Army Regulation 380–5

Security

Department of the Army Information Security Program

Headquarters
Department of the Army
Washington, DC
29 September 2000

UNCLASSIFIED

SUMMARY of CHANGE

AR 380–5
Department of the Army Information Security Program

This revision--

- Emphasizes the responsibilities of Headquarters Department of the Army, the Commander, the Command Security Manager, the Supervisor, and the Individual (chap 1).
- Updates information relating to Restricted Data, Formerly Restricted Data, Sensitive Compartmented Information, Communications Security Information, and Special Access Program Information (chap 1).
- Expands and clarifies exceptional situations and waivers (chap 1).
- Specifies the process for applying original classification (chap 2).
- Removes the declassification statement Originating Officials Determination Required or “OADR” (para 2-11).
- Changes the distribution process for security classification guides (para 2-18).
- Outlines the procedures for challenges to classification (para 2-22).
- Updates information regarding the Army Declassification Program (chap 3).
- Updates information relating to the deadline for automatic declassification, adding an additional 18 months (para 3-5).
- Gives clearer information in regards to destruction, declassification, purging, and clearing (chap 3).
- Replaces the statement “US ONLY” with “NOFORN” (para 4-6).
- Updates Warning Notices for printed documents and those on Automated Information Systems (para 4-12).
- Lists the obsolete restrictions and control markings (para 4-13).
- Outlines the requirements relating to For Official Use Only (FOUO) information (chap 5).
- Replaces the statement “Limited Official Use” with “Sensitive But Unclassified” (para 5-7).
- Outlines the requirements relating to Drug Enforcement Administration Sensitive Information (chap 5).

- Outlines the requirements relating to Department of Defense Unclassified Controlled Nuclear Information (chap 5).
- Outlines the requirements relating to sensitive information and the Computer Security Act of 1987 (chap 5).
- Outlines the requirements relating to distribution statements on scientific and technical documents (para 5-24).
- Outlines the requirements regarding the SF 312 (Classified Information Nondisclosure Agreement (NDA) (chap 6).
- Explains the requirements to access Department of the Army classified information by individuals or agencies outside the Executive Branch (para 6-8).
- Adds guidance to the use of speakerphones (para 6-14).
- Updates guidance on classified meetings, conferences, and acquisition meetings (para 6-18).
- Removes the requirement for the Entry/Exit Inspection Program and the Two-Person Integrity Program (para 6-36).
- Updates the federal specifications for locks (para 7-4).
- Updates procedures for handcarrying of classified material (chap 8).
- Outlines requirements for transportation plans (para 8-7).
- Emphasizes annual refresher training requirements for the security education program (para 9-7).
- Rescinds DA Form 2134 (Security Violation(s) Report) (para 10-3).
- Updates security controls on dissemination and marking of warning notices on intelligence information to include the latest version of Director of Central Intelligence Directive 1/7 (app D).
- Addresses security procedures for documents created for and on automated information systems and Internet web-based display (app E).
- Updates the Management Control Evaluation Checklist (app F, section I).
- Lists and describes the modern army recordkeeping system file numbers associated with this Regulation (app F, section II).
- Updates information of Special Access Programs (app I).
- Updates the abbreviations and terminology lists (glossary).

Headquarters
Department of the Army
Washington, DC
29 September 2000

*Army Regulation 380–5

Effective 31 October 2000

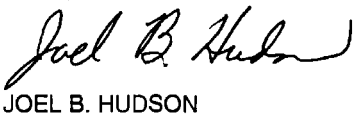
Security

Department of the Army Information Security Program

By Order of the Secretary of the Army:

ERIC K. SHINSEKI
General, United States Army
Chief of Staff

Official:



JOEL B. HUDSON
Administrative Assistant to the Secretary of the Army

History. This publication publishes a revision of this publication. Because the publication has been extensively revised, the changed portions have not been highlighted.

Summary. This regulation implements the policy set forth in Executive Order (E. O.) 12958, "Classified National Security Information", April 17, 1995, with amendments, and DOD 5200.1–R, "Information Security Program." It establishes the policy for classification, downgrading, declassification, and safeguarding of information requiring protection in the interest of national security.

Applicability. This regulation applies to all military and civilian members of the Active Army, Army National Guard of the United States (ARNGUS), and U.S. Army Reserve (USAR) and Department of the Army (DA) personnel. During mobilization, chapters and policies contained in this regulation may be modified by the proponent.

Proponent and exception authority. The proponent of this regulation is the Deputy Chief of Staff for Intelligence. The Deputy Chief of Staff for Intelligence has the authority to approve exceptions to this regulation that are consistent with controlling law and regulation, and as stated in this regulation. Paragraph 1–20 of this regulation further delineates waiver and exception to policy authority.

Army management control process. This regulation contains management control provisions and identifies key management controls that must be evaluated.

Supplementation. Supplementation of this regulation is permitted at command option, but is not required.

Suggested Improvements. Users are invited to send comments and suggestions on DA Form 2028, Recommended Changes to Publications and Blank Forms, through command channels to HQDA DCSINT (DAMI–CH), 2511 Jefferson Davis Highway, Suite #9300, Arlington, VA 22209–3910.

Distribution. This publication is available in electronic media only and is intended for command levels A, B, C, D, and E for the Active Army, the Army National Guard, and the U.S. Army Reserve.

Contents (Listed by paragraph and page number)

*This regulation supersedes AR 380–5, 25 February 1988; AR 380–150, 15 September 1982; AR 381–1, 12 February 1990; DA Pamphlet 380–1, 23 March 1990, and rescinds DA Form 2134, Security Violation(s) Report, January 1983.

UNCLASSIFIED

Contents—Continued

Contents—Continued

Contents—Continued

Contents—Continued

Contents—Continued

Contents—Continued

Contents—Continued

Contents—Continued

Appendixes

Contents—Continued

Table List

Figure List

Contents—Continued

RESERVED

Chapter 1
General Provisions and Program Management

Section I
Introduction

1–1. Purpose
This regulation establishes the policy for the classification, downgrading, declassification, transmission, transportation, and safeguarding of information requiring protection in the interests of national security. It primarily pertains to classified national security information, now known as classified information, but also addresses controlled unclassified information, to include for official use only and sensitive but unclassified. For the purposes of this regulation, classified national security information, or classified information, is defined as information and/or material that has been determined, pursuant to EO 12958 or any predecessor order, to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary or readable form. This regulation implements Executive Order (EO) 12958 and Department of Defense Regulation 5200.1–R. This regulation contains the minimum Department of the Army (DA) standards for the protection of classified information and material. Such standards may be enhanced but never lessened at command option. This regulation also establishes the DA policy on the safeguarding of Restricted Data (RD) and Formerly Restricted Data (FRD) as specified by the Atomic Energy Act of 1954. This regulation also provides guidance on the proper handling of sensitive unclassified material. A restatement and interpretation of the policy concerning the protection of controlled unclassified information is included in this regulation as chapter 5. This regulation does not establish the special, additional policy for the safeguarding of special category information to include Sensitive Compartmented Information (SCI) or Communications Security (COMSEC), which can be found in AR 380–28 and AR 380–40 respectively. It does address the protection of information in an automated environment (app E) and Special Access Programs (SAPs) (app I).

1–2. References
Required and related publications and prescribed and referenced forms are listed in appendix A.

1–3. Explanation of abbreviations and terms
Abbreviations and special terms used in this regulation are explained in the glossary.

Section II
Responsibilities

1–4. Secretary of the Army
The Secretary of the Army (SECARMY) will—

a. Appoint a senior agency official to be responsible for direction and administration of the program within the Army. The SECARMY may designate a separate senior official to be responsible for overseeing SAPs within the Army, if necessary.

b. Commit necessary resources to the effective implementation of the information security program.

c. Establish procedures to ensure that the head of each Major Command (MACOM) that creates, handles or stores classified and sensitive information, appoints an official to serve as security manager for the command, who will provide management and oversight of the command's information security program.

1–5. Headquarters Department of the Army (HQDA)
a. The Deputy Chief of Staff for Intelligence (DCSINT), Headquarters, DA (HQDA), is designated as the DA Senior Official of the Intelligence Community (SOIC), to direct, administer, and oversee the Army's information security program. The Chief of the Counterintelligence/Human Intelligence Division (DAMI–CH), Intelligence Policy Directorate, provides staff support for these functions. The DCSINT will—

(1) Promulgate (or cause to promulgate) policy, procedures, and programs necessary for the implementation of EO 12958 and resulting national and Department of Defense (DOD) Directives (DODD).

(2) Monitor, evaluate, and report on the administration of the Army's information security program. Ensure MACOM, Major Subordinate Commands (MSC) and other agencies, establish and maintain an ongoing self–inspection program, to include periodic reviews and assessments of their classified and sensitive products.

(3) Respond to information security matters pertaining to classified and sensitive information that originated in an Army command that no longer exists and for which there is no successor in function.

(4) Delegate SECRET and CONFIDENTIAL Original Classification Authority (OCA) to other Army officials. The SECARMY is the only Army official that may delegate TOP SECRET original classification authority.

(5) Commit the necessary resources for the effective policy development and oversight of the programs established by this regulation.

b. The Chief, Technology Management Office (TMO), HQDA, is the Army primary contact for the management and oversight of Army and Army–supported SAPs. The Chief, TMO will implement SAPs information security measures and all associated policies necessary to execute the SAPs security policy that is established and directed by the HQDA, DCSINT. See appendix I of this regulation and AR 380–381 for further guidance on SAPs.

c. The Deputy Chief of Staff for Personnel (DCSPER), HQDA, will execute the provisions of section 5.6(c)(7) of EO 12958, and establish policy to ensure that the systems used to evaluate or rate civilian and military personnel performance, include the management of classified, and when possible sensitive, information as a critical element/item/objective to be evaluated in the rating of—

(1) Original classification authorities.

(2) Security managers and security specialists.

(3) All other personnel whose duties significantly involve the creation or handling of classified and sensitive information.

d. The Comptroller of the Army, HQDA, will execute the provisions of section 5.6(c)(8) of EO 12958, establish and implement a system for accounting for the costs associated with the Army implementation of EO 12958, and for reporting those costs to the Director of the Information Security Oversight Office (ISOO) for publication.

1–6. The Commander

Security is a command function. Commanders, Officers in Charge (OIC), and heads of agencies and activities (referred to as commanders), will effectively manage the information security program within their commands, agencies, activities, or areas of responsibility (referred to as commands). Commanders may delegate the authority to execute the requirements of this regulation, where applicable, but not the responsibility to do so. Security, including the safeguarding of classified and sensitive information and the appropriate classification and declassification of information created by command personnel, is the responsibility of the commander. The commander will—

a. Establish written local information security policies and procedures and an effective information security education program.

b. Initiate and supervise measures or instructions necessary to ensure continual control of classified and sensitive information and materials.

c. Ensure that persons requiring access to classified information are properly cleared.

d. Continually assess the individual trustworthiness of personnel who possess a security clearance.

e. Designate a Command Security Manager (CSM) by written appointment. The CSM will be of sufficient rank or grade to effectively discharge assigned duties and responsibilities. As a general requirement, the CSM will be a commissioned officer (0–3 or above), warrant officer, or civilian in the grade of GS–12 or above. The MSC commander may, subject to MACOM or Administrative Assistant to the Secretary of the Army (HQDA SAAA) for the HQDA staff for policy approval, designate a CSM at a lower rank or grade in situations in which the rank or grade of the individual selected is sufficient to effectively discharge assigned responsibilities. The CSM will have direct access to the commander on matters affecting the information security program.

f. Ensure the CSM is afforded security training consistent to the duties assigned.

g. Ensure adequate funding and personnel are available to allow security management personnel to manage and administer applicable information security program requirements.

h. Review and inspect the effectiveness of the information security program in MSCs.

i. Ensure prompt and appropriate responses are given, or forward for higher echelon decision, any problems, suggestions, requests, appeals, challenges, or complaints arising out of the implementation of this regulation.

j. Ensure the prompt and complete reporting of security incidents, violations, and compromises, related to classified and sensitive information, as directed herein.

k. Ensure prompt reporting of credible derogatory information on assigned/attached personnel, to include recommendations for or against continued access.

1–7. The Command Security Manager

The command security manager is the principal advisor on information security in the command and is responsible to the commander for management of the program. The CSM will—

a. Advise and represent the commander on matters related to the classification, downgrading, declassification, and safeguarding of national security information.

b. Establish and implement an effective security education program as required by chapter 9 of this regulation.

c. Establish procedures for assuring that all persons handling classified material are properly cleared. 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 properly prepared, distributed, and maintained.

f. Conduct a periodic review of classifications, assigned within the activity, to ensure that classification decisions are proper.

g. Consistent with operational and statutory requirements, review all classified and sensitive documents in coordination with the Command Records Management Officer. Continually reduce, by declassification, destruction, or retirement, unneeded classified and sensitive material.

h. Submit Standard Form (SF) 311 (Agency Information Security Program Data) to DAMI–CH annually, as required.

i. Supervise or conduct security inspections and spot checks and notify the commander regarding the compliance with this regulation and other security regulations and directives.

j. Assist and advise the commander in matters pertaining to the enforcement of regulations governing the access, dissemination, reproduction, transmission, transportation, safeguarding, and destruction of classified and sensitive material.

k. Make recommendations, based on applicable regulations and directives, on requests for visits by foreign nationals, and provide security and disclosure guidance if the visit request is approved.

l. Ensure the inquiry and reporting of security violations is completed, including compromises or other threats to the safeguarding of classified and sensitive information, in accordance with chapter 10 of this regulation. Recommend to the decision official whether or not administrative sanction is warranted, and/or indicate corrective action that should be taken concerning security violations.

m. Ensure proposed public releases on classified and sensitive programs be reviewed to preclude the release of classified information or other sensitive unclassified information covered under the Freedom of Information Act (FOIA).

n. Establish and maintain visit control procedures in cases in which visitors are authorized access to classified information.

o. Issue contingency plans for the emergency destruction of classified and sensitive information and material and, where necessary, for the safeguarding of classified and sensitive information and material used in or near hostile or potentially hostile areas.

p. Be the single point of contact to coordinate and resolve classification or declassification problems.

q. Report data as required by this regulation.

1–8. The Supervisor

Supervisory personnel (to include those in command positions) have a key role in the effective implementation of the command's information security program. Supervisors, by example, words, and deeds, set the tone for compliance by subordinate personnel with the requirements to properly safeguard, classify, and declassify, information related to national security. The supervisor will—

a. Ensure subordinate personnel who require access to classified information are properly cleared and are given access only to that information, to include sensitive information, for which they have a need–to–know.

b. Ensure subordinate personnel are trained in, understand, and follow, the requirements of this regulation, and local command policy and procedures, concerning the information security program.

c. Continually assess the eligibility for access to classified and sensitive information of subordinate personnel and report to the CSM any information that may have a bearing on that eligibility.

d. Supervise personnel in the execution of procedures necessary to allow the continuous safeguarding and control of classified and sensitive information.

e. Include the management of classified and sensitive information as a critical element/item/objective in personnel performance evaluations, where deemed appropriate, in accordance with Army personnel policy and paragraph 1–5c of this regulation. Supervisors should include the protection of classified and sensitive information as a performance evaluation factor or objective for other personnel as the supervisor deems appropriate.

f. Lead by example. Follow command and Army policy and procedures to properly protect classified and sensitive information and to appropriately classify and declassify information as stated in this regulation.

1–9. The Individual

All DA personnel, regardless of rank, grade, title, or position, have a personal, individual, and official, responsibility to safeguard information, related to national security, that they have access to. All DA personnel will report, to the proper authority, the violations by others that could lead to the unauthorized disclosure of classified and sensitive information. This responsibility cannot be waived, delegated, or in any other respect, excused. All DA personnel will safeguard all information and material, related to national security, especially classified information, which they access, and will follow the requirements of this and other applicable regulations.

Section III
Program Management

1–10. Applicability definition
This regulation governs the Department of the Army information security program and applies to all DA personnel to include military and civilian members of the Active Army, Army National Guard (ARNG), and Army Reserve (USAR). Information relating to national security will be protected by DA personnel and employees against unauthorized disclosure. For the purposes of this regulation, DA personnel includes any active or reserve military personnel or National Guard, assigned or attached to a Department of the Army installation or activity, and persons employed by, assigned to, or acting for, an activity within the Department of the Army, including contractors, licensees, certificate holders, and grantees, and persons otherwise acting at the direction of such an activity.

1–11. General principles
a. All DA personnel, regardless of rank, title, or position, have a personal, individual, and official responsibility for the proper safeguarding and protection of the information they have access to, in particular, classified information.

b. Information will be classified, or protected as sensitive, only when it is in the interest of national security, and downgraded or declassified when it is determined that the information requires, in the interest of national security, a lower degree of protection against unauthorized disclosure than is currently required. Information or material, that requires protection against unauthorized disclosure, in the interest of national security, shall be classified as one of the three following categories or levels, as defined in this regulation:

(1) TOP SECRET.

(2) SECRET.

(3) CONFIDENTIAL.

c. Information and material, classified under this regulation, will be afforded the level of protection, against unauthorized disclosure, commensurate with the level of classification or sensitivity assigned, under the varying conditions that may arise in connection with its use, dissemination, storage, movement, transmission, or destruction. Responsible officials will ensure that classified and sensitive information and materials are adequately protected from compromise. Everyone must be continually aware of possible threats from all–source intelligence efforts of potential adversaries.

d. Access to classified information is authorized only to the following personnel:

(1) Persons with the appropriate need–to–know for the information in order to perform a lawful and authorized governmental function;

(2) Persons who have been granted a security clearance and access authorization at the appropriate level of clearance.

(3) Persons who have executed an appropriate non–disclosure agreement. AR 380–67 contains policy on the personnel security clearance program. Note: The holder, not the potential receiver, of the information, determines the need–to–know and is responsible for verifying the clearance and access authorization of the potential receiver. No person will be granted access to classified information solely by virtue of rank, title, or position.

e. Classified and sensitive information will be maintained only when necessary for the operation of the organization or when its retention is required by law, regulation, or records management policy.

1–12. Legal authority
The statutory authority for this regulation is derived from Title 18, of the United States Code (USC), the Atomic Energy Act of 1954, as amended, Executive Orders, issuances from the Office of Management and Budget (OMB), and the Security Policy Board (SPB).

1–13. Recordkeeping Requirements
This regulation requires the creation, maintenance, and disposition, of records, to document and support the business processes of the Army. Recordkeeping requirements are found in section II of appendix F, of this regulation, and AR 25–400–2.

Section IV
Program Direction

1–14. Background
Within the Federal Government, and the Office of Management and Budget, are a number of offices designed to oversee and implement EO 12958. These offices issue directives, as necessary and these directives are binding to all the components. Directives issued by these offices establish standards for—

a. Classification and marking principles.

b. Agency security education and training programs.

c. Agency self–inspection programs.
d. Classification and declassification guides.

1–15. Information Security Oversight Office Responsibility

The Director of the Information Security Oversight Office (ISOO) is delegated the responsibility for the implementation and monitorship functions of these programs. The details on the make–up and responsibilities of these offices are contained in EO 12958, a reprint of which can be found in appendix B, of this regulation.

