of these. Other doors should be firmly secured from the inside with a panic bolt (actuated by a panic bar), a deadbolt, a rigid wood or metal bar (fitted to preclude "springing"), extending across the width of the door and held in position by solid clamps, preferably on the door casing, or other means approved by the cognizant OPSEC Support Unit and Fire Marshal.

b. The new High-Security Padlock approved July 1982 became available within the supply system late fall 1982. It has the same Federal Stock Number as the Sargent and Greenleaf (S&G) Model 831B Padlock, which is being phased out of service.

H-13. Ceilings

Ceilings should be constructed of plaster, gypsum wallboard material, panels, hardboard, wood, plywood, ceiling tile, or other material offering similar resistance to and detection of unauthorized entry. Wire mesh, 18-gauge expanded metal screen, or other nonopaque material offering similar resistance to, and evidence of, unauthorized

entry into the area may be used if visual access to classified material is not a factor. When wall barriers do not extend to the ceiling, and a false ceiling is used, this false ceiling should be reinforced with wire mesh or 18-gauge expanded metal screen, alarmed and otherwise secured with heavy-duty builder's hardware. (This measure also applies when panels are removable, and entry can be gained into the area without visible detection.) When wire mesh or expanded metal screens are used, they must be secured to adjoining walls in a manner which precludes removal without leaving evidence of tampering. In those instances where barrier walls of an area extend to a solid ceiling, there is no need to reinforce a false ceiling; however, an Intrusion Detection System (IDS) should monitor this otherwise unobserved area.

H-14. Ceilings (unusual cases)

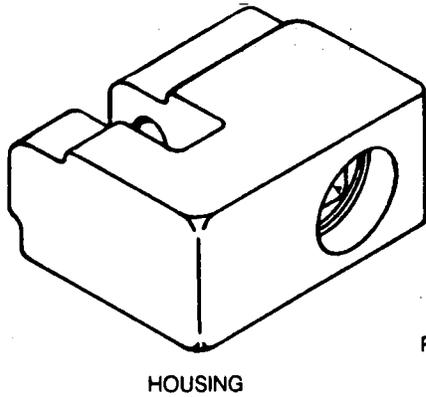
It is recognized that instances may arise where activities have a valid justification for not erecting a solid suspended ceiling as part of the area, especially in high-ceiling hangers. The activity may contend that the use of a suspended ceiling is impractical because of production methods, such as the use of overhead cranes for moving bulky equipment within the area. Cases also exist where the air conditioning system may be impeded by the construction of a solid suspended ceiling (such as ADP centers). At times, even the height of the classified material may make a suspended ceiling impractical. In such cases, special provisions should be made to ensure that surreptitious entry cannot be achieved by entering the area over the top of the barrier walls (for example, employ approved intrusion detection systems, sensors, and more frequent guard patrols). Areas of this type should be closely scrutinized to ensure that the structural safeguards are adequate to preclude entry via adjacent pipes, catwalks, and ladders, or to preclude observation, if visual access is a factor.

H-15. Miscellaneous openings

Where ducts, pipes, registers, sewers, and tunnels are of such size and shape as to permit unauthorized entry (in excess of 96 square inches, for example), they will be secured by 18-gauge expanded metal screen, wire mesh, or where more practical steel bars at least ½-inch in diameter with a maximum space of 6 inches between the bars. The steel bars will be securely fastened at both ends to preclude removal, and will have ¼-inch thick by 1-½-inch wide steel crossbars at 18-inch intervals to prevent spreading. When wire mesh, expanded metal screen, or steel bars are used, installation should ensure that classified material cannot be removed through the openings with the aid of any type of instrument. Care also will be taken to ensure that a barrier placed across any waterway (sewer or tunnel) will not cause clogging or offer obstruction to the free flow of water or sewage.

H-16. Approved alarm systems

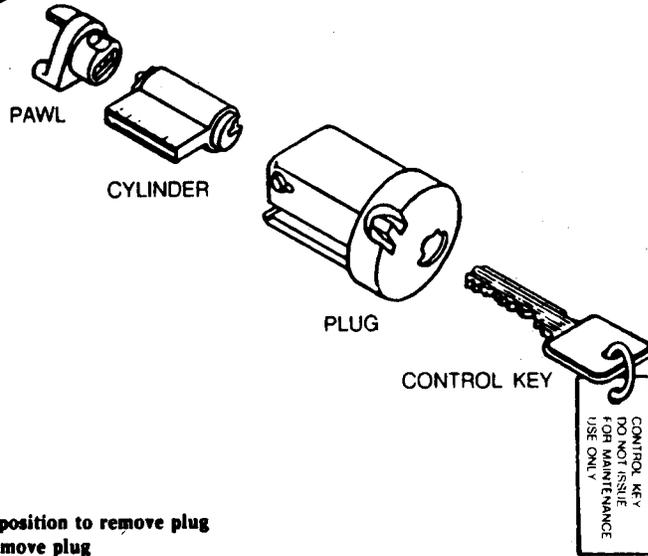
Information and limitation on use of approved intrusion detection systems, both commercial and DOD J-SIIDS equipment, can be found in DIA Manual 50-3, chapter III, dated 2 May 1980. Model designations of items specifically approved for use in protection of U.S. classified information and material are provided in that chapter, along with other pertinent information. All detailed information relative to an alarmed area and the electronic system protecting its classified defense information or material (i.e., electrical diagrams indicating wire runs, sensor and control placements, as well as sensor types and area of coverage, floor plans, and photographs revealing the position or existence of such items within the area), will be tightly controlled and marked For Official Use Only.



HOUSING

CYLINDER ACCESS INSTRUCTIONS

LK 1200 HIGH-SECURITY PADLOCK Per MIL-P-43607E



1. Insert control key. Turn key 7° past lock position to remove plug
2. Pull key away from housing which will remove plug
3. Remove pawl
4. Remove cylinder by pushing from key entry position
CAUTION—A ball is located behind the plug spring and could fall out
5. Slide new cylinder into plug. **CHECK** that carbide cylinder and lower protection is still in plug
6. Install pawl—grease with Molykote G-N or equivalent
7. Insert control key in cylinder and rotate to access position
8. Insert entire assembly into housing
9. Turn key to locked position and remove
10. Unlock with 'Operational Key'

Figure H-1. New high-security padlock

Appendix I Inspection Checklist for Security Containers

I-1.

Security containers are usually serviceable for 25 years if properly maintained. Their life span is often cut short by lock or locking bolt linkage malfunctions that require neutralization of the container. Most of these problems can be detected in early stages; and definite symptoms can warn about a developing problem. Users should be alert for these symptoms; if any of them are detected, the users should immediately contact their supporting maintenance activity for help. *Never* use force to try to correct the problem. Critically needed material should not be stored in containers showing any of these symptoms, since they cannot be counted on to open again; the user may be faced with a "lockout."

I-2.

Watch for the following signs of trouble:

a. A dial that is unusually loose (to include in and out play) or difficult to turn.

b. Any movement in the dial ring. (Apply twist to detect this.)

c. Difficulty in dialing the combination or opening the container.

Examples are listed below.

(1) The need to dial the combination more than once (when human error is not at fault).

(2) The need to dial numbers slightly above or below the correct number in the combination.

d. Difficulty with the control drawer or other drawers. Examples are listed below.