Section V
Special Types of Information

1–16. Atomic Energy Information (Restricted Data (RD)/Formerly Restricted Data (FRD))

The primary purpose of this regulation is to implement EO 12958 and its implementing Department of Defense directives. EO 12958 does not apply to information classified as Restricted Data (RD) or Formerly Restricted Data (FRD). Nothing in EO 12958 supersedes any requirement made by, or under, the Atomic Energy Act of 1954, as amended. Of particular importance is that neither RD nor FRD information is subject to the automatic declassification provision of EO 12958, as specified in chapter 3 of this regulation. RD and FRD information will not be declassified without the specific permission of the Department of Energy (DOE). RD and FRD shall be safeguarded, classified, downgraded, and declassified, per the provisions of the Atomic Energy Act of 1954, as amended, and by DOD and Army policy. The Army policy on the marking and safeguarding, of RD/FRD information, is contained in chapters 4 and 6, respectively, of this regulation. RD and FRD information will be safeguarded, as required by this regulation, for other information of a comparable level of security classification. The policy on the classification, downgrading, and declassification, of RD and FRD information, is stated in classification and declassification guidance promulgated by the DOE, or in guidance issued jointly by the DOD and DOE.

1–17. Sensitive Compartmented Information, Communications Security Information, and Special Access Programs Information

Security classification and declassification policies apply to SCI, COMSEC, and SAPs information in the same manner as other classified information (see app C for guidance on declassification of cryptologic information and appendix I, of this regulation, for more information on SAPs). SCI, COMSEC, and SAPs information will be controlled and safeguarded in accordance with AR 380–28, AR 380–40, and AR 380–381, respectively.

Section VI
Exceptional Situations

1–18. Military Operations, Exercises, and Unit Deactivations

a. Military Operations. The provisions of this regulation may be modified, but not lessened, by the commander or senior official, as necessary to meet local conditions relating to combat, combat operations, emergency conditions under operations other than war, to include peacekeeping operations, and any other emergency situation where that operation or situation requires exceptional measures to protect life or Department of the Army assets. The criteria for classification and sensitivity of national security information remains for all situations; however, nothing in this regulation prohibits commanders from protecting any other information they deem necessary, to carry out the military operations and emergency situations identified above. Classified and sensitive information may be introduced into combat areas or zones or areas of potential hostile activity, but only as necessary to accomplish the military mission.

b. Military Exercises. Military exercises pose a unique situation where the handling and protection of classified and sensitive information are concerned. During exercises troops are told to "train as you would fight." When material, used in exercises, are "Classified For Training Only," it will be handled as if it were real world classified and/or sensitive. This is good security practice and can help prevent possible security violations in the future. When real–world classified and/or sensitive material is introduced and/or used in military exercises, every effort will be used to prevent compromise and/or loss. While there may be circumstances and situations where inadvertent disclosure of classified and/or sensitive information may occur, it is up to the command security manager, and ultimately the commander, to ensure that the provisions of chapter 10, of this regulation, are followed.

c. Unit Deactivation. Original classification authority is assigned to a duty position not to an individual person. When an organization has been deactivated, the OCA's responsibilities will revert to their higher headquarters or that organization assuming responsibility over the out–going command's security decisions. Challenges to classification decisions, of the deactivated organization, will be directed to that headquarters with the security responsibilities of the outgoing unit.

1–19. Waivers and Exceptions to Policy

a. This regulation is based on national policy that is applicable to all U.S. Government departments, agencies, and DA personnel. In order to ensure the protection of information related to national security, and allow all agencies to

have confidence in the sharing of information with other agencies, the national, DOD, and DA policy, contained in this regulation, will be followed.

b. Unless otherwise noted, requests for waivers to the requirements contained in this regulation, will be submitted, through command channels, to DAMI–CH. Waivers to DOD requirements will be forwarded by DAMI–CH, for decision to the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I)). For requirements related to Two–Person Integrity (TPI), RD, Foreign Government Information (FGI) (including North Atlantic Treaty Organization (NATO)), and security arrangements for international programs, waivers will be forwarded to the Under Secretary of Defense (Policy)(USD(P)). Waivers for SAPs will be submitted, through SAPs channels, to DAMI–CH for coordination with TMO and, as required, forwarded to the Under Secretary of Defense (Special Programs) (USD(SP)). The ASD(C3I) and USD(P) are responsible for notifying the Director of the ISOO of the waivers approved that involve EO 12958 and its implementing directives.

c. Before submitting a request for waiver, the requesting authority will consider risk management factors such as criticality, sensitivity, and value of the information, analysis of the threats both known and anticipated, vulnerability to exploitation, and countermeasure benefits versus cost (national security cost and resource cost). Requests for waiver must contain sufficient information to permit a complete and thorough analysis to be made of the impact on national security if the waiver is approved. The waiver request will also describe all the factors creating the special situation and the alternative or compensatory measures which make sure the protection afforded the information is sufficient to reasonably deter and detect loss or unauthorized disclosure. The requesting command will maintain documentation regarding approved waivers, including the alternative or compensatory measures approved and in use, and furnish this documentation, upon request, to other agencies and to other Army commands, with whom classified information or secure facilities are shared.

Note: Waivers granted before the effective date of this regulation are canceled no later than one year after the effective date of this regulation. New/updated waiver requests may be submitted prior to cancellation date.

d. Throughout this regulation there are references to policy subject to MACOM approval or subject to policy as the MACOM directs. Where that language, in substance, is used, the MACOM commander, or the HQDA SAAA, for cases involving HQDA and its Field Operating Agencies (FOA), can delegate such approval authority. The delegations will be in writing. A copy of such delegations will be maintained by the appointing official and reviewed periodically for review of need for continuation. Where this regulation specifically specifies waiver authority to a MACOM commander or the HQDA SAAA, that authority resides solely with the MACOM commander or HQDA SAAA and will not be further delegated.

Section VII
Corrective Actions and Sanctions

1–20. General

Commanders will establish procedures to make sure that prompt and appropriate action is taken concerning a violation of the provisions of this regulation, especially in those cases involving incidents which can put classified information at risk of compromise, unauthorized disclosure, or improper classification of information. Such actions will focus on a correction or elimination of the conditions that caused or contributed to the incident.

1–21. Sanctions

a. DA personnel will be subject to sanctions if they knowingly, willfully, or negligently—

(1) Disclose classified or sensitive information to unauthorized persons.

(2) Classify or continue the classification of information in violation of this regulation.

(3) Violate any other provision of this regulation.

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

c. Original classification authority will be withdrawn for individuals who demonstrate a disregard or pattern of error in applying the classification and sensitivity standards of this regulation.

1–22. Reporting of Incidents

EO 12958, paragraph 5.7(e)(2), requires that the director of the ISOO be advised of instances in which classified information is knowingly, willfully, or negligently disclosed to unauthorized persons, or instances of classifying, or continuing the classification of, information in violation of this regulation. Reports of those instances will be submitted through command channels to DAMI–CH for forwarding to the director of the ISOO and other defense officials as appropriate. See chapter 10 for reporting of other security incidents.

Section VIII
Reports

1–23. Reporting Requirements
HQDA is required to report data necessary to support various requirements of EO 12958. Commanders will respond to those data calls when so notified. MACOMs and the HQDA SAAA will also submit a consolidated annual report, for all units under their security responsibility, on SF 311, to reach DAMI–CH no later than 1 October, or other date specified by DAMI–CH, each fiscal year. The report will cover the preceding fiscal year. DAMI–CH will consolidate and submit the annual SF 311 report for the Army. Interagency Report Control Number 0230–GSA–AN applies to this report.

1–24. Command security inspections
MACOM, agency, and MSC commanders will establish and maintain a self–inspection program for their command, and a program to inspect their subordinate units. The program must be based upon program needs and the degree of involvement with classified and sensitive information. The purpose of the program will be to evaluate and assess the effectiveness of the command's protection of classified and sensitive information and adherence to Army policy contained in this regulation. Inspections will be conducted annually unless the command's higher headquarters determines that the quantity of classified and sensitive holdings and material generated does not warrant that frequency. In those cases, inspections will occur not less frequently than once every other year. This will not dismiss other annual requirements outlined in this regulation.

Chapter 2
Classification

Section I
Classification Principles

2–1. Original vs. derivative classification
a. Original classification is the decision to designate a certain item of information as classified, at a particular level, and for a certain duration of time. Often these decisions are communicated in a published Security Classification Guide (SCG). These decisions can only be made by persons designated in writing by either the SECARMY or the DCSINT as Original Classification Authorities (OCA). There are relatively few officials in the Army that have the authority to apply original classification, and relatively few instances of original classification, in most Army commands. Derivative classification is the incorporating, restating, paraphrasing, or generating in new form, information that has already been determined to be classified, and ensuring that it is classified and handled at the level that the OCA has already determined will be done. Derivative classification can be accomplished by any properly cleared personnel. Derivative classifiers are not required to be appointed or designated unless so directed by Command option. Most DA personnel that classify information do so in a derivative manner from some other document or source. Derivative classification is most commonly accomplished by marking classified material based on the guidance from an SCG or from the source document. The derivative classifier must have enough subject matter knowledge to properly interpret and apply the instruction of the classification guidance. The original classification authority decides what portion(s) of a plan, program, or project needs to be classified. The derivative classifier applies that decision to the same type of information restated or generated in a new form.

b. For example, an OCA could make the decision that the maximum effective range of Missile XYZ is classified. The classification authority issues a security classification guide that states that the maximum effective range of the missile will be classified at the SECRET level. When the missile is tested and the results are documented, the person who writes the report, states that the maximum effective range of Missile XYZ is 250 miles, derivatively classifying that item of information as SECRET. In this case, the classification is derived from the security classification guide. Most classification in the Department of the Army is done in a derivative manner. Those DA officials authorized to apply original classification decisions are relatively few in number.

2–2. Policy
Original classification is the initial determination by an OCA that an item of information could be expected to cause damage to national security if subjected to unauthorized disclosure. Damage to the national security means harm to the national defense or foreign relations of the United States from the unauthorized disclosure of the information, to include the sensitivity, value, and utility of that information. It includes military operations in support of national objectives when those operations involve information that meets the criteria of classification. This decision will be made only by persons specifically authorized in writing to do so, have received training in the exercise of this authority, and have program or program support responsibility or cognizance over the information. The decision to

originally classify must be made based on the requirements of this regulation. Delegations of original classification authority will be limited to the minimum required and only to officials who have a demonstrable and continuing need to exercise it.

2–3. Delegation of authority

a. The Secretary of the Army has been granted original classification authority by the President of the United States. TOP SECRET OCA can be delegated only by the SECARMY. SECRET and CONFIDENTIAL original classification authority can only be delegated by the DCSINT or by the SECARMY. Delegation of authority includes information at that level and any lower level(s) of classification. This authority cannot be redelegated.

b. Requests for OCA will be submitted, through command channels, to DAMI–CH. These requests will specify the position title for which the authority is requested and detailed justification for the request. Original classification authority is assigned to a position title and not to an individual person. In order to ensure that the number of OCAs is strictly limited, the request must address why another OCA, within that official's command or area, cannot assume this responsibility.

c. Requests for original classification authority will be granted only when:

(1) Original classification is required during the normal course of operations;

(2) Sufficient expertise and information is available to the prospective original classification authority to allow effective classification decision making;

(3) The need for original classification cannot be handled by other existing OCAs; or

(4) Referral of decisions to existing original classification authorities, at the command or at higher levels in the chain of command, is not practical.

2–4. Required Training

Officials who have been delegated original classification authority will receive training, as required by chapter 9 of this regulation, before exercising this authority.

Section II
Derivative Classification

2–5. Policy

DA personnel who generate material which is to be derivatively classified are responsible for making sure that the classification is properly applied based on the original source material marking and local security classification guides. DA personnel who apply derivative classification should take care to determine whether their paraphrasing, restating, or summarizing of classified information has removed all or part of the basis for classification. Certain information that would otherwise be unclassified, may require classification when combined or associated with other unclassified information. This is referred to as classified by compilation. However, a compilation of unclassified items of information is normally not classified. In unusual circumstances, classification may be required if the combination of unclassified items of information provides an added factor that warrants classification. Similarly, a higher classification may be assigned to compilations of information that warrants higher classification than that of its component parts. Classification on this basis shall be fully supported, in writing, accompanying the compilation document. See paragraph 2–8 for specific classifying criteria.

2–6. Accuracy responsibilities

Officials who sign or approve derivatively classified material are responsible for the accuracy of the derivative classification. This applies to all forms of material and information regardless of the media involved. Personnel accomplishing derivative classification will—

a. Observe and respect the classification determinations made by original classification authorities.

b. Apply markings or other means of identification to the derivatively classified material, as required by this regulation, at the level and for the duration specified by the classification guide or source document. Where classification instructions do not reflect the new marking requirements of EO 12958, mark the level of classification as directed by the classification guide or source document and follow this regulation for all other marking requirements. Derivative classifiers are encouraged to keep informal records of which portions of a draft document are classified and by which source to make the classification of the finished product easier.

c. Use only authorized sources such as classification guides, other forms of official classification guidance, and markings on source material, from which the information is extracted. Refrain from guesswork.

d. Use caution when paraphrasing or restating information extracted from a classified source to determine whether the classification could have been changed in the process.

e. Take appropriate and reasonable steps to resolve doubt or conflicts in classification. In cases of apparent conflict between an SCG and a classified source document, concerning a discrete item of information, the instructions in the SCG will take precedence unless the source document is signed by the original classification authority. In such cases,

the OCA, or the point of contact for answering questions on classification, will be consulted. In the event that it is not possible to consult the OCA, the more restrictive classification instruction will be followed.

f. Make a list of sources used when material is derivatively classified based on "Multiple Sources" (more than one SCG, classified source document, or any combination). A copy of this list will be included in, or attached to, the file or record copy of the material. Derivative classifiers are encouraged to include this listing with all copies of the document, to make later declassification review easier if the file or record copy is unavailable.

g. Contact the classifier of the source document for resolution in cases in which the derivative classifier believes the classification applied to the information is not accurate.

Section III
The Original Classification Process

2–7. General

The decision to apply original classification requires the application of judgment, on the part of the classifier, that the unauthorized disclosure of the information could reasonably be expected to cause damage to the national security, and that the probable damage can be identified or described. It is not necessary for the original classifier to produce a written description of the damage at the time of classification, but the classifier must be prepared to do so if the information becomes the subject of a classification challenge, a request for mandatory review for declassification, or a request for release under the Freedom of Information Act. The decision to classify also has operational and resource impacts as well as impacts affecting the United States technological base and foreign relations. The decision to classify should consider all relevant factors. If there is doubt about classification, the OCA will research the matter to make an informed decision. If, after such research, there is a significant doubt about the need to classify information, it will not be classified. In making a decision to originally classify an item of information, an original classification authority will—

a. Determine that the information has not already been classified.

b. Determine that the information is eligible for classification pursuant to paragraph 2–8 of this regulation.

c. Determine that classification of the information is a realistic course of action and that the information can be protected from unauthorized disclosure when classified.

d. Decide that unauthorized disclosure could reasonably be expected to cause damage to the national security and that this disclosure is identifiable and can be described.

e. Select the appropriate level or category of classification and/or sensitivity to be applied to the information, based on a judgement as to the degree of damage unauthorized disclosure could cause.

f. Determine and include the appropriate declassification, downgrading, and/or exemption category instruction(s) to be applied to the information, when applicable.

g. Make sure that the classification decision is properly communicated so that the information will receive appropriate protection. Security classification guides will be used in this regard where appropriate (see paragraph 2–16).

2–8. Classification criteria

U.S. classification can only be applied to information that is owned by, produced by or for, or is under the control of, the United States Government. This is determined by the original classification authority that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security, and the information falls within one or more of the following categories specified in section 1.5 of EO 12958:

a. Military plans, weapons systems, or operations.

b. Foreign government information.

c. Intelligence activities (including special activities), intelligence sources or methods, or cryptology.

d. Foreign relations or foreign activities of the United States, including confidential sources.

e. Scientific, technological, or economic matters relating to the national security.

f. United States Government programs for safeguarding nuclear materials or facilities.

g. Vulnerabilities or capabilities of systems, installations, projects or plans relating to the national security. Note: When used, these seven classification categories are referred to by their reference letter, preceded by "1.5," the reference location within the EO. For example, "Military plans, weapons systems, or operations" would be "1.5(a)." See paragraph 4–9 for further details on "Classified by" marking.

2–9. Possibility of Protection

a. The OCA must determine that, if classification is applied or reapplied, there is a reasonable possibility that the information will be provided protection from unauthorized disclosure.

b. The reclassification of information which was once classified but was declassified and officially released to the public, by an authorized Army official, and had wide–spread access by the public, is prohibited. Army information that has not previously been disclosed to the public, under proper Army authority, can be classified or reclassified. This includes after a command has received a request for it. However, only if the reclassification is accomplished on a

document–by–document basis, with the participation, or under the direction of, the SECARMY, the Under Secretary of the Army, or the DCSINT. Guidance from DAMI–CH will be requested in those instances. The information that is reclassified must meet the criteria for classified information established in EO 12958 or successor orders and directives. In considering issues of reclassification or classification of previously unclassified information, the OCA will—

(1) Determine that control of the information has not been lost and can still be prevented from being lost; and

(2) In the case of information released to secondary distribution centers, determine that no secondary distribution has been made and can still be prevented.

c. Classified information will not be declassified automatically as a result of any unauthorized disclosure of identical or similar information. In these cases, the OCA will review the situation to determine if continued classification is warranted. 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.

2–10. Levels of classification

a. Once a decision is made to classify, information will be classified at one of the three levels listed below. For each level, the OCA must be able to identify or describe the damage that unauthorized disclosure reasonably could be expected to cause to the national security. These levels are:

(1) TOP SECRET – Will be applied to information in which the unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security.

(2) SECRET – Will be applied to information in which the unauthorized disclosure could reasonably be expected to cause serious damage to the national security.

(3) CONFIDENTIAL – Will be applied to information in which the unauthorized disclosure could reasonably be expected to cause damage to the national security.

b. If there is doubt about the classification level, the OCA will research the matter to make an informed decision. If significant doubt still remains about the classification level to be assigned, the lower level will be assigned.

2–11. Duration of classification

Information will be declassified as soon as it no longer meets the standards for classification. Information will remain classified as long as it is in the interest of national security and meets the criteria stated in this regulation. At the time an item of information is originally classified, the original classifier must decide the length of time the information will require classification and select an appropriate declassification date or event. The term "time or event phased declassification date," used for acquisition programs, is also synonymous with the term "declassification date" as used in this regulation. The declassification date indicates when the information no longer requires protection in the interests of national security. When deciding on the declassification date or event, the following options are the only ones available to the OCA:

a. At the time of original classification, the original classification authority will attempt to establish a specific date or event for declassification based upon the duration of the national security sensitivity of the information. The OCA will attempt to determine a date, within ten years from the date of classification, upon which the information can be automatically declassified. If that is not possible, they will attempt to determine a specific event, reasonably expected to occur within 10 years, that can be set as the signal for automatic declassification of the information. This is referred to as the "ten–year rule." The date or event will not exceed the time frame in subparagraph c, below.

b. If information has originally been assigned a date or event for declassification of ten years or less, in accordance with subparagraph a above, and the OCA later has reason to believe longer protection is required, the classification can be extended for successive periods of up to ten years at a time, not to exceed the time period in subparagraph e, below, where applicable.

c. If unable to determine a date or event that is ten years or less, the OCA will assign an exemption designation to the information, if the information qualifies for exemption from automatic declassification in ten years. This could be done if the unauthorized disclosure of the information could reasonably be expected to cause damage to the national security, if specific information requires a period beyond 10 years from the date of original classification, and the release of the information could reasonably be expected to result in one or more of the following:

(1) Reveal an intelligence source, method, or activity, or a cryptologic system or activity.

(2) Reveal information that could assist in the development or use of weapons of mass destruction.

(3) Reveal information that could impair the development or use of technology within a United States weapon system.

(4) Reveal United States military plans or national security emergency preparedness plans.