(1) Drawers rubbing against container walls. (The container may not be leveled, or tracks or cradles may not be aligned properly.)

(2) Problems with opening or closing drawers because the tracks or cradles need lubricant, material is jammed in behind the drawer, or the internal locking mechanism is tripped.

e. Difficulties in locking the control drawer. Examples are shown below.

(1) The control drawer handle or latch will not return to the locking position when the drawer is shut.

(2) On Sargent & Greenleaf locks, the butterfly in the center of the dial will not turn after the control drawer is shut and the dial has been turned to "0."

(3) The locking bolts move roughly, slip, or drag, or the linkage is burred or deformed.

Appendix J Communist Countries

Albania

Bulgaria

Cambodia

Chinese People's Republic (Communist China), including Tibet

Cuba

Czechoslovakia

Communist Korea (North Korea)

German Democratic Republic (East Germany), including the Soviet Sector of Berlin

Hungary

Laos

Mongolian People's Republic (Outer Mongolia)

Poland

Rumania

Union of Soviet Socialist Republics, including Estonia, Latvia, Lithuania, and all other constituent republics, Kurile Islands, and South Sakhalin (Karafuto)

Vietnam

Yugoslavia

Appendix K Classified Material Destruction Standards

K-1. General

This appendix contains basic concepts and guidelines that assist in determining the sufficiency of various destruction techniques. It also provides residue dimension standards that will assist in achieving secure destruction. No single destruction method has been found to be as effective, versatile, and secure as burning. However, since the ban on bulk incineration for environmental reasons, many mechanical destruction systems have become popular. These systems have inherent shortcomings that limit their application. Fortunately, the inefficient and outlawed incinerator has been replaced by the pyrolytic furnace. These furnaces operate in compliance with Federal Clean Air Act Regulatory Standards and should be given preference over mechanical destruction means when possible. Users should obtain written guarantee from the pyrolytic furnace seller attesting to the unit's ability to be licensed and to operate within the standards prevailing at the point of installation, since standards vary from State to State. Oversea commanders will conform to host nation standards if more restrictive than U.S. standards, unless emergency destruction is necessary.

K-2. Concepts of destruction

The guidelines in this appendix are practical and secure when employed in a timely manner to prevent excessive accumulation and in conjunction with the "secure volume" and "data density" concepts of destruction explained below.

a. *"Secure Volume" concept.* The "secure volume" concept of destruction processing stresses that security is enhanced not only by small residue particle size, but also by restricting the chances of successful reconstruction of that residue by increasing the number of pieces involved. This increase can be achieved in two ways: prohibit destruction until a quantity of no less than 20 similar pages of classified paper are destroyed at one time, or add sufficient similar type of unclassified pages of paper to the classified document to arrive at the minimum 20 similar page count. Either method will result in a "secure volume" of residue. The "secure volume" concept will be made a standing operating procedure for the use of all office-type approved security shredders. Bulk feeding procedures for the larger, high-volume destruction equipment systems (pulpers and pulverizers) normally ensure a "secure volume." (See destruction guidelines in table K-1.)

b. *"Data density concept."* The following standards apply to the destruction of graphic materials where "data density" (print or image ratio to blank space per square centimeter) is no greater than that employed to print this paragraph. Where smaller print is employed, the data density per square centimeter is greater than that appearing in the paragraph. Examples of high data density material are: microfilm, microfiche, and aerial photography. Consequently, a more stringent destruction standard is necessary when processing high data density materials than is established here for office copy paper-based items. To achieve a more stringent standard, a smaller sized security screen is employed, or the material is completely destroyed by burning in a suitable pyrolytic furnace. The data density determination and subsequent security screen size required to be used is the responsibility of the security officer or manager at each installation and activity. No single security screen standard for all graphic material destruction is desirable, due to differences in data density. Therefore, several security screen sizes are needed for each mechanical system using such screens and should be within reach of the operator to avoid excessive or insecure destruction. Excessive destruction represents "waste" and is extremely costly in terms of dollars, energy, and time, since it reduces the capacity of the system (pounds per hour) and frequently requires overtime pay for workers.

K-3. Approved routine methods of destruction

The methods for routine destruction of classified material shown

below are approved for use by DA elements. (See TB 380-41 (reference (v)) for COMSEC procedures.)

K-4. Approved routine security destruction equipment

a. Design specifications of equipment used for each of the destruction methods in paragraph K-3 will, as a minimum, conform to the following applicable standards:

- (1) Pyrolytic furnaces—Federal Clean Air Act, as amended.
- (2) Shredders—Interim Federal Specifications FF-S 001169 with amendment 3.
- (3) Pulping Machines—Interim Federal Specifications FF-P-00800A with amendment 2.
- (4) Pulverizing Machine—Interim Federal Specifications FF-P-00810A with amendment 3.
- (5) All others—to be approved by IMA per paragraph 9-101 prior to procurement.

b. Residue Standards

(1) *Pyrolysis.* Pyrolytic furnace ash residue must not contain unburned product. If unburned product is found, it will be treated as classified waste and maintenance personnel will be instructed to correct this fault in the furnace's burn cycle. Ash residue is to be examined and reduced by physical disturbance and will be considered destroyed when capable of passing through a ½-inch (13-mm) square wire sieve. Furnace operators should be permanently assigned and trained to perform necessary adjustments and maintenance and be cleared for access to the highest level of material being routinely destroyed.

(2) *Shredders.* Individual office-type security shredders, both Class I (crosscut) and Class II (continuous strip), are a potential security hazard if they are not employed on a "secure volume" basis. Their residue normally is accessible to or routinely removed by uncleared housekeeping personnel. Class II shredders (continuous ½-inch strip) are not authorized for destruction of material classified higher than SECRET. This limitation also applies to the heavy duty ¾-inch wide by ½-inch long crosscut shredder authorized for use only in data processing centers to destroy classified computer printouts and data processing cards. The Class I shredder identified by GSA Interim Federal Specifications FF-S-001169 as producing a residue measuring ½-inch + ¼-inch tolerance by ½-inch crosscut is approved for destruction in "secure volume" of TOP SECRET material. Any crosscut shredder whose residue particle size (total area) is equal to or smaller than that of the above Class I shredder (15.12-mm² or 0.02344in²) is similarly approved for TOP SECRET destruction, when used in accordance with the "secure volume" concept of operation. Classified microfilm, microfiche, or similar high data-density material will not be destroyed by shredding.

(3) *Pulping.* The Interim Federal Specifications FF-P-00800A with amendment 2 specifies the perforated screen or ring used in the masticating unit (through which all pulp must pass) will have ¼-inch (6.350-mm) or smaller diameter perforations. Since the pulping process entails wetting and desolving action, plastic-based or other water-repellent-type papers normally should not be put through this system. However, if wetting additives are used and the ratio of soluble to nonsoluble paper kept high (16 to 1 or greater), the masticating unit normally will tolerate that material. This toleration is totally dependent upon the sharpness of the pulper's cutters. Foreign matter, such as metal and glass, must be excluded from charge loads by visual inspections. Standard systems employing ¼-inch diameter perforated security screen are approved for the destruction of classified paper-based documents through TOP SECRET. TOP SECRET material will not be destroyed on equipment where security screens with larger perforations are in use. Random samples of residue from such units should be collected by the security manager for periodic examination. Samples may be sent to IMA for evaluation and comment.