(5) Reveal foreign government information.

(6) Damage relations between the United States and a foreign government, reveal a confidential source, or seriously undermine diplomatic activities that are reasonably expected to be ongoing for a period greater than ten years.

(7) Impair the ability of responsible United States government officials to protect the President, the Vice President, and other individuals for whom protection services, in the interest of national security, are authorized.

(8) Violate a statute, treaty, or international agreement. Note: When used, these eight exemption categories are either completely written out or referred to by their reference number preceded by the letter "X." For example, "Violate a statute, treaty, or international agreement" or "X8." See paragraph 4–10 for further details on exemption marking.

d. Information marked for an indefinite duration of classification under prior orders, for example, "Originating Agency's Determination Required" (OADR), or information classified under prior orders that contain no declassification instructions, will be declassified in accordance with chapter 3 of this regulation. The term OADR will no longer be used. When an exemption category is selected, there is no requirement to select a specific date or event for declassification at the time of original classification. In those cases in which the original classifier does not select a declassification date, the following will apply:

(1) The information, if placed in records that have been determined to have permanent historical value under Title 44, USC (see "permanent" files under AR 25–400–2), will be automatically declassified in 25 years from the date of original classification, unless specifically exempted or unless this policy is changed before that time.

(2) The information, if not placed in such records (mentioned in subparagraph (1) above), will remain classified until destroyed, or until the OCA determines a change in classification.

e. For information in records determined to have permanent historical value, successive extensions may not exceed a total of 25 years from the date of the information's origin. Continued classification of this information is governed by the automatic declassification provisions of this regulation contained in chapter 3.

f. Decisions to extend classification must take into account the potential difficulty of notifying holders of the extension, including the possible inability to ensure continued, uniform protection of the information. Officials who decide to extend a declassification date are responsible for notifying all known holders of the information of the decision and for obtaining assurance from those holders that notification has been made to organizations that were provided the information under further dissemination by those holders.

2–12. Communicating the Classification Decision

An original classification authority who has made a decision to originally classify information is responsible for communicating that decision to persons who will likely be in possession of that information. This will be accomplished by issuing classification guidance, discussed in section V of this chapter, or by making sure that a document containing the information is properly marked to reflect the decision. Marking requirements for classified material, including page and paragraph markings, are covered in chapter 4 of this regulation.

2–13. Compilation

Generally, a compilation of unclassified items of information is not classified. In unusual circumstances, compilation of items of information that are individually unclassified can be classified if the compiled information reveals an additional association or relationship that matches criteria for classification as described in paragraph 2–8 of this regulation. Classification by compilation will be fully supported by a written explanation that will be provided on, in, or with, the material containing the information. An OCA must be consulted if guidance is required concerning whether or not the compilation results in classification.

2–14. Acquisition Systems

Classification and safeguarding of information involved in the DOD acquisition process will conform to the minimum standards of this regulation, as well as the requirements of DODD 5000.1 and DOD Instruction (DODI) 5000.2 (or successor directives and instructions). The term "time or event phased declassification date", used for acquisition systems, is synonymous with the term "declassification date" used in this regulation.

2–15. Limitations and prohibitions

EO 12958 and the Atomic Energy Act of 1954 provide the only basis to classify information. Information will only be classified when it requires protection in the interest of national security as specified in this regulation. Classification cannot be used to conceal violations of law, inefficiency, or administrative error, or to prevent embarrassment to a person, organization, agency, or to restrain competition. Basic scientific research and its results can be classified only if it clearly relates to the national security. Section VI of this chapter covers information that is a product of non–government research and development, that does not incorporate, or reveal, classified information to which the producer, or developer, was given prior access.

Section IV
Security Classification Guides

2–16. Policy
A Security Classification Guide (SCG) will be issued for each system, plan, program, or project in which classified information is involved. Agencies with original classification authority will prepare classification guides to facilitate the proper and uniform derivative classification of information. These guides will conform to standards contained in directives and regulations issued under EO 12958 and this regulation.

2–17. Content
Security classification guides will, at a minimum, include the following information:

a. Identify specific items or elements of information to be protected and the classification level to be assigned each item or element. When deemed useful, specify the items or elements of information which are unclassified or which were previously classified and now are declassified.

b. Provide declassification instructions for each item or element of information, to include the applicable exemption category for information exempted from declassification within ten years. See paragraph 2–11 for exemption categories.

c. Provide a concise reason for classification for each item, element, or category, of information which, at a minimum, cites the applicable classification category or categories from section 1.5 of EO 12958 and that are listed in paragraph 2–8 of this regulation.

d. Identify any special handling caveats or warning notices or instructions, which apply to the items, elements, or categories of information.

e. Identify by name, or personal identifier, and position title, the OCA approving the guide, and the date of the approval. A personal identifier is any grouping of letters or numbers used in an organization code that the command uses to identify a particular position. Classification guides will normally be signed by the OCA and, where that is the case, the name and position title, rather than the personal identifier and position title, will be used.

f. Provide a point of contact, with telephone number, for questions concerning the guide, challenges to classification, and suggestions for improvement. Provide a statement in the guide encouraging personnel to informally question the classification of information before resorting to a formal challenge. Provide an address for formal classification challenges.

2–18. Approval, distribution, and indexing
a. Security classification guides will be personally approved in writing by the original classification authority who is authorized to classify information at the highest level designated by the guide, and who has program support or supervisory responsibility for the information or for the command's information security program.

b. Security classification guides will be distributed to those commands, contractors, or other activities expected to be derivatively classifying information covered by the guide.

c. One paper document copy of each approved SCG (less those for SAPs or programs involving SCI) and its changes will be sent to the Director of Freedom of Information and Security Review, Office of the Assistant Secretary of Defense. Also, one copy, in paper document (hard copy) and/or automated format (soft copy), will be sent to the Army Declassification Special Program Office. See AR 380–381 for guidance on distribution of classification guides for SAPs, and AR 380–28 for guidance on SCI programs.

d. Two copies of each guide, other than those covering SAPs or SCI information, will be provided to the Administrator, Defense Technical Information Center (DTIC). Each guide furnished to DTIC must bear the appropriate distribution statement required by DODD 5230.24. Security classification guides issued under this regulation, will be indexed in the DOD Index of Security Classification Guides (DOD 5200.1–I). The originator of the guide will submit DD Form 2024 (DOD Security Classification Guide Data Elements) to the Administrator, DTIC, upon approval of the guide. If the originator determines that listing the guide in DOD 5200.1–I would be inadvisable for security reasons, issuance of the guide will be separately reported, with an explanation of why the guide cannot be listed, to the Director, Special Programs, ODTUSD(P)PS, along with a separate memorandum to DAMI–CH. Report Control Symbol DD–C3I (B&AR) 1418 applies to the reporting requirements of this paragraph.

2–19. Review, revision, and cancellation
a. Security classification guides will be revised whenever necessary to promote effective derivative classification. When a guide is revised or reissued, and a specific date was selected for declassification instruction, computation of declassification instructions will continue to be based on the date of the original classification of the information, and not on the date of the revision or re–issuance. Guides will be reviewed by the originator for currency and accuracy at least once every five years, or if concerning a defense acquisition program, prior to each acquisition program milestone, whichever occurs first. Changes identified in the review process will be promptly made. If no changes are

required, the originator will advise the Administrator, DTIC, and DAMI–CH in writing, and the record copy of the guide will be so annotated with the date of review.

b. Guides will be cancelled only when:

(1) All information specified as classified by the guide has been declassified;

(2) When the system, plan, program, or project classified by the guide has been cancelled, discontinued, or removed from the inventory and there is no reasonable likelihood that information covered by the guide will be involved in other classified programs or will be the subject of derivative classification; or

(3) When a major restructure has occurred as the information is incorporated into a new classification guide and there is no reasonable likelihood that information covered by the guide will be the subject of derivative classification.

c. Impact of the cancellation on systems, plans, programs, and projects provided to other nations under approved foreign disclosure decisions, and impact of such decisions on existing U.S. SCGs of similar systems, plans, programs, or projects, will be considered in the decision. When a classification guide is cancelled because the system, plan, program, or project has been cancelled, discontinued, executed, or removed from the inventory, the information covered by the guide is not automatically declassified. That decision rests with the OCA and authorized declassification authorities within the Army. Upon cancellation of a guide, the OCA, or other designated declassification official, with the concurrence of the OCA, will consider the need for publication of a declassification guide. In place of a separate declassification guide, declassification guidance can be included in a classification guide for a similar, current system, plan, program, or project.

d. Revision, re–issuance, review, and cancellation of a guide will be reported to DTIC on DD Form 2024 as required for new guides. Copies of changes, reissued guides, and cancellation notices will be distributed as required for new guides as stated in paragraph 2–18 of this regulation.

Section V
Non–Government Information

2–20. Policy

Information that is a product of contractor or individual Independent Research and Development (IR&D) or Bid and Proposal (B&P) efforts, conducted without prior or current access to classified information associated with the specific information in question, cannot be classified unless:

a. The U.S. Government first acquires a proprietary interest in the information.

b. The contractor, conducting the IR&D/B&P, requests the U.S. Government activity to place the information under the control of the security classification system, without relinquishing ownership of the information.

2–21. Classification determination

a. The individual or contractor conducting an IR&D/B&P effort could believe that information, generated without prior access to classified information, or current access to classified information, associated with the specific information in question, might require protection in the interest of national security. The contractor would then safeguard the information and submit it to an appropriate Army, or other U.S. Government activity, for a classification determination.

b. The Army command receiving such a request will issue security classification guidance as appropriate if the information is to be classified. If the information is not under that command's OCA, the command will refer the matter to the appropriate OCA or inform the individual or contractor to take that action. The information will be safeguarded until the matter has been resolved.

c. The Army command that holds classification authority over the information will verify whether or not the individual or contractor is cleared and has authorized storage capability. If not, the appropriate contracting authority for the command will advise whether or not to process clearance action.

d. If the individual or contractor refuses to be processed for a clearance, and the government does not acquire a proprietary interest in the information, the information cannot be classified.

2–22. Classification challenges

a. If authorized holders of information have substantial reason to, in good faith, believe that the information is improperly or unnecessarily classified, they will communicate that belief through their command security manager, to the OCA of the information, to bring about any necessary correction. This can be done informally, or by submission of a formal challenge, to the classification as provided for in EO 12958 and this regulation. Informal questioning of classification is encouraged before resorting to formal challenge. Commanders will establish procedures through which authorized holders of classified information within their Commands, can challenge a classification decision, and will ensure that Command personnel are made aware of the established procedures. An authorized holder is any person who has been granted access to specific classified information being challenged. OCAs will establish written procedures through which authorized holders of classified information can challenge classification decisions. At a minimum, security classification guides will contain a point of contact to informally communicate classification challenges and an address to communicate formal classification challenges. EO 12958 establishes the Interagency Security Classification

Appeals Panel (ISCAP). One of the roles of the panel is to decide upon appeals by authorized holders of the information who have made a formal classification challenge as described in this section. See section 5.4, EO 12958, a reprint of which is found at appendix B of this regulation, for more details on the composition and function of this panel.

(1) Formal challenges to classification, made under this subsection, will include a sufficient description of the information being challenged, to permit identification of the information and its classifier, to include the OCA, where known, with reasonable effort. Challenges to classification made by Army personnel will include the reason why the challenger believes that the information is improperly or unnecessarily classified. Use of DA Form 1575 (Request for/or Notification of Regrading Action) may be used to make a formal challenge. The challenge request should be unclassified, if possible. The classification determination of the OCA will be upheld and carried forward until otherwise determined by the appropriate authorized official.

(2) Commanders will make sure that no retribution is taken against any personnel for making a challenge to a classification.

b. The following will be established by each OCA:

(1) A system for processing, tracking, and recording formal challenges to classification. The system used will differentiate the classification challenges with other reviews for possible declassification (for example, FOIA requests). Requests for information made under the FOIA will be handled as directed by AR 25–55.

(2) The OCA will provide a written response to the challenge within 60 calendar days following the receipt of the challenge. If the OCA cannot respond fully to the challenge within 60 calendar days from receipt, the challenge will be acknowledged and an expected date of response provided. This acknowledgment will include a statement that, if no response is received within 120 calendar days following receipt of the challenge, the challenger has the right to forward the challenge to ISCAP. The challenger can also forward the challenge to the ISCAP if the OCA has not responded to an internal appeal within 90 calendar days of receipt. An internal appeal is when the challenge comes from DA personnel to a Department of the Army OCA. An information copy of the request for appeal, submitted by DA personnel, whether or not to a Department of the Army OCA, will be sent to the original classification authority.

(3) If the challenge is denied and the original classification authority determines that the information is properly classified, the OCA will advise the challenger of the right to appeal the decision. The first level of appeal will be to the first superior general officer in the chain of command of the original classification authority. That general officer will either rule on the appeal, in an impartial manner, or will designate an impartial official, or panel of officials, knowledgeable in the subject matter of the information being challenged, to decide upon the appeal. Both the challenger and the OCA will be advised of the appeal decision. The same time frames and notification to the challenger, stated in subparagraph b, above, apply to the first level of the appeal procedure. If, as a result of the first level of appeal, the challenge is denied, and the appeal authority determines that the information is properly classified, the appeal authority will advise the challenger of the right to appeal the decision to the ISCAP. The Director of the ISOO serves as the Executive Secretary of the ISCAP. The correct address to furnish the challenge for appeals to that panel is to the Executive Secretary of the Interagency Security Classification Appeals Panel, c/o ISOO. As of the publication date of this regulation, the mailing address for ISOO is: Information Security Oversight Office (ISOO), National Archives and Records Administration, 700 Pennsylvania Avenue, NW, Room 5W, Washington D.C. 20408.

(4) If a challenge is received concerning information that has been the subject of a challenge, within the preceding two years, or which is the subject of pending litigation, the original classification authority need not process the challenge. The OCA has the option of whether or not to process the challenge. If the challenge is not processed, the challenger will be informed of the situation and that the matter may be appealed to the ISCAP.

(5) If a challenge is received concerning information that has been classified by another OCA within the Army, or by another agency in the U.S. Government, the challenger will be informed of this fact and directed to resubmit the challenge to the appropriate official.

(6) If a challenge is received concerning information classified by a foreign government or international organization, the receiver of the challenge will forward the request for classification review to the appropriate foreign government agency that classified the information. The request to the foreign government for classification review will state that within the United States it is the procedure to respond to these challenges or notify the challenger within 60 calendar days of receipt of the request, and that it would be appreciated if this same response time could be observed. The correspondence to the foreign government will also inquire if there is any appeal authority, and if so, that this authority be listed in the response if the challenge is denied. The challenger will be advised of this referral, if applicable. Army OCAs will be responsive to such informal inquiries and will recognize that the Army has no control over a timely, or lack of, response from the foreign government. The reply from the foreign government, upon receipt, will be forwarded by the requester to the challenger.

c. Information that is the subject of a classification challenge will continue to be classified and appropriately safeguarded until a decision is made to declassify it.

Chapter 3
Declassification, Regrading, and Destruction

Section I
Army Declassification Program

3–1. General
Information will be declassified when it no longer meets the standards and criteria for classification. The authority to declassify information resides with the OCA for that information and those appointed as declassification authorities, subject to the criteria specified in EO 12958 and/or successor orders and directives. Department of the Army files and records will not be declassified without prior review to determine if continued classification is warranted and authorized. EO 12958 contains provisions for four declassification programs as follows:

a. Original classification authority action.

b. Automatic.

c. Mandatory.

d. Systematic.

3–2. Special Program Manager
a. The Deputy Chief of Staff for Personnel is the Army Special Program Manager (SPM) for the execution of the centralized portion of the Army's automatic declassification program. The SPM will coordinate declassification actions with Army commands, as required. The authority to decide whether information meets the criteria for continued classification and/or exemption from automatic declassification, remains with the OCA for that information. The declassification decisions of the OCA for the information will be executed by the SPM and by other officials so designated by the OCA. OCAs will publish declassification guides or guidance and will forward them to the SPM and any other officials as deemed appropriate. Declassification guidance can be included in security classification guides or can be published separately, at the option of the OCA.

b. In executing the centralized portion of the Army declassification program, the SPM will review, or cause to be reviewed, those files subject to the automatic or systematic declassification provisions of EO 12958, located in the National Archives, Washington National Records Center (WNRC), and Presidential Libraries. The SPM will coordinate the declassification actions of Army commands concerning the review of records subject to the automatic declassification program when those records are located in repositories other than the National Archives, WRNC, and Presidential Libraries. Records stored at other locations will be reviewed by the command responsible for retiring the records, or by that command's successor in function, as appropriate.

c. MACOMs will establish programs to make sure that such records are reviewed and either declassified or exempted prior to the date for automatic declassification. Army commands will provide the SPM with the statistics concerning the declassification review, as the SPM directs.

3–3. Declassification of Restricted Data and Formerly Restricted Data
Restricted Data (RD) and Formerly Restricted Data (FRD) are not subject to EO 12958. This information is classified under the Atomic Energy Act of 1954, as amended. Declassification of RD and FRD information will only be affected with the express specific approval of the classification authority for the information. Generally, this is the Department of Energy (DOE) or DOE in conjunction with DOD.

3–4. Declassification of other than Army information
a. Information classified by other U.S. Executive Branch agencies or by foreign governments or international organizations, including foreign contractors, will be referred to the originating agency, or its successors in function. In the case of a foreign government, refer to its legitimate successor for a declassification decision.

b. Every effort will be made to make sure that Foreign Government Information (FGI) is not subject to declassification without the consent of the originating government. FGI can exist in two forms; foreign documents provided to the U.S. and included in Army files and foreign government classified information that is included in a U.S. classified document. If these documents are included in permanently valuable records of the U.S. Government and are subject to the 25–year automatic declassification provisions of EO 12958, declassification officials will consult with the originating foreign government for exemption from automatic declassification in accordance with section II of this chapter. FGI will be tabbed and the Department of State will be notified. The Office of the Deputy to the Under Secretary of Defense (Policy) (ODUSD(P)) for Policy Support should be contacted for assistance and guidance.

c. See appendix C for declassification guidance concerning cryptologic information primarily under the classification authority of the National Security Agency (NSA).

Section II
The Automatic Declassification System

3–5. General

a. EO 12958 sets forth policy on the declassification of information. In particular, EO 13142, the amendment to section 3.4 of the EO 12958, requires the automatic declassification of all U.S. classified documents (other than RD or FRD) contained in records that are more than 25 years old on 17 October 2001, or are determined to have permanent historical value under Title 44, USC, unless that information has been exempted from automatic declassification. The declassification requirement will exist for all records of permanent historical value as they become 25 years old. AR 25–400–2 identifies Army files determined to be of permanent historical value under Title 44, USC, unless that information has been exempt. If not exempt, automatic declassification will occur whether or not the records have been reviewed. Records that are reviewed and are then exempted will not be automatically declassified.

b. Army files subject to automatic declassification will be reviewed prior to the date for automatic declassification. That date is 17 October 2001, for records created prior to 17 April 1976, and 31 December each year thereafter, as records become 25 years old. For records otherwise subject to this section for which a review or assessment conducted by the agency and confirmed by the Information Security Oversight Office has determined that they contain information that was created by or is under the control of more than one agency, or are within file series containing information that almost invariably pertains to intelligence sources or methods, all classified information in such records will be automatically declassified, whether or not the records have been reviewed, within 8 years from the date of EO 12958, except as provided in paragraph 3–6. This date will be 17 April 2003. This is a change to EO 12958, as prescribed by EO 13412, the amendment to Executive Order 12958, dated 19 November 1999 (see appendix B for a copy of the amendment).

3–6. Exemption from automatic declassification

a. In accordance with EO 12958, the Army has identified and proposed specific designated file series, with description and identification of information in those file series, to be exempt from the 25–year automatic declassification.

b. Files containing information described in the list of exempt file series, must be located and marked to reflect the exemption from automatic declassification, the applicable exemption category, and the date or event for future declassification. Officials conducting a declassification review will apply the exemption markings at the time of the review.

c. Information contained in files not determined to be of permanent historical value under Title 44, USC, is subject to automatic declassification. DA retention and destruction requirements apply.

d. Information exempted from automatic declassification at 25 years remains subject to the mandatory and systematic declassification review provisions of this regulation.

e. Classified information not contained in the file series, mentioned in subparagraph a, above, exempted from the automatic declassification system, may be exempted from declassification if it falls within one of the nine exemption categories that are listed below. Under the provisions of EO 12958, section 3.4, the exempting official can exempt from automatic declassification specific information the release of which would be expected to:

(1) Reveal the identify of a confidential human source, reveal information about the application of an intelligence source or method, or reveal the identity of a human intelligence source when the disclosure of that source would damage the national security interest of the United States.

(2) Reveal information that would assist in the development or use of weapons of mass destruction.

(3) Reveal information that would impair U.S. cryptologic systems or activities.

(4) Reveal information that would impair the application of state of the art technology within a U.S. weapon system.

(5) Reveal U.S. military war plans that remain in effect.

(6) Reveal information that would seriously impair relations between the United States and a foreign government, or demonstrably undermine ongoing diplomatic activities of the U.S.

(7) Reveal information that would clearly impair the current ability of United States Government officials to protect the President, Vice President, and other officials for whom protection services, in the interests of national security, are authorized.

(8) Reveal information that would seriously impair current national emergency preparedness plans.

(9) Violate a statute, treaty of international agreement.

f. Requests for exemption for other than listed exemptions, must be reported to DAMI–CH, as a "Notice of the Intent to Exempt Information from Automatic Declassification." The notice will—

(1) Describe the specific information to be exempted.

(2) Explain why the information must remain classified.

(3) Except for the identity of a confidential human source or a human intelligence source, provide a specific date or event upon which the information will be declassified.

g. DAMI–CH will review the request for conformity with current policy. If the document meets that policy,

DAMI–CH, as the Senior Agency Official, will notify the ISSO of the intent to exempt this information from automatic declassification. See paragraph 1–15 for further information on the ISSO. Notification must be received by ISSO, acting as the Executive Secretary of the ISCAP, 180 days before the information is scheduled for automatic declassification. The notice must contain the information identified in paragraph 3–6e.

h. In the case of foreign documents, the declassification review official will review the provisions of paragraph 3–4b and then determine if exemption categories 6 or 9 (25X6 or 25X9) or both should be applied.

3–7. Marking of documents exempted from automatic declassification at 25 years

a. Documents that are exempted from automatic declassification after 25 years, will be marked with the designation "25X", followed by the number of the exemption category (see categories listed in paragraph 3–6e), or by a brief reference to the pertinent exemption. For example, "25X–Human Source," notes the information is exempted from automatic declassification because it reveals the identity of a human source, as described in exemption 1. It could also be marked 25X1. If the document is exempt because of a human source, do not mark a declassification date. All other exemptions will be marked with a future declassification date, or event, established by the exempting authority. For example, a document created in 1974 is reviewed and found to contain information that requires classification beyond 17 October, 2001, because of exemption category 4, "Reveal information that would impair the application of state of the art technology within a U.S. weapon system." The exemption authority determines that the information must remain classified at least 15 years past the mandatory declassification date of 1999 (1974 + 25 = 1999). They would set the declassification date in ten–year blocks, per paragraph 2–11. This means the information could be declassified on 31 December 2019 (1999 + 20 = 2019). In this case, the declassification instructions for the document could be written as: "Declassify on 25X4, 31 December 2019" or "Declassify On: 25X – State of the art technology within the U.S., weapon system, 31 December 2019".

b. Files, documents or other material that are subject to final storage, at the National Archives or Federal Records Center, must be marked in such a way that it is clear whether the material has been exempted or declassified, in addition to the markings stated in paragraph 3–7a. The SPM, under the direction of ISSO, will provide guidance on the method of marking or tabbing those files.

Section III
Mandatory Review for Declassification

3–8. General

a. Any individual or organization may request a review for declassification of information. Upon receipt of such a request, the command will follow the general policy for classification challenges (see chap 2, section VII). Response time frames for mandatory review can be extended at command option. The request will be referred to the originating or successor agency for declassification review. In either a classification challenge or request for mandatory review for declassification, the command will refuse to confirm or deny the existence or non–existence of requested information, when the fact of its existence or non–existence is properly classified. A mandatory declassification will not be conducted if declassification review occurred within the preceding two years.

b. Information originated by the incumbent President, the incumbent President's White House staff, committees, commissions, or boards appointed by the incumbent President, or other entities within the Executive Office that solely advise and assist the incumbent President, is exempt from the provisions of this section.

3–9. General

a. Heads of HQDA activities and MACOMs will, as permitted by available resources, establish systemic programs to review for declassification, information classified under EO 12958, and predecessor orders, in the custody of the Army that is contained in permanently valuable historical records, and is exempt from automatic declassification.

b. These efforts will concentrate on records that have been identified to have significant value for historical or scientific research, or promoting the public welfare, and have reasonable probability of being declassified upon review.

Section IV
Regrading

3–10. Downgrading information

Downgrading information is appropriate when the information no longer requires protection at the originally assigned level. Classified information can be upgraded to a higher level of classification only if holders of the information can be notified of the change so that the information will be uniformly protected at the higher level. The OCA is authorized to downgrade and upgrade information and is responsible for notifying holders of the change in classification.

3–11. Downgrading policy

a. Purpose and authority. Downgrading of information to a lower level of classification is appropriate when the information no longer requires protection at the originally assigned level and can be properly protected at a lower level.

The principal purpose of downgrading is to conserve security resources by avoiding protection of information at too high a level. Downgrading is accomplished by the OCA for the information only.

b. Downgrading decisions during original classification. Downgrading should be considered when OCAs are deciding on the duration of classification to be assigned. If downgrading dates or events can be identified, they must be specified along with the declassification instructions. Note that downgrading instructions do not replace declassification instructions.

c. Downgrading at a later date. Information may be downgraded by any official who is authorized to classify or declassify the information, namely the original classification authority. The OCA making the downgrading decision will notify holders of the change in classification.

3–12. Upgrading

Classified information may be upgraded to a higher level of classification only by officials who have been delegated the appropriate level of original classification authority, in accordance with chapter 2, section II, of this regulation. Information may be upgraded only if holders of the information can be notified of the change so that the information will be uniformly protected at the higher level. The OCA making the upgrading decision is responsible for notifying holders of the change in classification.

Section V
Classified Material Destruction Standards

3–13. General

Classified material will be destroyed completely to preclude recognition or reconstruction of the classified information contained in or on the material. Destruction methods include burning, crosscut shredding, wet pulping, melting, mutilation, chemical decomposition, and pulverizing. This section contains basic concepts and guidelines that assist in determining the sufficiency of the various destruction techniques. This section also provides residue dimension standards that will assist in achieving secure destruction. Destruction will be accomplished in accordance with these guidelines.

3–14. Concepts of destruction

The guidelines in this chapter are acceptable 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, not blank paper, 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 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 allow for "secure volume" destruction.

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. The data density determination and subsequent security screen size required to be used, is the responsibility of the Security Manager at each installation and activity. No single security screen standard for all graphic material destruction is established due to differences in data density. Therefore, several security screen sizes are needed for each mechanical system using such screens. The screens should be within reach of the operator, or otherwise easily accessible, to preclude insecure destruction.

3–15. Approved routine methods of destruction

The methods for routine destruction of classified material, shown below, are approved for use by Army commands when the "secure volume" and "data density," where applicable, concepts are employed.

a. Burning. A means of pyrolysis (high temperature multistage), by forced–air incinerators, or by any other incinerator or incendiary equipment which reduces the material to an ash such that reconstruction of the information is not possible. No other single destruction method has been found to be as effective, versatile, and secure, as burning. However, since there are limitations, in some areas, on bulk incineration, for environmental reasons, pyrolytic furnaces, as well as other mechanical destruction systems, have replaced incineration at many commands. Pyrolytic furnaces operate in compliance with Federal Clean Air Act Regulatory Standards, and are to be given preference over other incinerators, when possible. Commands are advised to obtain a written guarantee, from the pyrolytic furnace seller,

attesting to the unit's ability to be licensed, and to operate within the standards applicable at the point of installation, since standards vary from state to state. Commands located outside the United States, will conform to host nation standards, if they are more restrictive than U.S. standards, unless emergency destruction is necessary. Pyrolytic furnace ash residue and ash residue from other forms of burning will 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. The ash must be stirred to make sure destruction is complete and reconstruction is impossible. Ash residue is to be examined and reduced by physical disturbance and will be considered destroyed when capable of passing through a 1/2–inch (13–mm) square wire sieve. It is recommended that furnace operators 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.

b. Shredding. Crosscut shredders are the only authorized shredders approved for use in the destruction of classified information. The crosscut shredding machine must reduce the material to shreds no greater than 1/32nd of an inch (plus 1/64th inch tolerance) by 1/2 inch crosscut. The Class I shredder, identified by GSA Interim Federal Specifications FF–S–001169, meets this standard and is approved for use when the "secure volume" concept is employed. Any other cross–cut shredder whose residue particle size, total area, is equal to or smaller than that of the above Class I shredder, is similarly approved for classified 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 to the standards described in this section. They can only be destroyed as indicated in paragraph 3–16.

c. Pulping. Standard wet process pulpers, with a 1/4–inch or smaller diameter perforated security screen, are approved for the destruction of classified paper–based documents. 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 1/4–inch (6.35–mm) or smaller diameter perforations, and therefore, meets this standard. Since the pulping process entails wetting and dissolving action, plastic–based or other water–repellent–type papers will not be put through this system. However, if wetting additives are used and the ratio of soluble to non–soluble paper is kept high (16 to 1 or greater), the masticating unit 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. Since pulpers generally destroy only paper products, staples, paper clips and other fasteners must be removed so they do not clog the security screen. Commands will make sure that random samples of residue from pulpers are collected for periodic examination.

d. Pulverizing. 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; thus, within this category are hammer mills, choppers, hoggers, and hybridized disintegrating equipment.

(1) *Hammer mills.* Hammer mills destroy by a flailing action. Paper, lightweight plastics and wood, glass slides, and aluminum–offset plates, as well as other easily broken 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 a 1/4–inch (6.35–mm) or less diameter security screen, hammer mills are approved for destruction of classified paper–based materials and aluminum offset plates, provided the "secure volume" concept is employed. When required to destroy non–paper–based classified material or high–density substances such as classified microfilm and microfiche, the security screen size will be reduced to a diameter of at least 1/16th of an inch (1.588–mm) or smaller. If used to destroy plastic film–based 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, fuse or burn. To prevent this, paper and plastic–based films are to be alternately fed into the hammer mill.

(2) *Choppers.* Choppers cut by a scissors 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 classified paper–based documents using a 3/16–inch (5–mm) diameter perforated security screen, provided the "secure volume" processing concept is used.

(3) *Hoggers and hybrids.* Hoggers and other hybridized disintegrating equipment are principally for high–volume destruction operations, such as destroying one or more tons per day. Because there are many hogger and hybrid designs on the market, a better description 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 1/4–inch (6.35–mm) be employed for classified paper–based materials processed in these systems. If the command security manager determines that the residue from such a screen size consistently reflects excessive destruction, the security screen perforation size may be increased to 5/16–inch (7.94–mm), provided all processing through the device employs the "secure volume" concept and 50–pound minimum loads. In addition, the security manager will make sure that frequent residue examinations are made to determine that the destruction of the information is complete.

3–16. Appropriate material destruction techniques and methods for non paper–based material

Shredding, pulping, and pulverizing machines built to produce the above residue standards are used primarily in the destruction of classified paper–based products. Classified waste containing typing ribbon, aluminum and plastic offset printing mats, and other non–paper–based products require special handling. They must 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. Thus, every effort must be made to keep foreign matter out of burn bags. Non–paper–based classified material is to be disposed of as follows when a pyrolytic furnace is not available or is inappropriate:

a. Non water–soluble plastic coated, waxed paper, plastic acetate, or similar material. This material will be burned in a pyrolytic furnace or other incinerator or incendiary device, destroyed in one of the high–capacity dry pulverizing systems, or shredded. Such material will not be allowed to enter wet pulping systems. Carbon paper is an exception, since it has relatively low tensile strength.

b. Magnetic Storage Media (MSM), such as materials for audio and video recorders, computers, and Automated Data Processing (ADP) office equipment. See AR 380–19 and/or section VII below for standards for destruction and degaussing of classified information on MSM.

c. Typewriter ribbons and cassettes (mylar, nylon, and cotton–based ribbon). This category of material should be destroyed by burning, 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 requires the necessity of removing the ribbon from its reel by radially slitting with a razor blade. This ensures that no one strip is longer than 10–inches (25.4–cm). Longer strips have a tendency to become entangled in destruction equipment. Once cut from the reel, this material is to 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 shredder cannot be used. When using a heavy–duty shredder, the strips of ribbons 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 any 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.

d. 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, must 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 can be salvaged.

e. 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 or other incinerator. Where burning is not permitted, consideration is to be given to a centralized collection point for destruction by burning at another location. Several destruction devices, for use with classified non–COMSEC plastic base micrographic products, have been approved. They produce extremely fine particulate and, when employed in conjunction with the "secure volume" concept, achieve the proper level of security. Further information on these commercial devices is available from: Commander, Intelligence Materiel Activity (IMA), Fort Meade, Maryland 20755–5315. As a last resort, a properly screened (1/16–inch (1.588–mm) or smaller) hammer mill can be used. Hammer mills must be fed plastic film and other plastic–based materials very slowly to avoid heat build–up. It is best to wait and mix in batches of paper between charges of film to allow cooling and to remove softened plastic from the hammer mill. Further information on commercial devices is available from IMA.

f. Equipment and devices. Equipment, devices and other solid objects are best destroyed by burning, preferably 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 the desired results, which is the information is destroyed completely so as not to allow recognition or reconstruction of the classified information, and 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.

3–17. Technical advice on approved destruction devices and methods

Destruction devices generally can be obtained through the National Supply System (FSC Group 36, Part II). Technical guidance concerning appropriate methods, equipment, and standards for the destruction of classified electronic media and processing equipment components, can be obtained by submitting all pertinent information to the National Security Agency, Attention: NSA/CSS Directorate for Information Systems Security, Fort Meade, MD 20755. Technical guidance concerning the standards for the destruction of other storage media can be obtained from: Intelligence Materiel Activity (IMA), Fort Meade, MD 20755–5315.

3–18. Clearing, purging, declassifying, and destroying media

a. Clearing of media means erasing or overwriting all information on the media without the totality and finality of purging. The clearing procedure is adequate when the media will remain within the facility; however, removable media

must continue to be controlled at their prior classification or sensitivity level. Purging or sanitizing of media means to erase or overwrite, totally and unequivocally, all information stored on the media. Declassifying of media refers to the administrative action taken after it has been purged. Declassifying is required when the media must leave the facility under the control of uncleared personnel; for example, for maintenance operations.

b. The decision to declassify media will be made only after comparing the inherent risks (in the Magnetic Media Remanence Guide – Rainbow Series) with the financial or operational benefit of media declassification. For example, destruction of media is normally more appropriate than declassification and reuse, given the low cost of the media.

c. Media can be declassified only after purging. The appropriate ISSO must verify that the technique chosen for purging (or sanitizing) meets applicable requirements. Additionally, the ISSO must establish a method to periodically verify the results of the purging. As a minimum, a random sampling will be taken to verify each purge.

d. Degaussing must be accomplished using NSA–approved equipment from the Degausser Products List of the Information Systems Security Products and Services Catalogue. Information on degaussers is available through the information systems security management structure. Some listed products may be used only to degauss magnetic media that has coercivity no greater than 350 oersteds (also known as type I media), while others are approved for media with coercivity no greater than 750 oersteds (also known as type II media). Certain tape media have a coercivity greater than 750 oersteds (also known as type III media) and cannot, at this time, be completely degaussed. (See AR 380–19 for more information.)

e. A CD–ROM will be destroyed by scratching both surfaces with an abrasive substance, to render the CD unreadable, prior to breaking the CD into numerous pieces with an impact device, such as a hammer.

f. Storage media containing Sensitive Compartmented Information (SCI) will be handled as stated in AR 380–19, and media containing Special Access Program (SAPs) material will be handled as stated in AR 380–381.

Chapter 4
Marking

Section I
Marking Documents

4–1. Purpose and policy

Marking is the principal means of informing holders of classified and sensitive information of its classification/sensitivity level and protection requirements. Within the Department of the Army, classified and sensitive material will be identified clearly by marking, designation, electronic labeling, or if physical marking of the medium is not possible, by some other means of notification. The term "marking" as used in this regulation is intended to include all these methods of notification. The term "document" as used in this section is meant to apply to all classified and unclassified material, no matter what form (paper, electronic, etc.) it is in. Classification/sensitivity markings must be conspicuous. Original and derivative classifiers are responsible for application of the appropriate classification/sensitivity markings. The requirements for marking information and material within the intelligence community are a little different. These requirements can be found in appendix D, of this regulation, and successor Director of Central Intelligence Directives (DCID). The requirements of this chapter do not apply to the marking of security containers. The only markings allowed on security containers are those outlined in paragraph 7–8 of this regulation. Marking serves these purposes:

a. Alerts holders to the presence of classified and sensitive information.

b. Identifies, as specifically as possible and feasible, the exact information needing protection.

c. Indicates the level of classification/sensitivity assigned to the information.

d. Provides guidance on downgrading (if any) and declassification.

e. Gives information on the source(s) and reason(s) for classification of the information.

f. Warns holders of special access, control, dissemination, or safeguarding requirements.

4–2. Exceptions

a. Public Media — Classification and/or other security markings will not be applied to an article or portion of an article that has appeared in a newspaper, magazine, or other public medium. If such an article is evaluated to see if it contains classified and/or sensitive information, the results of the review will be properly marked, if classified and/or sensitive, and will be kept separate unless both the article and the results of the review are protected (stored and otherwise safeguarded as classified/sensitive information). DA personnel will neither confirm nor deny the presence of classified and/or sensitive information or the accuracy of such information when that information has appeared in the public media.

b. Confidential Source or Relationship — Classified documents and material will be marked in accordance with this regulation unless the markings themselves would reveal a confidential source or relationship not otherwise evident in the document, material, or information.

c. Restricted Data/Formerly Restricted Data — The marking requirements for the date or event for declassification do not apply to documents or other material that contain, in whole or part, RD or FRD information. Such documents or other material or portions thereof will 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 national security information contained therein, the approval of the originating agency.

4–3. Requirements

General requirements are shown in this section. Each of these requirements is explained in more detail in a separate section of this chapter. Figures 4–1 through 4–13, at the end of this chapter, provide examples of the most typical situations. These figures are not intended to cover all situations. Material other than paper documents require the same markings and must have the same information either marked on it or made available to holders by other means of notification. While not a requirement, the holder of an improperly marked classified document should contact the document originator to obtain correct markings. Classified and sensitive material will bear the following markings:

a. The overall (highest) classification/sensitivity of the information.

b. The command, office of origin, date, and if not evident by the name of the command, the fact that the document was generated by the Department of the Army.

c. Identification and date of the specific classified information in the document and its level of classification (page and portion markings).

d. Identification of the source(s) of classification ("Classified by" or "Derived from" line), and, for originally classified information, the concise reason(s) for classification. In cases of derivative classification, the reason(s) the source of the classified portion(s) is/are derived from.

e. Declassification instructions ("Declassify on" line), and downgrading instructions, if any downgrading applies.

f. Warning and sensitivity notices and other markings, if any, that apply to the document.