(4) *Pulverizers.* The Interim Federal Specifications FF-P-00810A with amendment 3 covers pulverizing as a dry destruction process. It does not, however, specify a specific dry destruction method; consequently, within this category are hammer mills, choppers, hoggers, and hybridized disintegrating equipment.

(a) *Hammer mills.* Hammer mills destroy by flailing action. Paper, lightweight plastics and wood, glass slides, and aluminum-offset plates, as well as other frangible materials, can be destroyed in a hammer mill. This process is extremely destructive, very noisy, and can be dusty if the air-handling system is not kept in good repair. Equipped with $\frac{1}{4}$ -inch (6.35-mm) or less diameter security screen, hammer mills are approved for destruction of TOP SECRET paper-based materials and aluminum offset plates, provided the "secure volume" processing concept is observed. When required to destroy nonpaper-based TOP SECRET material or high-data-density substances such as classified microfilm and microfiche, the security screen size will be reduced to a diameter of at least $\frac{1}{16}$ -inch (1.588-mm) or smaller. If used to destroy plastic film-base material, care must be exercised in the feeding of the hammer mill because of the high heat buildup that can result, causing film to melt or fuse or burn. To prevent this, paper and plastic-based films should be alternately fed into the hammer mill.

(b) *Choppers.* Choppers cut via scissor action between one or more fixed and one or more rotating square-edged surfaces. This system's waste volume expansion is the most compact of the various dry mechanical destruction systems. Choppers are approved for destruction of TOP SECRET and below paper-based documents using a $\frac{3}{16}$ -inch or 5-mm diameter perforated security screen, provided the "secure volume" processing concept is practiced.

(c) *Hoggers and hybrids.* Hoggers and other hybridized disintegrating equipment are principally for high-volume destruction operations (destroying 1 or more tons per day). Due to the many hogger and hybrid designs now on the market, a more descriptive explanation of this destruction methodology and the appropriate security screen size for each cannot be given here. It is recommended that secure volumes and a security screen size of $\frac{1}{4}$ -inch (6.35-mm) be employed for TOP SECRET paper-based materials processed in these systems. If the security officer or manager determines that the residue from such a screen size consistently reflects excessive destruction, the security screen perforation size may be increased to $\frac{5}{16}$ -inch (7.94-mm), provided all processing through the device employs the "secure volume" concept and 50-pound minimum loads. Further, frequent residue examinations are to be made by the security officer or manager to insure compliance with paragraph 9-101.

K-5. Appropriate material destruction techniques and methodologies

Shredding, pulping, and pulverizing machines built to above Federal Interim Specifications are used primarily in the destruction of classified paper-based products. Classified waste containing typing ribbon, aluminum and plastic offset printing mats, and other nonpaper-based products require special handling. They should be segregated, marked to reflect their content and classification, and dealt with on an individual basis. These items can cause serious damage if allowed to accidentally enter some of these machines. Consequently, every effort should also be exerted to keep foreign matter out of burn bags. Nonpaper-based classified material should be disposed of as follows when a pyrolytic furnace is not available for its inappropriate:

a. *Nonwater-soluble plastic coated, waxed paper, or similar material.* This type material will not be allowed to enter wet pulping systems. (Carbon paper is an exception, since it has relatively low tensile strength.) When possible, this type of material should be burned in a pyrolytic furnace, destroyed in one of the high-capacity dry pulverizing systems, or shredded.

b. *Typewriter ribbons and cassettes (mylar, nylon, and cotton-based ribbon).* This category of material should be destroyed in a pyrolytic furnace, since any other method involves both a serious risk of damage to the mechanical destruction equipment and the attendant mess of manual handling. Shredding, chopping, and hammer mill pulverizing entail the necessity of removing the ribbon from its reel by radially slitting with a razor blade. (This insures that no one strip is longer than 25.4 cm (10 inches).) Longer strips have a tendency to become entangled in destruction equipment. Once cut

from the reel, this material should be fed into the destruction system intermixed with paper-based material, sufficient to assist with its being purged from the system. A heavy-duty (1.5 horsepower or larger) crosscut security shredder can be used if fed slowly; however, the standard office-type class I or II shredder should not be used. When using a heavy-duty shredder, the strips of ribbon must be fed in so that they are also sliced across their longest dimension. This will minimize the possible jamming of the machine by having strips wrap around the cutting reel. When any other dry destruction process is used for ribbon strips, a security screen appropriate for TOP SECRET paper-based material must be used.

c. *Original microfilm and microfiche and other silver-based photographic material.* This category of material (having a silver content), to include black and white and colored photographs and negatives, x-rays, aerial films and photographs, and unexposed, expired film, should always be segregated and destroyed by pyrolysis in a silver reclamation furnace for both security and economic reasons. The silver content of these items remains with the ash and may be salvaged very profitably.

d. *Duplicate microfilm and microfiche.* Microfilm and microfiche duplicates normally are made by processes that do not employ silver. Therefore, this type of material can be burned along with other paper and plastic materials in a pyrolytic furnace. Where burning is not permitted, consideration should be given to centralized collection for pyrolytic destruction at another location. Two mechanical destruction devices for use with classified non-COMSEC plastic base micrographic products have been approved for use. They produce extremely fine particulate and when employed in conjunction with the "Secure Volume Concept" achieve the requisite level of security. Further information on these commercial devices is available from the Commander, Intelligence Material Activity (IMA), ATTN: AMXIM-PS, Fort Meade, MD 20755-5315. As a last resort, a properly screened ($\frac{1}{16}$ -inch (1.588-mm) or smaller) hammer mill may be used. Hammer mills must be fed plastic film and other plastic-based materials very slowly to avoid heat buildup. It is best to wait and intersperse batches of paper between charges of film to allow cooling and to remove softened plastic from the hammer mill. Further information on these commercial devices is available from IMA.

e. *Equipment and devices.* Equipment and devices and other solid objects are best destroyed in a pyrolytic furnace. Where destruction by exposure to flame is insufficient to achieve the necessary secure level of destruction, other means must be used. Dependent upon the nature of the item to be destroyed, the means selected must achieve desired results (para 9-101) and yet involve a minimum of hazard for personnel involved. Several common methods are listed below.

- (1) Burning and melting with an oxyacetylene torch.
- (2) Sledge hammer and hacksaw demolition.
- (3) Use of local smelter or foundry retort or open hearth or other furnace to melt beyond recognition.
- (4) Crushing by hydraulic press beyond recognition.
- (5) Hogging in a heavy-duty, industrial-type hogger equipped with a suitable security screen.

f. *Magnetic Storage Media (MSM) (such as materials for audio and video recorders, computers, and ADP office equipment).* Advanced technology has surfaced new magnetic recording materials that differ markedly in their magnetic properties from the low energy ferrous oxide coating of the 1960's and early 1970's. Outward appearance provides no clues, and if not labeled, they cannot be distinguished from the old low energy materials. The significance of this is that the National Security Agency (NSA) approved degaussers, listed in table K-2 (extracted from AR 380-380 (reference (h))), were only tested using the ferrous oxide (low energy) material. These new high energy (above 325 oersted coercivity) materials may or may not be adequately erased by these degaussers. The problem is currently under investigation by NSA. Until it is resolved, Army elements should not declassify degaussed material. Degaussing can be used as means of downgrading TOP SECRET and SECRET magnetic storage media to CONFIDENTIAL. Video tape is almost always high energy type MSM material and computer tape and ADP MSM are usually the low energy type. However,

exceptions do exist; audio tape cassettes may be in either category. Unless the user positively knows that the coercivity level of the material is below 325 oersteds, the user should not declassify MSM after degaussing. MSM can, however, be destroyed by mechanical

methods of cutting, incineration, or melting at temperatures above 600° Fahrenheit. Beware of the toxic fumes resulting from melting or smoldering plastics. When destroying magnetic media in a hammer mill, avoid heat build-up by slow feeding and the inter-mix of paper-based material.