4–4. Overall classification marking

Classified and sensitive documents will be marked to show the highest classification/sensitivity of information contained in the document. For documents containing information classified at more than one level, the overall marking will be at the highest level. For example, if a document contains some information marked "SECRET" and some information marked "CONFIDENTIAL", the overall marking would be "SECRET". This marking must be conspicuous enough to alert personnel handling the material that it is classified and must appear in a way that will distinguish it clearly from the text of the document. The overall classification/sensitivity will be conspicuously marked, stamped, or affixed (with a sticker, tape, etc.), top and bottom, on the front and back covers (if the document has covers), on the title page (if there is one), and on the first page, in letters larger than those on the rest of the page. If it is not possible to mark classification/sensitivity in letters which are larger than the rest of the text (for example, on covers of documents or graphics), apply classification/sensitivity markings in any manner that is immediately noticeable. To promote reproducibility, classification/sensitivity and associated markings will be applied in black or other dark ink. The use of red ink is discouraged. If the document or other material has no front cover, the first page will be the front page. If it has a cover, the first page is defined as the first page that can be seen when the cover is turned back or opened. In some documents, the title page and first page can be the same.

4–5. Date, command, office of origin, and agency

Classified and sensitive documents will be marked on the face of the document with the date of the document, the command that originated it, the office or agency which originated it, and "U.S. Army" or "Army" if it is not clear from the name of the command that it is a DA activity originating the document. This information will be clear enough to allow the recipient of the document to contact the preparing office if questions or problems about classification arise.

4–6. Page and portion marking

Each classified and/or sensitive document must show, as clearly as possible and feasible, which information in it is classified and/or sensitive and at what level. That will be done in the following manner:

a. Each interior page of a classified and/or sensitive document (except blank pages) will be conspicuously marked, top and bottom, with the highest classification/sensitivity of the information on the page. The marking must be conspicuous enough that it is clearly distinguishable from the regular text of the document. Blank interior pages are not required to be marked. This is the preferred method of page marking. As an alternative to marking pages according to individual page content, the interior pages can be marked with the highest overall classification/sensitivity of information within the document. If this alternative method is used, portion marking must be used and cannot be excepted as described in paragraph 4–6c, below.

b. Each section, part, paragraph, and similar portion of a classified and/or sensitive document will be marked to show the highest level of classification/sensitivity of information it contains, or that it is UNCLASSIFIED. "Portion marking" is the term used to meet this requirement. The term "paragraph marking" is generally used interchangeably with "portion marking". Whether referred to as portion or paragraph marking, the term includes the marking of all portions of a document, not just paragraphs. When deciding whether a subportion (such as a subparagraph) will be

marked separately as a "similar subportion", the deciding factor is whether or not the marking is necessary to eliminate doubt about the classification/sensitivity of its contents. Unless the original classification authority or originator of the document indicates otherwise on the document, each classified and/or sensitive portion of a document will be presumed to carry the declassification instructions (date, event, or exemption category) of the overall document.

(1) Each portion of text will be marked with the appropriate abbreviation ("TS" for TOP SECRET, "S" for SECRET, "C" for CONFIDENTIAL, or "U" for UNCLASSIFIED), placed in parentheses immediately before the beginning of the portion. If the portion is numbered or lettered, the abbreviation will be placed in parentheses between the letter or number and the start of the text. Some agencies permit portion marking at the end of the portion, rather than at the beginning. The Department of the Army does not. When extracts from non–DA documents are made and incorporated into DA documents, the portion marking will be placed at the beginning of the portion.

(2) Portions containing Restricted Data (RD) and Formerly Restricted Data (FRD) will have abbreviated markings ("RD" or "FRD") included with the classification marking, for example, "(S–RD) or (S–FRD)". Critical Nuclear Weapons Design Information (CNWDI) will be marked with an "N" in separate parentheses following the portion marking, for example, "(S–RD)(N)".

(3) The abbreviation "FOUO" will be used in place of "U" when a portion is UNCLASSIFIED but contains "For Official Use Only" information. AR 25–55 contains the definition and policy application of FOUO markings. See chapter 5, of this regulation, for further guidance, as well.

(4) Portions of DA documents containing foreign government or NATO information will include identification of the foreign classification in the marking in parentheses. For example, "(UK–S)" for information classified "SECRET" by the United Kingdom; and "(NATO–C)" for North Atlantic Treaty Organization (NATO) information classified as "CONFIDENTIAL".

(5) Paragraph 5–410, DODD 5200.1–R stated that the caveat "NOFORN" will no longer be used. This has since been rescinded. Effective with the release of Director of Central Intelligence Directives (DCID) 1/7 (see app D) and DCID 5/6, both dated 30 June 1998, the use of "US ONLY," to mark information that must be restricted to U.S. nationals, will cease. Until revoked, this type of information will be marked "NOFORN." This applies to all media, including hard copy, digital, and graphic.

(6) The subject and title of classified documents will be marked to show the classification of the information in the subject or title. The same abbreviations ("TS", "S", "C", "U", or "FOUO") will be used but the abbreviations will be placed in parentheses at the end of the subject or title.

(7) Charts, graphs, photographs, illustrations, figures, tables, drawings, and similar portions will be marked with the unabbreviated classification/sensitivity, such as "UNCLASSIFIED", based on the level of classified and/or sensitive information revealed. The marking will be placed within the chart, graph, etc., or next to it, such as on the frame holding the document. Captions and titles of charts, graphs, etc., will be marked as required for text portions (such as paragraphs) and will be placed at the beginning of the caption or title.

(8) See appendix D for an explanation of marking certain intelligence control markings (for instance, ORCON and PROPIN). Portion marking of those intelligence control markings will follow the policy as stated in DCID 1/7 and successor directives.

(9) See appendix I for an explanation of marking Special Access Programs (SAPs) material.

c. If an exceptional situation makes individual marking of each paragraph or other portion clearly impracticable, a statement can be substituted describing the fact that portion markings were not used, and which portions are classified and/or sensitive and their level of classification/sensitivity. Such a statement will identify the information as specifically as would have portion markings. For classification by compilation, the statement required by paragraph 2–13 meets this requirement.

d. Documents containing information classified by compilation will be marked as follows:

(1) If portions, standing alone, are UNCLASSIFIED, but the document is classified by compilation (see para 2–13), mark the portions as "(U)" and the document and pages with the classification of the compilation. You must also add an explanation of the classification as required in paragraph 2–13 of this regulation.

(2) If individual portions are classified and/or sensitive at one level, but the compilation results in a higher classification/sensitivity, mark each portion with its own classification/sensitivity and mark the pages, and the overall classification/sensitivity of the document, with the higher classification/sensitivity of the compilation. An explanation of the classification/sensitivity by compilation is required to be placed in the document, preferably on the cover or title page.

(3) DAMI–CH will be contacted for guidance on submission of waivers or exceptions to policy concerning the marking of documents classified and/or sensitive by compilation.

4–7. Sources of classification – overview

Each classified document will be marked with the source of the classification. For originally classified documents, that identification will be preceded by the term "Classified by". In cases of derivative classification, the source of classification is derived from either:

(1) A classification guide or guidance.

(2) A classified source document that was used to extract, summarize, restate, or paraphrase information from the source document into the new document.

(3) When compilations of items of information that are individually unclassified can be classified if the compilation reveals an additional association or relationship that matches criteria for classification pursuant to paragraph 2–8 of this regulation. For derivatively classified documents, the term "Derived from" will precede the identification of the source of classification. This is a change from previous policy. Previous policy required the use of the "Classified by" line for both originally and derivatively classified documents. Current policy requires the use of the "Classified by" line only for original classification documents and combination original and derived documents, and requires the use of the "Derived from" line for only wholly derived classified documents. See chapter 2 for a further explanation of the differences between, and requirements for, originally and derivatively classified documents.

4–8. Sources of classification – procedures

a. Originally classified documents. Each originally classified document will have a "Classified by" line placed on the face of the document. The "Classified by" line will identify the original classification authority responsible for classification of the information contained in the document. The OCA will be identified by name or personal identifier (see paragraph 2–17e for an explanation of the term "personal identifier"), and position title. If the information required to be included in the "Classified by" line would reveal classified information not evident from either the rest of the document or not evident from the face of the document, the "Classified by" line will be completed with an UNCLASSIFIED identification (such as an UNCLASSIFIED personal identifier) that can be traced through secure channels.

b. Derivatively classified documents. Each derivatively classified document will have a "Derived from" line placed on the face of the document. The term "Classified by" will not be used on classified documents that are wholly derivative. The "Derived from" line will be completed as follows:

(1) If all the information was derivatively classified using a single security classification guide (or guidance) or only one source document, identify the guide or the source document on the "Derived from" line. Include the date of the guide or document. If using a source document that cites a guide as classification authority, use the guide rather than the source document on the "Derived from" line.

(2) If more than one security classification guide, source document, or combination of guide(s) and document(s) provided the derivative classification guidance, use the term " Multiple Sources" on the "Derived from" line. If "Multiple Sources" is placed on the "Derived from" line, a record of the sources will be maintained on or with the file or record copy of the document. Whenever feasible, this list should be included with all copies of the document. If the document has a bibliography or list of references, that can be used as the listing of sources as long as it is annotated to delineate the sources of classification from the other references. A document derivatively classified on the basis of a source document that is itself marked "Multiple Sources" will cite the source document on its "Derived from" line rather that the term "Multiple Sources". (For example, "Derived from: Headquarters, Department of the Army Report, Security 2001, an Army Odyssey, 10 February 1997, Office of the Deputy Chief of Staff for Intelligence (DAMI–CH).")

c. Combination of original and derivative classification. There can be situations in which some information in a document is originally classified at the time of preparation of the document and some information is derivatively classified. In those cases, mark the document with a "Classified by" line and place "Multiple Sources" on the line. For the information originally classified in the document, the OCA will be included in the list of sources required in paragraph 4–8b(2).

4–9. Reason for original classification

Each originally classified document will bear a concise line that describes the reason for the decision to classify. This requirement applies only to originally classified documents and does not apply to derivatively classified documents. The "Reason" line will not be used on wholly derivatively classified documents. The "Reason" line is placed between the "Classified by" line and the "Declassify on" line. The reason(s) to classify relates to the categories of what can be classified, as specified in paragraph 2–8. The "Reason" line will either:

a. State one or more of the reasons listed in paragraph 2–8. For example: "Reason: Military plans, weapons systems, or operations"; or "Reason: Foreign government information"; or "Reasons: Military plans, weapons systems, or operations; and foreign government information".

b. State the reason in terms of listing the number "1.5" followed by the letter, in parentheses, that corresponds with the appropriate category or categories of information listed in section 1.5 of E.O 12958. This is the same list shown in paragraph 2–8 of this regulation. For example: If the information is classified because it concerns military plans, weapons systems, or operations, mark the document: "Reason: 1.5(a)". If the document is classified because it contains foreign government information, mark the document: "Reason: 1.5(b)". If the document is classified for both reasons, mark the document: "Reasons: 1.5(a) and 1.5(b)."

c. For those cases in which the document contains both originally classified and derivatively classified information,

state the reason(s), as described in subparagraph a or b of this paragraph, and add the words, "and derivatively classified source" or "and derivatively classified sources", where more than one derivative source document is used.

4–10. Declassification instructions—"Declassify on" line

Each classified document (except those containing RD and FRD) will be marked on the face of the document with a "Declassify on" line, with instructions for the declassification of the information. This applies for all classified documents, both originally and derivatively classified. The "Declassify on" line will be completed as follows:

a. Originally classified documents. If all the classified information is the product of original classification, the OCA will specify the instruction on the "Declassify on" line. The instruction will specify either a date for declassification, an event for declassification, or an indication that the information is exempt from declassification within ten years.

(1) If any information in the document has been exempted from declassification within ten years, referred to as the "Ten Year Rule," the "Declassify on" line will be completed with an "X" followed by a number or numbers which show the applicable exemption category or categories from paragraph 2–11c. There is no alternative to listing the category in this manner. For example, a document containing information requiring classification beyond ten years because it would reveal information that would impair the development or use of technology within a U.S. weapon system (category number 3 under paragraph 2–11c) would be marked: "Declassify on: X3". As another example, a document containing information requiring classification beyond ten years because it reveals U.S. military plans (category number 4 under paragraph 2–11c) would be marked "Declassify on: X4". Note: Listing the exemption category number rather than the words describing the category is the preferred method of citing declassification exemption instructions within DOD.

(2) For cases in which it is possible for the Original Classification Authority to select a date or event for declassification at a point occurring more than ten years in the future, the date or event would follow the exemption category number. An example is "Declassify on: X3, 11 November 2011". There can be cases in which it is not possible for the OCA to select a future date or event for declassification. In those cases, only the exemption category will be listed. Examples for those cases, such as "Declassify on: X3", are shown in subparagraph (1), above.

(3) If more than one exemption applies, the OCA will list each exemption. For example, a document originally classified beyond ten years because it would reveal information that would impair the development or use of technology within a U.S. weapons system (exemption category 3) and that also contains foreign government information (exemption category 5) would be marked, "Declassify on: X3,5".

(4) Regardless of the exemption category used, or whether or not a date or event for declassification has been selected, the information can be subject to the automatic declassification provisions of the current EO or statute on classification. EO 13142, the most recent amendment to EO 12958, section 3.4, requires all classified information contained in records that will be more than 25 years old on 17 October 2001, and have been determined to have permanent historical value under Title 44, USC, to be declassified on 17 October 2001, unless the information has been exempted. The current criteria for exemption for 25 year old information is contained in chapter 3 of this regulation and in section 3.4 of EO 12958. It is impossible to predict what criteria will apply to any future automatic declassification programs. It is important for OCAs to carefully select the appropriate exemption category (with or without a declassification date or event) for currently classified information. Future automatic declassification programs might use a formula to convert current exemptions to future criteria used in reviewing old classified documents. If more than one exemption applies, it is important to list each exemption category.

b. Derivatively classified documents. In a derivatively classified document there may be one source from which the classification is derived, or there may be several sources. The source may have been classified after 14 October 1995 (the date the requirements of EO 12958 went into effect) and reflects the current system of conveying declassification instructions. The source may have been classified prior to 14 October 95 under the former system in which the use of the term Originating Agency Determination Required (OADR) was often used. Or, the source may have been classified after 14 October 95 but still reflects the former system of conveying declassification instructions. Even in cases in which only one source document is used, and often in cases in which several sources are used, different declassification instructions may apply to the various items of information in the document being created. To ensure that all the information in the document is protected for as long as necessary, the most restrictive declassification instruction that applies to any of the information in the document will be placed on the "Declassify on" line. The term "most restrictive" means the latest date or event, or the date or event furthest in the future. Throughout this regulation the term "OADR" is used strictly because there are documents out there with this term. The term "OADR" is no longer authorized.

(1) If all the information in the document has the same declassification instruction (i.e. same date, event, or exemption category or categories), and that instruction is an allowable option under the new policy contained in EO 12958 as stated in this regulation, place that instruction on the "Declassify on" line. The allowable options are:

(a) A date or event for declassification within 10 years from original classification.

(b) An exemption category for information classified beyond 10 years (see paragraph 4–10a) such as "X4." When an exemption category is used, it may or may not be followed by a declassification date or event, depending upon whether the original classification authority has selected a declassification date or event.

(c) For documents that will be over 25 years old on 17 October 2001, and are contained in records that have been determined to have permanent historical value under Title 44 of the USC, an exemption category or categories as shown in chapter 3.

(d) The source may be marked with one of the indefinite markings used before the term "OADR" was authorized. In such cases, any information with indefinite declassification instructions will be treated as though it were marked as "OADR".

(e) There are two different lists of exemption categories. One list applies to information that requires classification for more than 10 years. This list is contained in paragraph 2–11c. The other list applies to information contained in the exempted file series list and that will be more than 25 years old by 17 October, 2001. That list is contained in paragraph 3–6e.

(2) If all the information in the document has been extracted from a document created before 14 October 1995 (the effective date of EO 12958) and was marked "OADR", place the statement "Source marked OADR" on the "Declassify on" line, followed by the date of the document after the words "Date of Source". For example, a derivative classifier extracts classified information from a document dated 3 June 1992 and marked "OADR". The newly created document containing that extract will be marked, "Declassify on: Source marked OADR; Date of Source: 3 June 1992." When using several sources of information marked " OADR", the "Date of Source" line will reflect the most recent date (the document with the latest date). For example, one source is dated 2 August 1993 and one is dated 1 September 1995. In this case, the newly created derivatively classified document will be marked:
Derived from: Multiple Sources
Declassify on: Source marked OADR;
Date of Source: 1 September 1995

(3) No matter what combination of indefinite declassification instructions and document dates used as sources to derivatively classify the document, the document originator will only select the source document with the most recent date and this will determine the date to place on the "Date of Source" line. Follow this policy for all cases involving information classified under previous Executive Orders that contain indefinite declassification instructions. Follow this policy for all cases involving information extracted from a document created after 14 October 1995 that was mistakenly marked as OADR. Where practical and feasible, notify the originator of that mistakenly marked document of the outdated declassification instructions and obtain the current correct markings.

(4) If the document is classified by more than one source ("multiple sources") and different declassification instructions apply, the derivative classifier will place the most restrictive declassification instruction on the "Declassify on" line. The most restrictive declassification instruction is the date or event that will occur farthest in the future (the longest date from now). The following applies:

(a) If declassification dates are specified for all of the sources of information used in the document, place the latest date (date farthest in the future) on the "Declassify on" line. For example, in creating a new document, information is extracted from documents marked for declassification on 20 March 1998, 1 June 2002, and 3 April 2009. The newly created document will be marked: "Declassify on: 3 April 2009".

(b) If the sources of classification are a combination of a date or dates with an event or events, the declassification instruction will reflect whichever date and event occurs later (date or event farthest in the future). If the date of the event(s) is unknown, the declassification instruction will reflect the most restrictive date and latest occurrence of the event(s). For example, one source specifies a declassification date of 11 November 2011, and the other a declassification event upon execution of operations. In this case, the document will be marked: "Declassify on: 11 November 2011 or execution of operations, whichever is later".

(c) If any of the information in the document does not have a specific date or event for declassification, the originator of the derivatively classified document will apply the most restrictive declassification instruction, according to the following:

1. When using information classified under a previous EO, any information with an indefinite declassification (such as Group 3 or OADR) is treated as if it were marked "OADR" and marked as specified in paragraph 4–9b.

2. When using information from sources marked with the current EO 12958 exemption markings (X1 through X8), the "Declassify on" line will be marked with all exemptions that apply to all sources used. For example, if one source cited "X2", another cited "X3" and the third cited "X5", the Declassify on line would read: "Declassify on: X2,3,5". The most recent date will be used on the "Date of Source" line. For example, a derivatively classified document that uses three sources with the latest source dated 10 February 1996, will be marked:
Derived from: Multiple Sources
Declassify on: Sources marked X2,3,5
Date of Source: 10 February 1996

3. When using one or more sources marked with an indefinite declassification from a previous Executive Order (such as OADR) as well as one or more sources marked with the current EO 12958 exemption markings (X1 through X8), the "Declassify on" line will cite the exemption category or exemption categories as well as "source marked OADR". The "Date of Source" line will cite the date of the most recent source. For example, a derivatively classified document that uses the three sources mentioned in subparagraph (2), above, and also uses a source dated 1 September

1995 and marked OADR will be marked:
Derived from: Multiple Sources
Declassify on: Sources marked X2,3,5 and OADR
Date of Source: 10 February 1996

4. The above rules apply to derivatively classified documents when a combination of original classification and derivative sources are used. The term "sources" as used above also includes the classification guides or guidance supplied by the original classifier.