**Table K-1
Destruction Guidelines—Secure Volume Concept ¹**

Equipment	Micro Film/Fiche	TS Paper Base	TS Plastic Base	Secret or Lower
Pyrolytic Furnace	Yes	Yes	Yes	Yes
Shredders (Size)				
(1) 1/32" by 1/2" or less	No	Yes	Yes	Yes
(2) 3/32" by 1/2"	No	No	No	Yes ²
(3) 1/32" continuous strip	No	No	No	Yes
Wet pulpers with 1/4" screen ³	No	Yes	No	Yes (Paper only)
Pulverizers				
Hammer Mill ⁴	Yes	Yes (with 1/4" screen)		
Chopper ⁵	No	Yes (with 3/16" screen)		
Hoggers and Hybrids ⁶	No	Yes (with 1/4" to 5/16" screen)		

Notes:

¹ Secure volumes should equal or exceed: For 1/32" shredders— 20 pages of similar type paper and print, when first used, to ensure a secure volume in waste receptacle. For 2/32;" computer center machines a minimum of 400 pages is required to create a secure volume. For burning, or wet or dry pulverizing— 108 cubic inches (9" X 12" X 1") of similar type material or more each disposal cycle.

² This shredder is approved only for computer printouts in mass, ADP cards, and computer tapes (two at a time) classified SECRET and below.

³ Manufacturers: SOMAT, Pagar, etc.

⁴ Manufacturers: J.B. Sedberry, W. W. Grinder, etc., with 1/6" or smaller security screen.

⁵ Manufacturers: SEM, DAVCO, etc.

⁶ Manufacturers: DDS, Jacksonville Blow Pipe, etc.

**Table K-2
NSA-approved magnetic tape degaussing devices ¹**

Manufacturer/model ²	Floppy disk adapter	Cassette adapter ²
General Kinetics Inc. (GKI) Magnetic Tape Eraser/K80	Not required	K80-R
AMPEX Magnetic Tape Degausser/SE20		
Hewlett-Packard Automatic Tape Degausser/3603A		
Bell and Howell or Consolidated Electrodynamics Corp. Automatic Tape Degausser/TD-2903-4A/TD 2903-4B	P/N 529872	P/N 531972
Electro-Matic Products Conveyorized Degausser/2PTFB15-15/2PTFB15-18 ³	Not required	Not required
Data Devices International/Cambrian Computer Link Corp./515	P/N 529872 Attachment supplied	P/N 531972 Attachment supplied

Notes:

¹ The commercial tape degaussing devices and adapters discussed in this table have been approved by NSA for the effective erasure of magnetic tapes and other magnetic media on which classified or sensitive data have been written. (In addition, see para 5f.)21 NSA drawing 98230-ON126996 can be used to make an adapter for degaussing magnetic cards. (Not required for Electro-Matic products.)

² For tapes wider than 1/2", the tape must be turned and degaussed again.

³ These larger conveyerized degaussers, while more costly, are more suitable for large DPLs processing large quantities of tapes.

Appendix L
Section 793, Title 18, United States Code Gathering,
Transmitting, or Losing Defense Information

793 Gathering, transmitting or losing defense information.

a. Whoever, for the purpose of obtaining information respecting the national defense with intent or reason to believe that the information is to be used to the injury of the United States, or to the advantage of any foreign nation, goes upon, enters, flies over, or otherwise obtains information concerning any vessel, aircraft, work of defense, navy yard, naval station, submarine base, fueling station fort, battery, torpedo station, dockyard, canal, railroad, arsenal, camp factory, mine, telegraph, telephone, wireless, or signal station, building, office, research laboratory or station or other place connected with the national defense owned or constructed, or in progress of construction, or in progress of construction by the United States or under the control of the United States, or of any of its officers, departments, or agencies, or within the exclusive jurisdiction of the United States, or any place in which any vessel, aircraft, arms, munitions, or other materials or instruments for use in time of war are being made, prepared, repaired, stored, or are the subject of research or development, under any contract or agreement with the United States, or any department or agency thereof, or with any person on behalf of the United States, or otherwise on behalf of the United States, or any prohibited place so designated by the President by proclamation in time of war or in case of national emergency in which anything for the use of the Army, Navy, or Air Force is being prepared or constructed or stored, information as to which prohibited place the President has determined would be prejudicial to the national defense; or

b. Whoever, for the purpose aforesaid, and with like intent or reason to believe, copies, takes, makes, or obtains, or attempts to copy, take, make, or obtain, any sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, document, writing, or note of anything connected with the national defense; or

c. Whoever, for the purpose aforesaid, receives or obtains or agrees or attempts to receive or obtain from any person, or from any source whatever, any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note, of anything connected with the national defense, knowing or having reason to believe, at the time he receives or obtains, or agrees or attempts to receive or obtain it, that it has been or will be obtained, taken, made, or disposed of by any person contrary to the provisions of his chapter; or

d. Whoever, lawfully having possession of, access to, control over, or being entrusted with any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense, which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted or attempts to communicate, deliver, transmit or cause to be communicated, delivered or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it on demand to the officer or employee of the United States entitled to receive it; or

e. Whoever having unauthorized possession of, access to, or control over any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered or transmitted or attempts to communicate, deliver, transmit or cause to be communicated, delivered or transmitted the same

to any person not entitled to receive it, or willfully retains the same and fails to deliver it on demand to the officer or employee of the United States entitled to receive it; or

f. Whoever, being entrusted with or having lawful possession or control of any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, (1) through gross negligence permits the same to be removed from its proper place of custody or delivered to anyone in violation of his trust, or to be lost, stolen, abstracted, or destroyed, or (2) having knowledge that the same has been illegally removed from its proper place of custody or delivered to anyone in violation of his trust, or lost, or stolen, abstracted, or destroyed, and fails to make prompt report of such loss, theft, abstraction, or destruction to his superior officer—

Shall be fined not more than \$10,000 or imprisoned not more than ten years, or both.

g. If two or more persons conspire to violate any of the foregoing provisions of this section, and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be subject to the punishment provided for the offense which is the object of such conspiracy.