5. With sources having a combination of differing declassification instructions, it is important to determine which is the most restrictive. The most restrictive marking will always be used. This rule applies for all derivative classifications including those in which there is a combination of derivative sources and original classification. A marking that does not provide a definite declassification date will always be considered more restrictive than one with a specific date. For instance, a document that is classified by two sources, one dated 19 August 1994 and marked "OADR" and the other dated 10 December 1995 and marked "Declassify on: 24 May 2004", will be marked: "Declassify on: Source marked "OADR", Date of Source: 19 August 1994". See subportion (3) directly above for an example of a case in which one source is marked OADR and the other is marked with one or more of the exemption categories (X1 through X8) of Executive Order 12958.

4–11. Sources that were created prior to 1976

Chapter 3 provides the policy for marking information contained in records that will be more than 25 years old on 17 October 2001, and have been determined to have permanent historical value under title 44, USC. In summary, under EO 13142, amendment to EO 12958, section 3.4, information more than 25 years old by 17 October 2001, and that is contained in records that have been determined to have permanent historical value under title 44, USC will be automatically declassified starting on 17 October 2001, unless that information is exempted from declassification. The exemption categories, required markings, and the DA policy for handling this program are discussed in chapter 3 of this regulation. This section is not intended to prescribe the policy for addressing the review of that information. That policy is contained in chapter 3. This section prescribes the policy to follow when material, that will be over 25 years old by 17 October 2001, is used as the source for derivatively classifying a newly created document. Commands will consult AR 25–400–2 and local records managers for advice on what constitutes a file determined to have permanent historical value under Title 44, USC. In creating new documents using the old sources that will be over 25 years on 17 October 2001, it will make a difference whether or not the information has already been reviewed to determine if it is in a record that has been determined to have permanent historical value and whether or not it has been reviewed to determine if it will be declassified or exempted from automatic declassification. There are three possible options:

a. The information is determined to be of permanent historical value under title 44, USC, has been reviewed for continued classification, and qualifies under one or more of the exemptions listed in paragraph 3–6e of this regulation (section 3.4 of EO 12958). If it qualifies for exemption, the exemption category and the future date or event for declassification (if one applies) will be shown on the document, file, or record. When one of these documents is used as a source in classifying a derivatively classified newly created document, use the term shown on the document or record that was applied when the information was reviewed. That term will be "25X" followed by the appropriate exemption category that pertains to information exempted from declassification at 25 years and state the new declassification date or event, if one has been determined. For example, "25X3(31 December 2015)" if the information is exempted because it reveals information that would impair U.S. cryptologic systems and now has been determined to be declassified on 31 December 2015. Sometimes there will only be the exemption category with no date or event listed for declassification. For example, "25X1" if the information would reveal the identity of a human intelligence source.

b. The information is contained in a record that has been determined to have permanent historical value under title 44, USC, has been reviewed, and has been determined to not qualify for exemption. This information will have been marked with a declassification date or event on or before 17 October 2001. This date or event will be used as declassification instructions.

c. The information is either in a record that has been determined to not have permanent historical value under title 44 USC; or is in a record that has been determined to have permanent historical value under title 44 USC but has not yet been reviewed for declassification. This information would be subject to declassification 25 years from the date of its origin. Thus, the date of the source document will be placed, as the following, for declassification instructions:
Source marked OADR
Date of Source:(fill in applicable date)

4–12. Warning notices

In certain circumstances, warning notices will be required if the document contains certain categories of information for which the notice applies. In addition to the notices listed below, other notices may be required by other DA regulations. Unless another regulation or authorized administrative publication prescribes different placement, these notices will be placed on the cover (or first page where there is no cover) of the document.

a. Restricted Data (RD). Documents containing RD will be marked: "RESTRICTED DATA" THIS MATERIAL

CONTAINS RESTRICTED DATA AS DEFINED IN THE ATOMIC ENERGY ACT OF 1954. UNAUTHORIZED DISCLOSURE SUBJECT TO ADMINISTRATIVE AND CRIMINAL SANCTIONS.

b. Formerly Restricted Data (FRD). Documents containing FRD, but no Restricted Data, will be marked: "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."

c. Critical Nuclear Weapons Design Information (CNWDI). Messages containing CNWDI will be marked at the beginning of the text as "RD CNWDI." Documents containing CNWDI will be marked: "Critical Nuclear Weapons Design Information DOD Directive 5210.2 applies"

d. Intelligence Information. The policy on the control, dissemination, and marking of warning notices concerning intelligence information is contained in appendix D. Placement of these intelligence control markings will follow the same policy as stated in appendix D.

e. COMSEC Material. The following marking will be placed on COMSEC documents before release to contractors: "COMSEC Material – Access by Contractor Personnel Restricted to U.S. Citizens Holding Final Government Clearance."

f. Reproduction Notices. Classified information that is subject to dissemination or reproduction limitations will be marked with notices that say, in essence, the following: "Reproduction requires approval of originator or higher DOD authority of the originator". "Further dissemination only as directed by (insert appropriate office or official) or higher DOD authority"

g. Special Access Programs (SAPs) Documents. Special Access Programs documents may be identified with the phrase "Special Access Required" and the assigned nickname, codeword, trigraph, or digraph. AR 380–381 contains the Department of the Army policy on marking SAPs material. See appendix I for further information.

h. DODD 5230.24 requires distribution statements to be placed on technical documents, both classified and unclassified. These statements facilitate control, distribution and release of these documents without the need to repeatedly refer questions to the originating activity. The originating office may, of course, make case–by–case exceptions to distribution limitations imposed by the statements. Distribution statements on technical documents will be marked with notices that say, in essence, the following:

(1) Distribution Statement A — Approved for public release; distribution is unlimited.

(2) Distribution Statement B — Distribution authorized to U.S. Government agencies only; [reason]; [date]. Other requests for this document shall be referred to [controlling DOD office].

(3) Distribution Statement C — Distribution authorized to US Government agencies and their contractors; [reason]; [date]. Other requests for this document shall be referred to [controlling DOD office].

(4) Distribution Statement D — Distribution authorized to the DOD and US DOD contractors only; [reason]; [date]. Other requests for this document shall be referred to [controlling DOD office].

(5) Distribution Statement E — Distribution authorized to DOD Components only; [reason]; [date]. Other requests for this document shall be referred to [controlling DOD office].

(6) Distribution Statement F — Further distribution only as directed by [controlling DOD office] or higher DoD authority; [date].

(7) Distribution Statement X — Distribution authorized to US Government agencies and private individuals or enterprises eligible to obtain export–controlled technical data in accordance with regulations implementing 10 USC 140c; [date]. Other requests must be referred to [controlling DOD office].

i. Documents containing information provided by a foreign government. See section VI of this chapter for complete policy on marking foreign government information in classified DA documents. U.S. classified documents that contain extracts of information provided by a foreign government will be marked with the following warning notice: "FOREIGN GOVERNMENT INFORMATION"

j. Documents containing information provided by a foreign government or international organization. See section VII of this chapter for complete policy on marking information provided by a foreign government or international organization. Examples of an international organization are the United Nations (UN) and the North Atlantic Treaty Organization (NATO). The following example pertains to NATO. The same policy applies to any other international organization by replacing the word "NATO" with the appropriate name or abbreviation for that organization. DA classified documents that contain extracts of NATO classified information will bear a marking substantially as follows: "THIS DOCUMENT CONTAINS NATO CLASSIFIED INFORMATION"

k. The following warning notice must appear on all U.S. Government owned or operated automated information systems:

"THIS IS A DOD COMPUTER SYSTEM. BEFORE PROCESSING CLASSIFIED INFORMATION, CHECK THE SECURITY ACCREDITATION LEVEL OF THIS SYSTEM. DO NOT PROCESS, STORE, OR TRANSMIT INFORMATION CLASSIFIED ABOVE THE ACCREDITATION LEVEL OF THIS SYSTEM. THIS COMPUTER SYSTEM, INCLUDING ALL RELATED EQUIPMENT, NETWORKS, AND NETWORK DEVICES (INCLUDES INTERNET ACCESS), ARE PROVIDED ONLY FOR AUTHORIZED U.S. GOVERNMENT USE. DOD COMPUTER SYSTEMS MAY BE MONITORED, FOR ALL LAWFUL PURPOSES, INCLUDING TO ENSURE THEIR USE IS AUTHORIZED, FOR MANAGEMENT OF THE SYSTEM, TO FACILITATE PROTECTION AGAINST

UNAUTHORIZED ACCESS, AND TO VERIFY SECURITY PROCEDURES, SURVIVABILITY, AND OPERATIONAL SECURITY. MONITORING INCLUDES, BUT IS NOT LIMITED TO, ACTIVE ATTACKS BY AUTHORIZED DOD ENTITIES TO TEST OR VERIFY THE SECURITY OF THIS SYSTEM, DURING MONITORING, INFORMATION MAY BE EXAMINED, RECORDED, COPIED AND USED FOR AUTHORIZED PURPOSES. ALL INFORMATION, INCLUDING PERSONAL INFORMATION, PLACED OR SENT OVER THIS SYSTEM MAY BE MONITORED. USE OF THIS DOD SYSTEM, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO MONITORING. UNAUTHORIZED USE OF THIS DOD COMPUTER SYSTEM MAY SUBJECT YOU TO CRIMINAL PROSECUTION. EVIDENCE OF UNAUTHORIZED USE COLLECTED DURING MONITORING MAY BE USED FOR ADMINISTRATIVE, CRIMINAL, OR OTHER ADVERSE ACTION. USE OF THIS SYSTEM CONSTITUTES CONSENT TO MONITORING FOR ALL LAWFUL PURPOSES."

l. Other Warning Notices. Subparagraphs a through k above represent the most commonly used warning notices. They do not necessarily represent the only warning notices. There is nothing in this regulation that prohibits other authorized warning notices from being applied to classified documents. Where other regulations authorize and require special warning notices, they may be applied to DA classified documents.

4–13. Obsolete Restrictions and Control Markings

a. The following control markings are obsolete and will not be used, in accordance with the following guidelines:

(1) *WNINTEL and NOCONTRACT.* The control markings, Warning Notice – Intelligence Sources or Methods Involved (WNINTEL), and NOT RELEASABLE TO CONTRACTORS/CONSULTANTS (abbreviated NOCONTRACT or NC) were rendered obsolete effective 12 April 1995. No permission of the originator is required to release, in accordance with this directive, material marked WNINTEL. Holders of documents prior to 12 April 1995 bearing the NOCONTRACT marking should apply the policies and procedures contained in DCID 1/7, section 6.1, for possible release of such documents.

(2) *Remarking.* Remarking of material bearing the WNINTEL, or NOCONTRACT, control marking is not required; however, holders of material bearing these markings may line through or otherwise remove the marking(s) from documents or other material.

(3) Obsolete markings. Other obsolete markings include: WARNING NOTICE–INTELLIGENCE SOURCES OR METHODS INVOLVED, WARNING NOTICE–SENSITIVE SOURCES AND METHODS INVOLVED, WARNING NOTICE–INTELLIGENCE SOURCES AND METHODS INVOLVED, WARNING NOTICE–SENSITIVE INTELLIGENCE SOURCES AND METHODS INVOLVED, CONTROLLED DISSEM, NSC PARTICIPATING AGENCIES ONLY, INTEL COMPONENTS ONLY, LIMITED, CONTINUED CONTROL, NO DISSEM ABROAD, BACKGROUND USE ONLY, USIB ONLY, NFIB ONLY.

b. Questions with respect to current applications of all control markings authorized by earlier directives on the dissemination and control of intelligence and used on documents issued prior to the effective date of DCID 1/7, 30 June 1998, should be referred to the agency or department originating the intelligence so marked.

4–14. Downgrading instructions

Downgrading instructions are not required for every classified document, but they must be placed on the face of each document to which they apply. When the original classification authority has determined that a document will be downgraded to a lower classification upon the passage of a date or event, the document will be marked: "Downgrade to SECRET on…" followed by the date or event, and/or "Downgrade to CONFIDENTIAL on…" followed by the date or event. This marking is placed immediately before the "Declassify on" line and is used in addition to, and not as a substitute for, declassification instructions.

4–15. The Modern Army Recordkeeping System

a. Purpose. The purpose of Army recordkeeping is to properly manage information, from its creation through final disposition, according to federal laws and Army recordkeeping requirements. AR 25–400–2:

(1) Establishes the Modern Army Recordkeeping System (MARKS) as a portion of the Army Information Resources Management Program (AIRMP).

(2) Furnishes the only legal authority for destroying nonpermanent Army information.

(3) Provides life–cycle management instructions for the systematic identification, maintenance, storage, retirement, and destruction of Army information recorded on any medium (paper, microforms, electronic, or any other).

(4) Ensures that the commander and staff have the information needed to accomplish the mission; that they have it when and where they need it; that they have it in usable format; and that it is created, maintained, used, and disposed of at the least possible cost.

(5) Preserves those records needed to protect the rights and interests of the Army and its members and former members, and those that are of permanent value.

(6) Ensures records related to matters involved in administrative or legal proceedings will be retained until the staff judge advocate or legal adviser authorizes resumption of normal disposition.

(7) Provides for the systematic removal of less active records from office space to low–cost storage space.

b. Application. MARKS applies to—

(1) All unclassified Army records, including For Official Use Only (FOUO) and sensitive, regardless of media.

(2) All classified Army records through SECRET. Records that are TOP SECRET may be set up under MARKS, or in any manner that will make accountability and control easier. Regardless of the arrangement used, however, the disposition instructions in this regulation, and under MARKS, will be applied to TOP SECRET records.

c. Principles.

(1) Within the MARKS system, records are identified and filed under the number of the primary directive that prescribes those records be created, maintained, and used.

(2) The file number is the key to MARKS. It identifies the records for filing and retrieval. MARKS numbers are made up by the prescribing directive number followed by an alpha suffix. See section II, appendix F, for the recordkeeping requirements of file titles and dispositions for records created and maintained under the purview of this regulation.

d. Further guidance. Further guidance on the management and disposition of files and records can be found in AR 25–400–2.

Section II
Marking Special Types of Documents

4–16. Documents with component parts

If a classified and/or sensitive document has components likely to be removed and used or maintained separately, each component will be marked as a separate document. Examples of components are annexes, appendices, major parts of a report, or reference charts. If the entire major component is UNCLASSIFIED, it can be marked on its face, top and bottom: "UNCLASSIFIED", and a statement added: "All portions of this (annex, appendix, etc.) are UNCLASSIFIED." No further markings are required on this type of component.

4–17. Transmittal documents

Transmittals are documents that have classified and/or sensitive documents enclosed with or attached to them. An example is a letter with classified enclosures or a document that is used to describe the transmission of classified equipment, documents, or other material. The transmittal document itself may contain information classified and/or sensitive the same or higher than the material transmitted. Often the transmittal document itself is UNCLASSIFIED or classified at a lower level than the material being transmitted or enclosed.

a. If the transmittal contains information classified and/or sensitive the same or higher than the documents being transmitted, the transmittal will be marked the same as any other classified and/or sensitive document.

b. If the information in the transmittal is UNCLASSIFIED or classified at a lower level than one or more of the documents being transmitted, the transmittal will be marked as follows:

(1) Mark the face of the transmittal conspicuously, top and bottom, in letters larger than the rest of the text, with the highest classification found in any of the enclosed documents being transmitted. For example, an UNCLASSIFIED transmittal that has one SECRET and two CONFIDENTIAL enclosures or attachments will be marked "SECRET".

(2) Mark the face of the transmittal to show its classification status when separated from the material being transmitted. For example, the following or similar statements apply: "UNCLASSIFIED WHEN SEPARATED FROM CLASSIFIED ENCLOSURES," "UNCLASSIFIED WHEN ATTACHMENT 3 IS REMOVED," "CONFIDENTIAL UPON REMOVAL OF ENCLOSURES," "REGRADED CONFIDENTIAL WHEN SEPARATED FROM ENCLOSURES," etc.

c. Any special warning notices that apply to the transmittal or to the documents being transmitted will be placed on the face of the transmittal document. Transmittals that are classified standing alone will be marked the same as other classified documents. UNCLASSIFIED transmittals will not be portion marked. The marking of classification at the top and bottom of interior pages of an UNCLASSIFIED transmittal is not required, but is encouraged.

4–18. Classification by compilation

When a document is classified and/or sensitive by compilation as discussed in paragraph 2–13, it will be marked as specified in paragraph 4–6d.

4–19. Translations

Translations of U.S. classified and/or sensitive information into a foreign language, will be marked with the appropriate U.S. classification/sensitivity markings and the foreign language equivalent. Section VIII, of this chapter, contains a list of foreign language classifications. The translations will clearly show the United States as the country of origin.

4–20. Electronically transmitted messages

This section does not pertain to documents transmitted by facsimile (FAX) transmission. Classified and/or sensitive

electronically transmitted messages will be marked the same as any other classified and/or sensitive document, with the following special provisions:

a. The first item in the text of the message will be the overall classification/sensitivity.

b. For messages printed by an automated system, overall and page markings will be applied by that system, provided they stand out conspicuously from the text. In older systems, this may be achieved by surrounding the markings with asterisks, stars, or other symbols. See appendix E of this regulation and AR 380–19 for more guidance.

c. A properly completed "Classified by" or "Derived from" line, reason, declassification instructions, and downgrading instructions (when applicable), will be included in the last lines of the message. Inclusion of a "Classified by" or "Derived from" line in the message is a new requirement. Declassification and downgrading instructions will not be used for messages containing Restricted Data or Formerly Restricted Data (RD or FRD). The abbreviations "CLAS" for "Classified by", "DECL" for "Declassify on", "DERV" for "Derived from" and "DNG" for "Downgrade to" may be used on messages.

4–21. Documents marked for training purposes

Documents that contain no classified and/or sensitive information, but are marked with classification/sensitivity markings for training purposes, will be marked to clearly show that they are actually UNCLASSIFIED. An appropriate statement will be placed on each page of the document, for example, "CLASSIFIED FOR TRAINING ONLY", "UNCLASSIFIED SAMPLE", or "CLASSIFICATION MARKINGS FOR TRAINING PURPOSES ONLY". The term "training purposes only" does not mean the sending of mock or fake classified and/or sensitive messages during field exercises and subsequently marking them for automatic declassification/destruction on ENDEX (end–of–exercise). It is used for the purpose of providing examples of how classified and/or sensitive markings are properly applied, such as handbooks and other like publications.

4–22. Files, folders, and groups of documents

Files, folders, and similar groups of documents containing classified and/or sensitive information will be clearly marked as to the highest classification/sensitivity of information contained therein. The classification/sensitivity marking will be on the outside, front and back, and top and bottom, of the file or folder. Attaching a document cover sheet to the outside of the file or folder is acceptable in satisfying this requirement. When cover sheets are used, they will not be attached when the file is in a secure storage container. When cover sheets are removed, when the item is in secure storage, the file or folder must be marked to indicate the highest level of classified and/or sensitive information contained in the file.

4–23. Printed documents produced by AIS equipment

There are no special provisions for documents produced by Automated Information Systems (AIS) which function as word processing systems (see appendix E of this regulation for further guidance). Documents produced on an AIS will be marked like other documents. For other AIS–generated documents, special exceptions may apply where the application of the marking requirements of this chapter are not feasible. These exceptions are:

a. Classification/sensitivity markings on interior pages of fan–folded printouts are required. These markings may be applied by the AIS equipment even though they may not meet the standard requirement of being conspicuous. At a minimum, the first page of the document and the back of the last page will be over–stamped, with the classification/sensitivity, in letters larger than the print.

b. Special warning notices, identification of classification sources, and declassification (and downgrading, where applicable) instructions will either be marked on the cover of the document, or on the first page if there is no cover, or will be placed on a separate notice attached to the front of the document.

c. Pages or other portions of AIS printouts removed for separate use or maintenance, will be marked in the standard manner as individual documents.

Section III
Marking Special Types of Material

4–24. General policy

When classified and/or sensitive information is contained in AIS equipment, hardware, AIS media, or on film, tape, or other audio/visual media, or in another form not commonly thought of as a document, the marking provisions of this and other applicable regulations will be met in a way that is compatible with the type of material. The main concern is that holders and users of the material are clearly warned of the presence of classified and/or sensitive information needing protection. The information provided by the other markings required by this regulation will also be made available, either on the material or in a document or notice that accompanies it. Particular exceptions are noted below. The requirements of this chapter do not apply to the marking of security containers. The only markings allowed on security containers are those outlined in chapter 7 of this regulation.

4–25. Telephone or communications directories

Telephone or communications directory notice. Official U.S. Army telephone or communications directories will display the following notice on the front cover or prominently within the general information section: ATTENTION! DO NOT PROCESS, STORE, OR TRANSMIT CLASSIFIED INFORMATION ON NONSECURE TELECOMMUNICATIONS SYSTEMS. OFFICIAL DOD TELECOMMUNICATIONS SYSTEMS—INCLUDING TELEPHONES, FACSIMILE MACHINES, COMPUTER NETWORKS, AND MODEMS—ARE SUBJECT TO MONITORING FOR TELECOMMUNICATIONS SECURITY PURPOSES AT ALL TIMES. USE OF OFFICIAL DOD TELECOMMUNICATIONS SYSTEMS CONSTITUTES CONSENT TO INFORMATION SYSTEMS SECURITY MONITORING.

4–26. Blueprints, schematics, maps, and charts

Blueprints, engineering drawings, charts, maps, and similar items not contained in a classified and/or sensitive document will be marked with the overall highest classification/sensitivity of information contained therein. The classification/sensitivity marking will not be abbreviated, and will be conspicuous. The classification/sensitivity marking should be applied to the top and bottom of the material, if possible, or in some manner as to ensure the classification/sensitivity is readily known. The legend or title must also be marked to show its classification/sensitivity. An abbreviated marking in parentheses following the legend or title may be used. If the item is large enough that it is likely to be rolled or folded, the classification/sensitivity markings will be placed to be visible when the item is rolled or folded.

4–27. Photographs, negatives, and unprocessed film

a. Photographs and negatives will be marked with the overall highest classification/sensitivity of information contained thereon. Photographs will be marked on the face, if possible. If not possible to mark the face, the classification/sensitivity marking will be placed on the reverse side of the photograph. Other markings required by this regulation will be placed on photographs along with the classification/sensitivity marking, or will be included in accompanying documentation.

b. Roll negatives, positives, and unprocessed film, containing classified and/or sensitive information, will be marked with the overall highest classification/sensitivity of the information contained on the film. This marking will be placed either on the film itself, or on the canister, if one is used. If placed on the film itself, the marking will be placed at the beginning and end of the roll.

4–28. Slides and transparencies

a. Each slide or transparency will be marked with the highest level of classification/sensitivity contained on the slide or transparency, so that the marking is visible to personnel seeing the item projected, and to personnel physically holding the item. Each slide or transparency will have the classification/sensitivity and special warning notices (if any) marked on both the image area of the item and on the border, holder, or frame. Other required security markings (for example, classification authority and declassification instructions) may be placed in the image area; on the border, holder, or frame; or in a document or notice accompanying the item.

b. When a group of slides or transparencies is used together and maintained together as a set, for example, in the case of a set of briefing slides, each slide or transparency will have the classification/sensitivity marking and special warning notices (if any) on it, applied as described in subparagraph a, above. The other required security markings may be placed on the first slide or transparency (or the border, holder, or frame for the first item) in the set; these markings are not required to be placed on the other slides or transparencies in the set.

4–29. Motion picture films and videotapes

Classified and/or sensitive motion picture films and videotapes must be marked with their classification/sensitivity and warning notices (if any) at the beginning and end of the played or projected portion. Other required security markings will be placed at the beginning of the projected or played portion. Reels and cassettes will be marked with the overall classification/sensitivity of the item and kept in containers marked with the classification/sensitivity and other required security markings.

4–30. Sound recordings

Sound recordings containing classified and/or sensitive information will have an audible statement of their classification/sensitivity and warning notices (if any) at the beginning and end of the recording. Reels or cassettes will be marked with the overall classification/sensitivity of the item and kept in containers marked with the classification/sensitivity and other required security markings of the item. Where this is not possible, this information will be recorded on documentation accompanying the item.

4–31. Microfilms and microfiche

Microfilm, microfiche, and similar media, will be marked so that the overall classification/sensitivity and warning notices (if any) are shown in the image area and can be read or copied as part of the item. Such items also will be marked with the classification/sensitivity markings and at least an abbreviation of any warning notices applied in such

a way as to be visible to the unaided (naked) eye. Other required security markings will be either placed on the item or included in an accompanying document or notice.

4–32. Removable AIS storage media

a. Further details on the policy to protect and mark classified and/or sensitive information stored on AIS media is contained in AR 380–19, and appendix E, of this regulation. The following minimum standards are required for removable AIS storage media. Removable AIS storage media include magnetic tape reels, disk packs, diskettes, CD–ROMs, removable hard drives, disk cartridges, optical disks, paper tape reels, magnetic cards, tape cassettes and micro–cassettes, and any other device on which data is stored, and which normally is removable from the system by the user or operator. All such devices, containing classified and/or sensitive information, will be conspicuously marked with the highest level of classification/sensitivity stored on the device, and with any warning notices that may apply to the information. Other required markings, for example, classification authority and declassification instructions, will be marked on the outside of the device. An exception is, if classified and/or sensitive documents or files are prepared on a word processor and are stored on a floppy disk, and each document or file bears its own classification authority and declassification instructions, as entered with the word processor, the disk does not need to be marked with this information. If the required information is not stored in readily accessible format on the media, it must be marked on the outside of the media (for example, with a sticker or tag) or placed on documentation kept with the media.

b. One of the misconceptions many AIS users have, is in the use of media and AIS equipment of differing classifications. If a user places a removable medium, such as a diskette, that is marked and contains only unclassified data, into a classified AIS, they assume that as long as they don't save classified information on it, then their diskette is still unclassified. By the AIS merely accessing the diskette there arises the possibility of classified information being written to the diskette. Classified information is most often unknowingly transferred to the diskette in this manner, in one of the following three methods: "lost clusters;" "unallocated space;" and "slack space."

(1) A cluster is a group of disk sectors. The operating system assigns a unique number to each cluster and then keeps track of files according to which clusters they use. Occasionally, the operating system marks a cluster as being used even though it is not assigned to any file. This is called a lost cluster. You can free up disk space by reassigning lost clusters, but you should first make sure that the clusters do not, in fact, contain valuable data. In DOS and Windows, you can find lost clusters with the ScanDisk utility. DOS and Windows keep track of clusters with the File Allocation Table (FAT). The size of each cluster depends on the disk's partition size.

(2) Unallocated space is space on a storage medium that the Disk Operating System (DOS) regards as available for use when needed. As far as DOS is concerned, the space is empty. In actuality the space may contain deleted files, which are not gone until they are overwritten, or partial fragments of old files to include old file slack.

(3) The DOS and Windows file systems use fixed–size clusters. DOS and older Windows systems use a 16–bit file allocation table (FAT), which results in very large cluster sizes for large partitions. Even if the actual data being stored requires less storage than the cluster size, an entire cluster is reserved for the file. Unless a file is EXACTLY one or more clusters in length, which is unlikely, there will always be space between the file's "End of File" marker and the end of the cluster associated with that file. Any data that is located in that space, or the empty space itself, is referred to as file slack. An unintended consequence of the way that DOS handles its buffers, is that the buffer's contents may be "dumped" into file slack or "slack space". When files are written over a used diskette, one that had files on it but they were erased but not fully reformatted, the new files do not overwrite all the preceding data, therefore there is still readable data in the files slack space area. Also, whenever a file is used on an AIS, it acquires slack space from the hard drive. This can inadvertently be transferred back onto the diskette. Normal text editing software cannot read this area, however there are programs available to accomplish this. For example, if the partition size is 2 GB, each cluster will be 32 K. Even if a file requires only 4 K, the entire 32 K will be allocated, resulting in 28 K of slack space. Windows 95 (OSR 2), Windows 98, and Windows NT 4.0 resolve this problem by using a 32–bit FAT (FAT32) that supports cluster sizes as small as 4 K for very large partitions, however this still does not preclude the possibility of data in slack space.

c. This area has always been a sore spot for DA organizations. Material used or produced on, for, and by, an AIS, comprises the greater majority of an organization's day–to–day operations. For details on the security procedures for documents created for and on an AIS, web–based display, and common AIS security related misconceptions, see appendix E of this regulation.

4–33. Fixed and internal AIS storage media

Systems Managers will make sure that AIS, including word processing systems, provide for classification/sensitivity designation of data stored in internal memory or maintained on fixed storage media.

4–34. Standard form (SF) labels

a. If not marked otherwise, items covered by this section will be marked with the following labels:

(1) SF 706 – (TOP SECRET Label for ADP Media).

(2) SF 707 – (SECRET Label for ADP Media).

(3) SF 708 – (CONFIDENTIAL Label for ADP Media).

(4) SF 710 – (UNCLASSIFIED Label for ADP Media).

(5) SF 711 – (Data Descriptor Label for ADP Media).

(6) SF 712 – (CLASSIFIED SCI Label).

b. SF 710 is not required to be used in environments where there is no classified information created or used. In environments where classified information is created or used, SF 710 labels will be used to identify unclassified media from the classified AIS removable storage media. Media that is classified at the SCI level will have both the SF 711 and the SF 712 labels attached. The SF 711 will indicate the security classification of the data.

Section IV
Changes in Markings

4–35. Downgrading and declassification in accordance with markings

a. When a document is marked for downgrading or declassification on a date or event, the downgrading or declassification is automatic at the specified time unless notification to the contrary is received from the originator, the original classification authority, or other appropriate authority. There is no requirement to refer the document to the originator on or before the date or event for a downgrading or declassification decision. If a holder of the document has reason to believe it should not be downgraded or declassified, the holder will notify the originator and OCA (if known) of the information.

b. When a document is declassified in accordance with its markings, the overall and page markings will be canceled, if practical. If it is not practical to cancel the marking on each page on a bulky document, the page marking will be canceled, as a minimum, on the first page, on the cover (if there is one), title page (if there is one), and on any interior page that is copied or removed from the document.

c. If a document is downgraded (assigned a lower level of classification/sensitivity) in accordance with its markings, the old classification/sensitivity markings will be canceled and substituted with the new, lower classification/sensitivity marking. New classification/sensitivity markings will be applied under the same policy as stated in subparagraph b, above, for declassification markings.

4–36. Downgrading and declassification earlier than scheduled

If a document is declassified or downgraded earlier than indicated by its markings, the rules for remarking as stated in paragraph 4–35 will be followed. In addition, the date of remarking and the authority for the action will be placed on the face of the document. The date of the remarking is considered the date that the remarking was authorized (for instance, date of the notice to remark) or, if no date is specified, the date that the material was physically remarked. The authority for the action is the identity of the OCA, or the designated declassification authority, who directed the action and the identification of the correspondence, classification guide, or other instruction or notification which required it.

4–37. Upgrading

If a document is upgraded (assigned a higher level of classification/sensitivity), all classification/sensitivity markings affected by the upgrading will be changed to the new markings, without exception. In addition, the date of the remarking and the authority for the action will be placed on the face of the document. The date of the remarking is considered the date that the remarking was authorized (for instance, "Date of Notice to Remark") or, if no date is specified, the date that the material was physically remarked. The authority for the action is the identity of the OCA who directed and action and the identification of the correspondence, classification guide, or other instruction or notification which required it.

4–38. Posted notice on bulk quantities of material

When the volume of material involved in a remarking action is so large that individually remarking each document is determined by the commander to cause serious interference with operations, the custodian will attach a notice to the storage unit providing the required information as stated in paragraphs 4–35, 4–36, and 4–37. When individual documents are permanently removed from the storage unit, they must be individually marked as required in paragraphs 4–35, 4–36, and 4–37. If documents are removed to be transferred in bulk to another storage unit, they need not be remarked if the new storage unit also has a proper notice posted.

4–39. Extensions of duration of classification

If information has been marked for declassification on a specific date or event and the duration of classification is subsequently extended, the "Declassify on" line will be changed to show the new declassification instructions, the identity of the OCA authorizing the extension, and the date of the authorizing action. For example, "Declassify on: Classification extended on 1 Dec 2005 to 1 Dec 2015 by LTG Soldier, Commanding General, US Army Classification Command."

Section V
Remarking and Using Old Classified Material

4–40. Old markings
Some classified and/or sensitive documents are still in use which were marked, as specified by earlier versions of this regulation, based upon an earlier EO. There is no requirement to remark this material with the new markings specified by this regulation and EO 12958. This material will not be remarked unless specific instructions are received from the original classification authority. If the material is marked for automatic downgrading or declassification on a specific date or event, it will be remarked as specified in paragraph 4–34. If the document does not specify a specific date or event for downgrading or declassification (for example, if it is marked "Declassify on: OADR"), it will not be remarked until it reaches 25 years. Chapter 3 contains the policy on the marking of information over 25 years old.

4–41. Earlier declassification and extension of classification
The requirements for declassification, exemptions from automatic declassification, and extensions of original classification dates apply to all classified information, including that classified under previous Executive Orders. Specific policy on classification and marking of information classified by previous Executive Orders is addressed in this regulation.

Section VI
Safeguarding Joint Chiefs of Staff Papers

4–42. General
This section prescribes responsibilities and establishes procedures to secure and distribute Joint Chiefs of Staff (JCS) papers within the Army.

4–43. References
a. AR 380–10, Technology Transfer, Disclosure of Information and Contacts with Foreign Representatives.
b. JCS Policy Memorandum 39, Release Procedures for JCS Papers.
c. SF 135 (Records Transmittal and Receipt) and SF 135A (Records Transmittal and Receipt (Continuation).

4–44. 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.
(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 HQDA (DAMO–ZJC), WASH DC 20310–0421.

4–45. Requirements
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 outlined in paragraph 4–46.

4–46. Access
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).

4–47. 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, who have actual or potential access to JCS papers, will be briefed on their responsibilities regarding JCS papers at the time of initial assignment, and annually thereafter.

4–48. 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 20 August (YYYY), the Joint Chiefs of Staff approved/ requested/directed (fill–in the information)."

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 (OJCS) will officially notify the holders.

4–49. Release and Distribution of Joint Strategic Planning System Documents

Release and distribution of Joint Strategic Planning System (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. JSPS documents will be accounted for by a continuous chain of receipts.

d. The CSA may distribute JSPS documents, except Joint Strategic Capabilities Plan (JSCP), 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.

4–50. Release and Distribution of Joint Operation Planning System Documents

Release and distribution of Joint Operation Planning System (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 plans.

(2) Related documents prepared by supported, supporting, and subordinate commanders.

4–51. 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), WASH 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.

d. Release of JSPS and JOPS documents will be as outlined in paragraphs 4–49 and 4–50, above.

4–52. 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 cognizant Army staff agency for validation.

d. These requests will be forwarded with recommendations to HQDA (DAMO–ZCJ), WASH DC 20310–0421 for action.

e. The numbers of JCS green papers (JCS 0000/000) less than 10 years old will not be referenced in the text of any extract for release to agencies outside DA.

f. Nonconcurrent JCS documents interfiled in nonconcurrent DA records may be transferred to records centers according to established requirements. In this case, SF 135 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.

4–53. Reproduction of JCS documents

JCS documents will not be reproduced except as authorized under paragraph 4–49b.

Section VII
Foreign Government Information

4–54. Policy

Each foreign government has its own policy on what information is classified and/or sensitive and for how long it will remain classified and/or sensitive. The classification/sensitivity and declassification policy of another government cannot and, in many cases, does not parallel that of the United States. When Foreign Government Information (FGI) is disclosed to the United States, it is done so with the understanding that the information will be protected and will not be declassified or released to another nation or to the public without the express permission of the originating government. This applies to both foreign government documents as well as in situations in which foreign government information is incorporated in a classified U.S. document. It is, therefore, important to identify foreign government information that is contained in U.S. classified documents. Throughout this regulation, when the term "foreign government" is used, the policy also applies to international pact organizations (for instance NATO), unless otherwise specified.

4–55. Equivalent U.S. classification designations

Foreign classification designations generally parallel U.S. classification designations. The exception is that many foreign governments have a fourth (lowest) classification level called "RESTRICTED". A table of the equivalent foreign and international pact organization security classifications is contained in section VIII.

4–56. Marking NATO documents

Classified documents originated by NATO, if not already marked with the appropriate classification in English, will be so marked. Other markings, such as the "Classified by/Derived from" line and declassification instructions will not be placed on documents originated by NATO. Documents originated by NATO that are marked "RESTRICTED" will be marked with the following additional notation: "TO BE SAFEGUARDED IN ACCORDANCE WITH USSAN INSTRUCTION 1–69". The USSAN Instruction 1–69 is implemented within the Department of the Army in AR 380–15 (AR 380–15 is classified NATO CONFIDENTIAL).

4–57. Marking Other Foreign Government Documents

a. If the security classification designation of the foreign government document is shown in English, no other classification marking will be applied. If the foreign classification designation is not shown in English, the equivalent overall U.S. classification designation (TOP SECRET, SECRET, or CONFIDENTIAL) will be marked conspicuously on the document. See figure 4–14 for English terms to use in marking classified NATO documents. When a foreign government document is marked with a classification designation having no U.S. equivalent, such as RESTRICTED, it will be marked as specified in paragraph b, below.

b. Most foreign governments use a fourth (lowest) classification designation. Such designations are or equate to the foreign classification RESTRICTED. If foreign government documents are marked with any of these classification designations, no other classification marking will be applied. For such cases, the notation: "THIS CLASSIFIED MATERIAL IS TO BE SAFEGUARDED IN ACCORDANCE WITH AR 380–5, DOD Directive 5200.1–R, OR THE

NISPOM". An alternative authorized marking is "THIS CLASSIFIED MATERIAL IS TO BE SAFEGUARDED IN ACCORDANCE WITH DOD 5200.1–R OR THE NISPOM". When that is used, it will be understood that the governing regulation for DA commands is still AR 380–5.

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.

4–58. Marking Foreign Government Information Provided in Confidence

Foreign documents containing FGI not classified by the foreign government but provided in confidence to the Department of the Army or any other element of the U.S. government or its contractors, will be classified if the information is covered under one or more or the reasons for classification listed in chapter 2. If it is deemed classified, it will be marked with the appropriate U.S. classification. If not, classification markings will not be applied to the document. If it is not otherwise obvious that the document was provided in confidence, DA commands can place the notation "FOREIGN GOVERNMENT (or list the name of the country) INFORMATION PROVIDED IN CONFIDENCE". That notation is not a requirement but is a consideration for cases in which the document, or copies of the document, can leave the control of the personnel who were aware of the confidentiality under which the information was provided.