Appendix M
Section 794, Title 18, United States Code Gathering
or Delivering Defense Information to Aid Foreign
Government

794 Gathering or delivering defense information to aid foreign government

a. Whoever, with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign nation, communicates, delivers, or transmits, or attempts to communicate, deliver, or transmit, to any foreign government, or to any faction or party or military or naval force within a foreign country, whether recognized or unrecognized by the United States, or to any representative, officer, agent, employee, subject, or citizen thereof, either directly or indirectly, any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, note, instrument, appliance, or information relating to the national defense, shall be punished by death or by imprisonment for any term of years or for life.

b. Whoever, in time of war, with intent that the same shall be communicated to the enemy, collects, records, publishes, or communicates, or attempts to elicit any information with respect to the movement, numbers, description, condition, or disposition of any of the Armed Forces, ships, aircraft, or war materials of the United States, or with respect to the plans or conduct, or supposed plans or conduct of any naval or military operations, or with respect to any works or measures undertaken for or connected with, or intended for the fortification or defense of any place, or any other information relating to the public defense, which might be useful to the enemy, shall be punished by death or by imprisonment for any term of years or for life.

c. If two or more persons conspire to violate this section, and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be subject to the punishment provided for the offense which is the object of such conspiracy.

Appendix N
Section 795, Title 18, United States Code
Photographing and Sketching Defense Installations

795 Photographing and sketching defense installations

a. Whenever, in the interest of national defense, the President defines certain vital military and naval installations or equipment as requiring protection against the general dissemination of information relative thereto, it shall be unlawful to make any photograph, sketch, picture, drawing, map, or graphical representation of such vital military and naval installations or equipment without first obtaining permission of the commanding officer of the military or naval post, camp, or station, or naval vessels, military and naval aircraft, and any separate military or naval command concerned, or higher authority, and promptly submitting the product obtained to such commanding officer or higher authority for censorship or such other action as he may deem necessary.

b. Whoever violates this section shall be fined not more than \$1,000 or imprisoned not more than one year, or both.

Appendix O
Section 797, Title 18, United States Code Publication
and Sale of Photographs of Defense Installations

797 Publication and sale of photographs of defense installations

On and after thirty days from the date upon which the President defines any vital military or naval installation or equipment as being within the category contemplated under section 795 of this title, whoever reproduces, publishes, sells, or gives away any photograph, sketch, picture, drawing, map, or graphical representation of the vital military or naval installations or equipment so defined, without first obtaining permission of the commanding officer of the military or naval post, camp, or station concerned, or higher authority, unless such photograph, sketch, picture, drawing, map, or graphical representation has clearly indicated thereon that it has been censored by the proper military or naval authority, shall be fined not more than \$1,000 or imprisoned not more than one year, or both.

Appendix P
Section 798, Title 18, United States Code Disclosure
of Classified Information

798 Disclosure of classified information

a. Whoever knowingly and willfully communicates, furnishes, transmits, or otherwise makes available to an unauthorized person, or publishes, or uses in any manner prejudicial to the safety or interest of the United States or for the benefit of any foreign government to the detriment of the United States any classified information

—
(1) concerning the nature, preparation, or use of any code, cipher, or cryptographic system of the United States or any foreign government; or

(2) concerning the design, construction, use, maintenance, or repair of any device, apparatus, or appliance used or prepared or planned for use by the United States or any foreign government for cryptographic or communication intelligence purposes; or

(3) concerning the communication intelligence activities of the United States or any foreign government; or

(4) obtained by the processes of communication intelligence from the communications of any foreign government, knowing the same to have been obtained by such processes—shall be fined not more than \$10,000 or imprisoned not more than ten years, or both.

b. As used in subsection (a) of this section—the term “classified information” means information which, at the time of a violation of this section, is, for reasons of national security, specifically designated by a United States Government Agency for limited or restricted dissemination or distribution; The terms “code”, “cipher,” and “cryptographic system” include in their meanings, in addition to their usual meanings, any method of secret writing and any mechanical or electrical device or method used for the purpose of disguising or concealing the contents, significance, or meanings of communications; The term “foreign government” includes in its meaning any person or persons acting or purporting to act for or on behalf of any faction, party, department, agency, bureau, or military force of or within a foreign country, or for or on behalf of any government or any person or persons purporting to act as a government within a foreign country, whether or not such government is recognized by the United States; The term “communication intelligence” means all procedures and methods used in the interception of communications and the obtaining of information from such communications by other than the intended recipients; The term “unauthorized person” means any person who, or agency which, is not authorized to receive information of the categories set forth in subsection (a) of this section, by the President, or by the head of a department or agency of the United States Government which is expressly designated by the President to engage in communication intelligence activities for the United States.

c. Nothing in this section shall prohibit the furnishing, upon lawful demand, of information to any regularly constituted committee of the Senate or House of Representatives of the United States of America, or joint committee thereof.

Index

- Abbreviations, 4-202, 4-302, 4-305
- Access, 1-300, 7-100-7-206
- Accountability, 7-304
- ACED. *See* Anti-Compromise Emergency Destruct
- Activity entry and exit, 5-300-5-303
- Addressing, 8-201
- ADP. *See* Automatic Data Processing
- Administrative discrepancies, 14-103
- Administrative violations, 14-103
- Adverse action, 2-103, 14-101, 14-103
- Agency Information Security Program Data Report, 13-400
- Agency of origin, identification of, 4-103
- Aircraft, 8-101, 8-102, 8-104, 8-301-8-303
- Alarm systems, 5-101, 5-102, appendix H
- Anti-Compromise Emergency Destruct (ACED), 5-203
- Archivist of the United States, 3-200, 3-202
- Articles from public media, 4-102
- Associated markings, 1-301, 4-310
- Atomic energy material, 1-204. *See also* Restricted Data; Formerly Restricted Data
- Attention lines, 8-201
- Automatic Data Processing (ADP)
 - Internal storage, 4-304
 - Media, 4-304, 7-304, 8-202
 - Products, 4-202, 4-303, 4-305
 - Punched cards, 4-303, 8-202
 - Systems, 1-206
- AWOL. *See* Knowledgeable AWOL
- Basic scientific research information, 2-204, 2-205
- Bibliographies, 4-209
- Bills of lading, 8-105
- Briefcases, 8-200
- Bulky material, 8-105
- Burn bags, 9-102, 9-103
- Carbon paper, 4-307, 5-201, 9-104
- Carve-out, 1-302, 12-105, 12-108
- CCI. *See* Controlled Cryptographic Item
- Certified mail, 8-103
- Challenges to classification. *See* Classification, challenges
- Changes
 - Classification guides, 2-400
 - Declassification instructions, 3-600
 - Top Secret documents, 7-300
- Charts, 4-202, 4-301
- Classification
 - Approval, 2-101
 - Authority, 1-303, 1-600, 4-104, 11-100. *See also* Original classification, authority
 - Categories, 2-202
 - Challenges, 2-103
 - Conflicts, 2-500-2-503
 - Criteria, 2-202
 - Decisions, 2-200, 2-201
 - Derivative, 1-316, 1-601, 2-212, 4-401
 - Distribution statements, 2-405
 - Doubts about, 1-400
 - Duration of, 1-400, 2-300-2-302, 3-100, 4-601, 11-101
 - Evaluations, 2-600
 - Guides and guidance, 1-304, 2-102, 2-400-2-406, 2-901, 4-401, appendix G
 - Improper, 14-101
 - Levels, 1-500-1-503
 - Limitations on, 2-204
 - Of previously unclassified information, 2-801, 2-802
 - Planning, 2-102
 - Policy, 1-400
 - Reevaluation of, 2-210, 6-112
 - Source of, 4-103, 4-104, 4-207
 - Statements, 4-202
 - Tentative, 2-600, 2-702
- 'Classified by' line, 4-104, 4-207, 4-402
- Classified Document and Material Storage Standards and Information, appendix H
- Classified equipment, 8-104, 8-200
- Classified information, 1-305
- Classified Material Destruction Standards, appendix K
- Classified meeting, 1-305
- Classified waste, 7-106, 9-104
- Classifier, 1-306, 4-207
 - Accountability of, 2-100
- Clearance. *See* Security, clearance
- Cleared carriers, 8-102, 8-103
- CNWDI. *See* Critical Nuclear Weapon Design Information
- Code words, 7-209, 12-104, appendix C
- Colleges, 7-106
- Combat operations, 1-203
- Combinations
 - Changing, 5-104, 5-202
 - Classifying, 5-104
 - Dissemination, 5-104
 - Recording, 5-104
- Commercial aircraft, 8-301-8-303
- Communications security (COMSEC) information. *See* COMSEC information
- Communist countries, 5-205, 10-104, appendix J
- Compilation, 2-211
 - Marking of, 4-203
- Component
 - Definition. *See* DoD Component
 - Marking, 4-201
- Compromise, 1-308, 2-209, 2-210, 4-102, 5-202, 5-205, 6-100-6-109, 8-104, 8-200
- COMSEC information, 1-205, 1-307, 4-504, 5-203, 7-102, 7-206, 8-102, 8-103, 8-106, 8-202, 13-200
- Conferences, 5-205, 7-210, 10-104
- Confidential information, 1-503
 - Control of, 7-208, 7-302
 - Dissemination of, 7-208
 - Receipts for, 8-202
 - Storage of, 5-102
 - Transmission of, 8-103
- Confidential foreign source, 2-203
- Confidential source, 1-309, 2-202, 2-203, 4-102
- Congress, 7-101
- Constant Surveillance Service (CSS), 8-103
- Construction standards, appendix H
- Container. *See* Security, containers
- Container checks, 5-202
- Continental United States (CONUS), 1-310
- Continuous evaluation of eligibility, 7-105, 10-404, 13-304
- Contractors. *See* Industrial security
- Contracts. *See* Industrial security
- Controlled Cryptographic Item (CCI), 1-311
- CONUS. *See* Continental United States
- Conversations, 5-204
- Copying machines. *See* Reproduction, equipment
- Correspondence about unauthorized disclosure, 2-209
- Courts, 7-101
- Cover sheets, 4-205, 5-201
- Criminal acts, 14-104
- Critical Nuclear Weapon Design Information (CNWDI), 1-312, 4-202, 12-101
- Cryptographic system, 5-204, 8-101
- Cryptology (cryptographic information), 1-603, 3-202, 3-203, 6-101, 13-200
- CSS. *See* Constant Surveillance Service
- Custodian, 1-313
 - Responsibilities, 5-200
- Damage assessments, 6-105, 6-107
- Damage criteria, 1-501, 1-502, 1-503
- DEA. *See* Drug Enforcement Administration
- Debriefings, 10-105
- Declassifications, 1-314, 2-301-2-302, 3-100-3-602, 4-400, 11-200-11-202
 - Authority, 1-603
 - Consultation, 11-202
 - Coordination, 3-102
 - Date, 2-301, 4-103, 4-401, 4-402
 - Event, 1-315, 2-301, 2-400, 4-103, 4-402
 - Markings, 4-207, 4-305, 4-400-4-402
 - Policy, 1-401
 - Review, 4-401, 7-101, 7-105. *See also* Mandatory review; Systematic review
- 'Declassify on' line, 4-402, 11-304
- Defense Courier Service, 8-101
- Defense Information Security Committee (DISC), 13-500-13-501
- Defense Investigative Service (DIS), 10-105
- Defense Technical Information Center (DTIC), 2-405, 2-801
- Delegation of original classification authority, 1-600
- Deliberate compromise, 6-109
- Deputy Under Secretary of Defense (Policy) (DUSD(P)), 12-101, 12-103-12-109, 13-102, 13-200, 13-304, 13-400, 13-500-13-501
- Derivative Classification. *See* Classification, derivative
- Desk, 5-202
- Destruction, 9-100-9-105, appendix K
 - Certificates, 7-300, 9-103, 9-105
 - Equipment, 5-203, appendix K
 - Methods, 9-101, appendix K
 - Official, 9-102
 - Priorities, 5-203
 - Records, 9-102-9-103
 - Standards, 9-101, appendix K
- Disagreements about classification. *See* Classification, conflicts
- DIS. *See* Defense Investigative Service

DISC. *See* Defense Information Security Committee
Disciplinary action, 1-201
Disclosure records, 7-300
Discovery of Compromise, 6-102
Discs and disc packs, 4-304
Dissemination, 7-200-7-210
Dissertations, 7-106
Distribution lists, 7-207, 7-208
Distribution of classification guides, 2-405
Documents, 1-317, 2-206
 Component marking, 4-201
DOD Component, 1-318
Double-check. *See* End-of-day checks
Doubts, resolution of. *See* Classification, doubts about
Downgrading, 1-319, 2-803, 3-500-3-501, 4-103, 4-402
 Authority, 1-603
Drafts, 5-201
Drawings, 4-301
Drug Enforcement Administration, 7-104
DTIC. *See* Defense Technical Information Center
Duration of classification. *See* Classification, duration of
DUSD(P). *See* Deputy Under Secretary of Defense (Policy)
Electronically transmitted messages, 4-103, 4-207, 4-402
Emergency
 Destruction, 5-203
 Planning, 5-203
End-of-day checks, 5-202
Envelopes, 8-200
Equipment, items of, 2-207
Equivalent Foreign and International Pact Organization Security Classifications, appendix A
Escorts, 8-102, 8-300-8-303
Espionage, 6-109, 10-101
Espionage Act, appendixes L, M, N, O, P
Event. *See* Declassification event
Exercise terms, 7-209, appendix C
Express mail, 8-103
Extension of duration of classification, 2-302, 4-601
Extracts, 2-212, 4-203, 4-600, 11-304
FAA. *See* Federal Aviation Administration
Faculty members, 7-106
FBI. *See* Federal Bureau of Investigation
Federal Aviation Administration, Security Field Offices, 8-302, appendix D
Federal Bureau of Investigation, 7-104, 10-105
Field operations, 5-102, 13-304
Field safes, 5-102
File folders, 4-205
Films, 4-302
First class mail, 8-103
'For Official Use Only,' (FOUO), 1-500
Foreign countries, security in, 5-206
Foreign disclosure of classification guides, 2-400
Foreign government information, 1-320, 2-203, 3-305, 4-103, 4-104, 4-202, 11-100-11-401, appendix A
'Foreign Government Information' marking, 11-304
Foreign governments, 7-102
 Transmission to, 8-104, 8-202
Foreign intelligence, 7-203, 12-101
Foreign interest, representatives of, 1-329
Foreign nationals, 1-320, 5-205, 5-206, 7-102, 7-105, 15-303
Foreign Relations Series, 3-601
Foreign representative, 1-320
Foreign travel briefing, 10-104
Formerly Restricted Data, 1-204, 1-321, 3-202, 3-307, 4-102, 4-202, 4-204, 4-207, 4-402, 4-502, 7-204
Forms
 DA Form 455, 7-300, 8-202
 DA Form 969, 7-300
 DA Form 1574, 6-105
 DA Form 1575, 2-103, 3-501
 DA Form 1965, 8-202
 DA Form 2134, 6-102
 DA Form 2543, 10-105
 DA Form 2692, 10-105
 DA Form 3964, 5-200, 7-300, 7-301, 7-305, 8-202, 9-103
 DD Form 2, 8-302
 DD Form 173, 4-207
 DD Form 254, 1-304, 2-404, 2-901, 12-108
 DD Form 844, 7-305
 DD Form 1513, 8-104
 DD Form 2024, 2-406, appendix G
 DD Form 2501, 5-300, 5-302
 SF 135, 15-101, 15-304
 SF 153, 8-202
 SF 189, 10-102, 10-105
 SF 311, 9-105, 13-400
 SF 700, 5-104, 5-202
 SF 701, 5-202
 SF 702, 5-202
 SF 703, 4-205, 5-201
 SF 704, 4-205, 5-201
 SF 705, 4-205, 5-201
 SF 706, 4-304
 SF 707, 4-304
 SF 708, 4-304
 SF 710, 4-304
FOUO. *See* For Official Use Only
Freedom of Information Act, 2-204, 3-303, 3-306, 3-602, 10-100
GAO. *See* General Accounting Office
General Accounting Office (GAO), Officials Authorized to Certify Security Clearances, 7-101, appendix B
General Counsel, DoD, 6-105
General officers, 10-105
General Services Administration
 Approved Security Container, 5-101, 5-105, 5-200
Government installation, 1-321
Government Printing Office, 7-101
Graphs, 4-202
Hand-carrying, 8-101, 8-102, 8-300, 8-301, 8-302, 8-303, 10-106
 Approval of, 8-303
Harps, 5-102, appendix H
Historical research, 7-101
IDS. *See* Alarm systems
Illustrations, 4-202
Independent research and development, 2-702
Index of Security Classification Guides (DoD 5200.1-I), 2-406, appendix G
Industrial security, 1-202, 2-702, 2-703, 2-900, 2-901, 5-205, 7-100, 7-101, 7-102, 7-105, 8-101, 8-102, 8-103, 8-104, 8-302, 8-303, 12-105, 12-108
Information, 1-322
 Security, 1-323
Information Security Oversight Office (ISOO), 3-103, 13-102, 14-104
Inspection Checklist for Security Containers, appendix I
Inspections, 5-301, 5-302, 5-303, 12-102, 12-105, 13-303, 13-304, appendix F
Installation. *See* Government installation
Intelligence, 3-202, 3-204, 10-101
 Activity, 1-324
 Sources or methods, 2-203, 3-204, 4-503
Internal Control Review Checklist, appendix F
International organizations, 7-102
Intrusion detection systems. *See* Alarm systems
Inventories
 Top Secret, 7-300
Investigation, 6-104
Investigative agencies, 7-104, 14-104
ISOO. *See* Information Security Oversight Office 'ISOO Report,' 13-400
JCS Information, 7-206, 15-100-15-305
Judicial proceedings, 7-101
Keys, 5-102
Knowledgeable AWOL, 6-110
Law enforcement agencies, 7-104
Legal proceedings, 7-101
Limitations on classification, 2-204
Limited access authorizations, 7-101
Limited Official Use, 1-500
Locking bars, 5-102, 5-103
Lock-outs, 5-105, appendix I
Locks, appendix H
 Electrical, 5-104
Loss of classified information, 6-102, 6-103
Magnetic
 Cards, 4-304
 Tape, 4-304
Mail, 7-303, 8-102, 8-103
Maintenance of security containers, 5-105
Management, 13-100-13-501
Mandatory review, 1-603, 2-204, 3-300-3-307, 11-202
 Appeals, 3-304
 Fees, 3-304
 Processing, 3-304
 Referral, 3-304
 Requests, 3-303
Map and plan file, 5-102
Maps, 4-301
Marking, 4-100-4-601, 7-304, 8-201, 11-300-11-304, appendix A
 Material, 4-103, 4-300, 4-500
 Requirements, 4-200
Markings, old. *See* Old markings
Material, 1-325
 Classifying, 2-207

Meetings, 1-305, 5-205, 7-210, 10-104
Messages. *See* Electronically transmitted messages
Microfiche, 4-302
Microfilm, 4-302
Microforms, 4-302, 4-400
Money, 5-100
Monitorship, 13-303, 13-304
'Multiple Sources,' 4-103, 4-104
Multiservice programs, 2-401
Narcotics, 5-100
NARA. *See* National Archives and Records Administration
National Archives and Records Administration (NARA), 3-200-3-202, 3-303
National security, 1-326
National Security Agency (NSA), 13-200
National Security Council, 13-100
National Telecommunications and Information Systems Security Committee (NTISSC), 7-102
NATO, 7-205, 10-105
Information, 5-104, 8-103, 9-103, 11-100, 11-300, 11-301, 11-304, 11-400, 11-401, 12-101
Need-to-know, 1-327, 7-100, 7-103, 12-200
Negligence, 14-101
Nicknames, 7-209, 12-104, appendix C
'NOCONTRACT,' 4-503
'NOFORN,' 4-503
Nongovernment
Operations, 1-202
Research and development, 2-204
'Notice of Declassification and Other Associated Markings,' 4-305
NSA. *See* National Security Agency
NTISSC. *See* National Telecommunications and Information Systems Security Committee
Nuclear weapons, 8-107
'OADR.' *See* 'Originating Agency's Determination Required'
Old markings, 2-301, 4-600, 4-601
Open publication, effect of, 2-209
'OPEN-CLOSED' signs, 5-202
Operations Security. *See* OPSEC
OPSEC, 10-101
'ORCON,' 4-503
Original classification, 1-328
Authority, 1-600, 11-100
Identification of, 4-103, 4-104
Records of, 1-602
Requests for, 1-600
'Originating Agency's Determination Required' ('OADR'), 2-301, 4-103, 4-207, 4-401, 4-402, 4-600, 11-304
Overall classification marking, 4-103, 4-200
Overnight storage, 8-300
Packages, 8-200
Padlocks, 5-101, 5-102, 5-202, appendix H
Page marking, 4-200, 4-202, 4-203, 4-206, 4-207, 4-305
Paragraphs, 4-202
Parenthetical markings, 4-202, 4-203, 4-204
Patent Secrecy Act, 2-701
Patents, 2-701
Penalties, 10-101, 14-101-14-103
Photographs, 4-302
Polygraph exams, 12-103
Portion marking, 4-202, 4-203, 4-206, 4-500, 11-302, 11-304
ADP products, 4-202
Posted notice, 4-404
Predecessor orders, 2-301, 2-302
Preliminary inquiry, 6-103
Preparation for transmission, 8-200-8-203
Presidential Appointees, 7-101
Information, 3-301
Presumption of damage, 2-203
Private sources, 2-700-2-703
Project phases, 2-403
'PROPIN,' 4-503
Protected distribution system, 8-101
Protective Security Service (PSS), 8-102
PSS. *See* Protective Security Service
Punched cards. *See* Automated Data Processing, punched cards
Receipts, 8-103, 8-104, 8-201, 8-202
Secret, 7-301
Top Secret, 7-300
Receiving classified information, 7-303
Reclassification, 2-204
Recordings, 4-302
Records of original classification authority, 1-602
Reevaluation of classification, 2-210
References, 2-204, 2-206, 4-209
Refresher briefings, 10-103
Registered mail, 8-102, 8-103
Registers
Top Secret, 7-300
Regrade, 1-329
'REL,' 4-503
Remarking, 4-400, 4-402-4-404, 4-600, 4-601
Removal during nonduty hours, 5-200
Reports of investigation, 5-202, 6-104, 6-105, 14-104
Reproduced documents, control of, 7-305
Reproduction, 3-602, 4-200, 4-505, 7-305
Approval, 7-305
Equipment, 7-305
Notices, 7-305
Requests for original classification authority, 1-600
Research, development, test and evaluation, 2-402
Reserve Officers Training Corps (ROTC), 7-101, 7-106
Response times, 5-102
Restricted, 11-300, 11-301, 11-302, 11-304, 11-401
Restricted Data, 1-204, 1-312, 1-330, 2-205, 3-202, 3-307, 4-102, 4-202, 4-204, 4-207, 4-402, 4-501, 7-204, 8-107, 8-201, 12-101
Retention, 7-304, 9-105
Top Secret, 7-300
Review of classification guidance, 2-404, 2-901
Revocation of clearance, 14-104
ROTC. *See* Reserve Officers Training Corps
Safekeeping, 1-402, 5-100-5-106, 11-400, 11-401
Safes. *See* Security, containers
Sample markings, 4-402
Sanctions, 14-101, 14-104
SCI. *See* Sensitive Compartmented Information
Scientific research information, 2-204, 2-205
Scientific research information, secret, 1-502
Control of, 7-301
Destruction of, 7-301, 9-102, 9-103
Dispatch and receipt records, 7-301
Dissemination of, 7-208
Receipts for, 7-301, 8-202
Storage of, 5-102
Transmission of, 8-102
Secret Service, 7-104
'Secure room,' appendix H
Security
Classification authorities, training of, 1-600
Classification Guide Preparation, appendix G
Clearance, 1-331, 7-100, 7-101, 7-105, 7-106, 10-102, 10-105, 10-107, 14-104, appendix B
Education, 10-100-10-106, 13-304
Forces, 5-102
In depth, 5-102
Manager, 13-304
Representative, 1-331
Termination statement, 10-105
Violations, 5-202, 14-101-14-104
Security containers, 5-100-5-106, appendix I
Maintenance of, 5-105
Repair of, 5-105
Turn-in or transfer of, 5-106
Segregation of releasable information, 5-206
Senior official, 13-301-13-303
Sensitive Compartmented Information (SCI), 1-205, 1-332, 2-405, 8-102, 10-106
Serialization of Top Secret documents, 7-300
Shipment, 7-303
Notices, 8-105
Of bulky material, 8-105
Shipping containers, 8-200
Ships, 8-102, 8-103
Short title, 2-206
Simulated classified documents, 4-306
Slides, 4-302
Source, confidential. *See* Confidential source
Source of classification. *See* Classification, source of

Special Access Programs, 1-302, 1-333, 4-205, 4-308, 7-100, 7-201, 7-305, 12-100-12-109
 Special activity, 1-334, 3-204
 State Department Courier System, 8-101
 State-of-art, 2-208
 Stencils, 5-201
 Storage, 5-100-5-106, 8-104
 Equipment, 5-100-5-106
 Purchase of, 5-103
 Facilities (designating), 5-104
 Of Confidential, 5-102
 Of Secret, 5-102
 Of Top Secret, 5-102
 Standards, appendix H
 Student officers, 7-106
 Subjects, 2-206, 4-204
 Suicide, 6-111
 Supplementary controls, 5-101, 5-102
 Systematic review, 1-603, 3-200-3-204, 11-201, appendix M
 Guidelines, 3-201
 Procedures, 3-202
 Tape Cassettes, 4-304
 Telephones, 5-204, 10-101
 Tentative classification, 2-600, 2-702
 Termination briefings, 10-105
 Territories, 1-336
 Test certification label, 5-101, 5-105
 Thesis, 7-106
 'Third agency rule,' 7-202
 Titles, 2-206, 4-204
 Top Secret, 1-501
 Access rosters, 7-300
 Control of, 7-300
 Control Officers, 7-300
 Copy numbering, 7-300
 Destruction of, 7-300,9-102
 Disclosure records, 7-300
 Dissemination of, 7-207
 Inventories of, 7-300
 Receipts for, 7-300
 Registers, 7-300
 Retention of, 7-300
 Serialization, 7-300
 Storage of, 5-102
 Transfer of accountability for, 7-300
 Transmission of, 8-101
 Working papers, 7-304
 Training of classification authorities, 6-100
 Training material, 4-306
 Transferred material, 3-400-3-402
 Translations, 4-208
 Transmission, 8-100-8-303
 Transmittal documents, 4-206, 4-500
 Transportation Plan, appendix E
 Travel briefing. *See* Foreign travel briefing
 Trials, 7-101
 TSCO. *See* Top Secret Control Officer
 Two-man control, 5-102
 Two-person integrity rule, 7-100, 7-305, 9-102
 Typewriter ribbons, 4-307, 5-201, 9-104
 Unauthorized absence, 6-110
 Unauthorized disclosure, 1-335, 2-209, 2-210, 6-100-6-106, 6-110, 14-101, 14-104
 Unclassified material, 4-105, 4-201
 United States, 1-336
 United States Code
 Section 793, Title 18, appendix L
 Section 794, Title 18, appendix M
 Section 795, Title 18, appendix N
 Section 797, Title 18, appendix O
 Section 798, Title 18, appendix P
 Universities, 7-106
 Updating classification guides, 2-404
 Upgrading, 1-337, 2-800, 2-802, 4-403
 Vaults, 5-101, 5-102, appendix H
 Vehicles, 8-200
 Video tapes, 4-302
 Violations, 14-101-14-104
 Of law, 14-104
 Reporting of, 14-104
 Visitors, 7-105
 Waivers and exceptions, 13-200
 Portion marking, 4-202
 Storage, 5-102
 Storage equipment, 5-103
 Top Secret inventories, 7-300
 Top Secret working papers, 7-304
 Transmission, 8-203
 Warning notices, 4-500-4-506
 Witnesses
 Congressional, 7-101
 Court, 7-101
 'Destruction,' 9-103
 'WNINTEL,' 4-504
 Word processing, 4-304
 Working papers, 4-200, 7-304, 9-103

UNCLASSIFIED

PIN 004067-000

USAPA

ELECTRONIC PUBLISHING SYSTEM
TEXT FORMATTER ... Version 2.64

PIN: 004067-000

DATE: 03-09-00

TIME: 16:37:39

PAGES SET: 151

DATA FILE: s63.fil

DOCUMENT: AR 380-5

DOC STATUS: NEW PUBLICATION