4–59. Marking of Foreign Government Information in Department of the Army Documents

In addition to the other markings required in this regulation, the following markings will be used in classified DA documents containing FGI (see definition of "Foreign Government Information" in appendix J).

a. When used in a classified DA document, FGI must be marked to prevent premature declassification or unauthorized access by third country nationals. A DA document that contains FGI will be marked on the face of the document to indicate that FGI is contained therein. In most situations the document will be marked "THIS DOCUMENT CONTAINS (insert name of country) INFORMATION". As an alternative—and to be used in cases in which identification of the country would provide additional classified information or in cases in which the foreign country does not wish to be identified—the document will be marked: "THIS DOCUMENT CONTAINS FOREIGN GOVERNMENT INFORMATION" or "FOREIGN GOVERNMENT INFORMATION". In those situations the record file copy of the document will contain the identification of the foreign government providing the information. A DA document containing NATO classified information will be marked on the face of the document, "THIS DOCUMENT CONTAINS NATO CLASSIFIED INFORMATION". The face of the document is considered to be the cover and title page, or the first page where there is no cover or title page. In addition, the portions will be marked to identify the classification level, including UNCLASSIFIED, and the country of origin. Examples of portion marking are as follows: TOP SECRET information from the United Kingdom (UK–TS), SECRET information from Germany (GE–S), NATO SECRET information (NATO–S) or (NS), CONFIDENTIAL information from France (FR–C), and UNCLASSIFIED information from Costa Rica (CR–U). In unusual situations in which the foreign government does not wish to be specifically identified, the portions will be marked "FGI" together with the appropriate classification; for example, (FGI–S). In those cases the originator will maintain the identity of the foreign country furnishing the information with the record file copy of the document. Except in those unusual situations in which the foreign country does not wish to be identified, the "Classified by" or "Derived from" line will identify the U.S. as well as foreign classification sources. In cases in which multiple U.S. and one or more foreign sources are used, the term "Multiple sources and the Government of (insert name of foreign country or countries)" will be used on the "Classified by" or "Derived from" line. In those cases in which identification of the foreign country furnishing the information would reveal additional classified information, or when the foreign country does not wish to be identified, the foreign sources of classification will be maintained with the record file copy of the document and the term "Foreign Government" will be shown in addition to the U.S. sources on the "Classified by" or "Derived from" line.

b. When foreign government RESTRICTED or NATO RESTRICTED information is included in an otherwise unclassified DA document, the document will be marked NATO RESTRICTED. All marking requirements for classified documents will apply, to include portion markings which will show the letter "R" after the abbreviation for the country that furnished the information (for example, RESTRICTED information furnished by Canada (CA–R); or (NATO–R) or (NR) for NATO RESTRICTED. Each page containing the RESTRICTED information would be so marked as "(insert name of country or international organization) RESTRICTED" or "THIS PAGE CONTAINS (insert name of country or international organization) RESTRICTED INFORMATION". In addition, the applicable notice from paragraph a., above, will be included on the face of the document.

c. The "Classified by" or "Derived from" line of a DA document that is classified only because it contains classified foreign government information will be completed as described in this chapter for derivative classifications and, therefore, the term "Derived from" will be used. The "Declassify on" line will read "Source not marked".

Sample of Marking an Originally Classified Document

CLASSIFICATION MARKINGS FOR TRAINING PURPOSES ONLY
SECRET

Subject: Sample of Marking an Originally Classified Document (U)

1. (C) This page is UNCLASSIFIED and is marked SECRET for training purposes only. IMPORTANT: *You must be an Original Classification Authority to originally classify a document*. A majority of cleared personnel who generate classified documents are NOT Original Classification Authorities (OCAs). To be an OCA you must be appointed by the Secretary of the Army or the DCSINT. In most cases, documents are classified based on a Security Classification Guide or guidance (that was approved by an OCA) or upon information taken out of a source document (or both). This sample memo only pertains to those relatively few cases in which an OCA is generating a document that the OCA is originally classifying.

2. (S) In this example, the OCA is an official that has been delegated Original Classification Authority for a particular program. The OCA must be identified (see paragraph 4-8a), the reason that the information is classified must be stated (see paragraph 4-9), and the OCA must indicate a date, event, or exemption category for declassification (see paragraph 4-9a). If there is more than one reason or exemption, then all must be listed. In this example, the OCA has selected reason 1.5(a) (military plans, weapons systems, or operations). Instead of a date or event for declassification within 10 years, the OCA has authorized exemption category X2 (reveal information that could assist in the development or use of weapons of mass destruction) that must be protected beyond 10 years.

I.M. Trying
Director, Security Awareness

Classified by: LTG A. SECRET, Chief of Weapons Programs, Army Security Is Important Command
Reason: 1.5(a)
Declassify on: X2
Date of source: 26 March 1999

SECRET
CLASSIFICATION MARKINGS FOR TRAINING PURPOSES ONLY

Figure 4-1. Sample of Marking an Originally Classified Document

Sample of Marking a Classified Document that is Exempt from the 25-Year Automatic Declassification

CLASSIFICATION MARKINGS FOR TRAINING PURPOSES ONLY
SECRET

Subject: Sample of Marking a Classified Document that is Exempt from the 25 Year Automatic Declassification (U)

1. (C) This page is UNCLASSIFIED and is marked SECRET for training purposes only. Chapter 3 provides the policy for marking information contained in records that will be more than 25 years old on 17 April 2000 and have been determined to have permanent historical value under title 44, USC. In summary, under EO 12958 (section 3.4) information more than 25 years old by 17 April 2000 and that is contained in records that have been determined to have permanent historical value under title 44, USC will be automatically declassified starting on 17 April 2000 *unless* that information is exempted from declassification.

2. (S) In this example, the OCA is an official that has been delegated Original Classification Authority for a particular program. The OCA must be identified (see paragraph 4-8a) and the reason that the information is classified must be stated (see paragraph 4-9) The OCA has indicated the information is exempt from automatic declassification within 25 years (see paragraph 4-11). In this example, the OCA has selected reason 5 (reveal U.S. military war plans that remain in effect). Instead of a date or event for automatic declassification, the OCA has used this exemption category and included a date outside the 25-year window.

R.U. Real
Director, Security

Classified by: BG I. INCHARGE, Chief, Army Program Command
Reason: 1.5(a)
Declassify on: 25X5(December 31, 2026)
Date of source: 22 April 1998

SECRET
CLASSIFICATION MARKINGS FOR TRAINING PURPOSES ONLY

Figure 4-2. Sample of Marking a Classified Document that is Exempt from the 25–Year Automatic Declassification

Sample of Marking an Originally and Derivatively Classified Document

CLASSIFICATION MARKINGS FOR TRAINING PURPOSES ONLY
SECRET

Subject: Sample of Marking a Classified Document That Contains Some Information Originally Classified and Some Information Derivatively Classified From A Source Document (U)

1. (U) This page is UNCLASSIFIED and is marked SECRET for training purposes only in order to illustrate classification markings. In the case of either derivatively or originally classified documents, the classification/declassification markings are usually placed at the bottom of the face of the document on either the left, right, or center.

2. (S) In this example, the Original Classification Authority (OCA) is generating a document that has information that the OCA originally classified on 21 August 1996 but also contains information classified by another OCA that was taken from a source document dated 11 November 1995. In this case, the document is considered to be a derivatively classified document even though some of the information is originally classified. If there is any derivatively classified information, the document *must* be marked under the rules for derivative classification. In this example, the OCA classified information under two exemption categories, X3 and X6, because the information could not be declassified within ten years. The source document shows a declassification date of 10 December 2001 (the other OCA did not select an exemption category). The declassification date is always the most restrictive date or event (one that occurs farthest in the future). Since the X3 and X6 is an indefinite declassification date, it is always selected over a specific date. The date of the source is always the date of the most recent source used (in this case, the date of original classification, 21 August, 1996).

R. U. Confused
Chief, I.M. Ready Command

Classified by: Multiple Sources
Reasons: 1.5e, 1.5d, and derivatively classified source
Declassify on: Source marked X3,6
Date of Source: 21 August 1996

SECRET
CLASSIFICATION MARKINGS FOR TRAINING PURPOSES ONLY

Figure 4-3. Sample of Marking an Originally and Derivatively Classified Document

Sample of Marking a Document Derivatively Classified from Information in Old Document

CLASSIFICATION MARKINGS FOR TRAINING PURPOSES ONLY
SECRET

Subject: Sample of How to Mark a Classified Document Derivatively Classified from Information in Old Document (U)

1. (C) This page is totally UNCLASSIFIED, if this paragraph were really CONFIDENTIAL, it would be marked "C" in parentheses just after the paragraph number, or just before the first word if there is no paragraph numbering used. Mark the classification of the subject or title at the end of the subject or title. This makes it easier to refer to the memo or other document if the subject or title is kept UNCLASSIFIED. If the subject or title is classified, then use the appropriate abbreviation of (C), (S) or (TS) for CONFIDENTIAL, SECRET, and TOP SECRET, respectively.

2. (U) In this example the lead-in part of the paragraph is UNCLASSIFIED, but the subparagraphs are classified at different levels. Each portion of the paragraph stands on its own and is marked according to the information in that particular section.

a. (S) The new way to mark classified documents contains some changes. Portion (paragraph), page, and overall markings as well as where to place warning notices has essentially not changed (see paragraphs 4-3 through 4-6 for overall, page, and portion markings, and 4-12 for warning notices). The main point to remember is: could the reader figure out what is classified and at what level by the markings? The answer must be yes.

b. (C) What has changed? Quite a lot.

3. (S) In this example, the memo is derivatively classified based solely on information classified under the old system (EO 12356) and marked "Declassify on OADR". Remember, OADR is no longer used.

H. P. CULVER
Chief, How to Classify Division

Derived from: HQDA Memo, 10 Feb 94
Subj: "Security is a FORCE MULTIPLIER"
Declassify on: Source marked OADR
Date of Source: 10 February 1994
SECRET
CLASSIFICATION MARKINGS FOR TRAINING PURPOSES ONLY

Figure 4-4. Sample of Marking a Document Derivatively Classified from Information in Old Document

Sample of Marking a Document When each Portion is Unclassified but Together are classified by Compilation

CLASSIFICATION MARKINGS FOR TRAINING PURPOSES ONLY
CONFIDENTIAL

Subject: Sample of Marking a Document When each Portion is Unclassified but Together are Classified by Compilation (U)

1. (U) This page is totally UNCLASSIFIED, and is marked classified for training purposes only. Mark the classification of the subject or title at the end of the subject or title, keeping the title UNCLASSIFIED, if possible. This makes it easier to refer to the memo or other document if the subject or title is kept UNCLASSIFIED.

2. (U) In this example the each of the paragraphs are UNCLASSIFIED, but the whole page is classified at the assigned level. Each portion of the paragraph stands on its own as UNCLASSIFIED and is marked according to the information in that particular section. The problem arises when the information is presented together.

3. (U) A classification guide, dated 28 May 1996, that concerns a very sensitive military operation, states that the type of information, when compiled, revealed in this memo, is classified as CONFIDENTIAL, and exempted by category number 4, section 1.6 of EO 12958. Exemption 4 concerns information on U.S. military plans, or national security emergency preparedness plans.

4. (U) Therefore, a statement, such as the one in paragraph 5, will be included and all appropriate page and portion markings included.

5. (U) This portion is UNCLASSIFIED when extracted alone. When it is combined with one or more of the above paragraphs, this compilation is CONFIDENTIAL based on Section 1.5a, Executive Order 12958.

H. P. CULVER
Chief, How to Classify Division

Derived from: BO Missile Classification Guide and multiple sources
Declassify on: Source marked X4
Date of Source: 28 May 1996

CONFIDENTIAL
CLASSIFICATION MARKINGS FOR TRAINING PURPOSES ONLY

Figure 4-5. Sample of Marking a Document When each Portion is Unclassified but Together are classified by Compilation

Sample of Marking a Document Derivatively Classified from One Source Classified under the Current System

CLASSIFICATION MARKINGS FOR TRAINING PURPOSES ONLY
SECRET

Subject: Sample of How to Mark a Classified Document that is Derivatively Classified from One Source Classified under the Current System (C)

1. (S) This page is UNCLASSIFIED and is marked SECRET for training purposes only to illustrate classification markings. Note that in this example, the subject of the memo is classified CONFIDENTIAL. It is helpful to choose an UNCLASSIFIED subject or title, but sometimes use of a classified subject or title cannot be avoided.

2. (C) In this example, the memo is classified because it concerns a weapons system and that weapons system has a Security Classification Guide. In the classification guide, it states that the type of information in this memo is classified and at the levels of classification indicated. The classification guide reflects the new system of classifying and marking required as a result of EO 12958. The classification guide says that the information contained in this memo will be declassified "X3". That means it requires protection for more than 10 years based on exemption category number 3, found in section 1.6 of EO 12958. Exemption category 3 concerns information if released would impair the development or use of technology within a U.S. weapons system. The Original Classification Authority does not have to select a specific date or event for declassification (but can if deemed feasible) if the information qualifies under one of the exemption categories. In this case, no date or event for declassification was selected by the Original Classification Authority. The classification guide is dated 21 August 1996.

I. M. MOOSE
Chief, Army Needs Security Office

Derived from: Oxnard Missile (OM-1) Classification Guide: Dated 21 August 1996
Declassify on: Source marked X3
Date of Source: 21 August 1996

SECRET
CLASSIFICATION MARKINGS FOR TRAINING PURPOSES ONLY

Figure 4-6. Sample of Marking a Document Derivatively Classified from One Source Classified under the Current System

Sample of Marking a Document Derivatively Classified from Source Classified under the Old System and a Source Classified under the Current System

CLASSIFICATION MARKINGS FOR TRAINING PURPOSES ONLY

CONFIDENTIAL

Subject: Sample of How to Mark a Classified Document Derivatively Classified from a Source Classified under the Old System and a Source Classified under the Current System (U)

1. (C) This page is totally UNCLASSIFIED and is only marked CONFIDENTIAL for training purposes to illustrate classification markings.

2. (C) There have been many changes in the area of classification and declassification instructions that go on the front of the document. This may include: all information in the document is originally classified, all derivatively classified, a combination of original and derivative classifications, some of the information classified was marked under the old system, all of the information classified was marked under the old system, some or all originally classified information was marked under the old system but marked different ways, some or all RD, FRD or FGI in the document, etc.

a. (U) The new marking system is national policy and is implemented in this regulation.

b. (C) In this example, this memo is derivatively classified using two sources. One source (dated 19 August 1995) was marked under the old system as "Declassify on: OADR". The other source (dated 24 May 1996) is marked under the current system as "Declassify on X3 (meaning that it requires classification beyond ten years based on exemption category 3, as defined in Sec. 1.6, EO 12958). The "date of source" is date of the most recent source.

I. Wanna Learn
Chief, Hooah Division

Derived from: Multiple Sources
Declassify on: Sources Marked X3 and OADR
Date of Source: 24 May 1996
CONFIDENTIAL
CLASSIFICATION MARKINGS FOR TRAINING PURPOSES ONLY

Figure 4-7. Sample of Marking a Document Derivatively Classified from Source Classified under the Old System and a Source Classified under the Current System

Sample of a Document Derivatively Classified from Multiple Sources

CLASSIFICATION MARKINGS FOR TRAINING PURPOSES ONLY
TOP SECRET

Subject: Sample of How to Mark a Classified Document Derivatively Classified from Multiple Sources (U)

1. (TS) This page is UNCLASSIFIED and is marked TOP SECRET for training purposes only. While there are many possible situations for derivative classification, only the more common ones are shown in these figures.

2. (S) In this example, this memo is derivatively classified based on data on several subjects and those subjects are covered by two different Security Classification Guides.

a. (TS) One classification guide is dated 28 May 1996 and concerns a very sensitive military operation. That Security Classification Guide states that the type of information revealed in this memo is classified as TOP SECRET. A declassification date or event was not selected by the Original Classification Authority and the information was designated as exemption category number 4, section 1.6 of EO 12958. Exemption 4 concerns information on U.S. military plans, or national security emergency preparedness plans.

b. (C) The other classification guide is dated 10 December 1996 and concerns a weapons system. That guide states that the type of information revealed in this memo is classified CONFIDENTIAL. A declassification date or event was not selected by the OCA and the information was designated as exemption category 3, which concerns information that if revealed would impair the development or use of technology within a U.S. weapons system. Even though the first guide pertains to information classified at the higher level (TOP SECRET), the "Date of Source" line is always the most *recent* date of all the sources used--in this case, the date of the guide pertaining to the CONFIDENTIAL data in this memo.

Helen P. Security
Chief, Project Moose Radar

Derived from: Multiple Sources
Declassify on: Sources marked X3 and X4
Date of Sources: 10 December 1996

TOP SECRET
CLASSIFICATION MARKINGS FOR TRAINING PURPOSES ONLY

Figure 4-8. Sample of a Document Derivatively Classified from Multiple Sources

Sample of Marking a Document Where the Cover Memo is Unclassified but the Attachments are Classified

CLASSIFICATION MARKINGS FOR TRAINING PURPOSES ONLY
CONFIDENTIAL

Subject: Sample of Marking a Document Where the Cover Memo is Unclassified but the Attachments are Classified (U)

1. (U) This page is totally UNCLASSIFIED, and is marked classified for training purposes only. Mark the classification of the subject or title at the end of the subject or title, keeping the title UNCLASSIFIED, if possible. This makes it easier to refer to the memo or other document if the subject or title is kept UNCLASSIFIED.

2. (U) In this example this cover memorandum is UNCLASSIFIED, but the attachments are classified at the assigned level. Each portion of the paragraph, on this memorandum, stands on its own as UNCLASSIFIED and will be marked according to the information in that particular section. The cover memorandum will be marked with the highest overall classification of the complete package.

3. (U) When it is expected that the memorandum may be separated from the rest of the package, a statement, similar to the one in the lower right area, will be affixed.

4. (U) When this memorandum is separated from the rest of the package, be sure to line out the classification and remark it as UNCLASSIFIED (see paragraph 4-35 for more details).

I. M. ANOCA
Chief, I Can Classify Group

Derived from: BOOM Project Classification Guide
Declassify on: Source marked X2
Date of Source: 31 October 1998

Regrade UNCLASSIFIED when
separated from CLASSIFIED attachment

CONFIDENTIAL
CLASSIFICATION MARKINGS FOR TRAINING PURPOSES ONLY

Figure 4-9. Sample of Marking a Document Where the Cover Memo is Unclassified but the Attachments are Classified

Sample of Restricted Data (RD) and Formerly Restricted Data (FRD) with Warning Notice

CLASSIFICATION MARKINGS FOR TRAINING PURPOSES ONLY
SECRET
SUBJECT: Sample of Restricted Data (RD) and Formerly Restricted Data (FRD) with Warning Notice (U)

1. (U) Restricted Data (RD) is 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 will not include data declassified or removed from the Restricted Data category under section 142 of the Atomic Energy Act of 1954, as amended. Formerly Restricted Data (FRD) is 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, this information is treated in the same manner as Restricted Data.

2. (S-RD) Documents containing RD information are portion marked in the same manner as other classified documents. Paragraphs containing RD are further indicated by the additional abbreviation of "RD" following the collateral level, as shown at the beginning of this paragraph.

3. (C-FRD) A document containing RD also has the warning notice shown below. When documents contain both RD and FRD, the RD warning notice takes precedence and the FRD notice is omitted.

4. (S) Do not include downgrading or declassification instructions on a document containing RD or FRD. These documents are exempt from predetermined downgrading or declassification action. The DOD does not originate RD or FRD, therefore, all documents should reflect the "Derived from" byline.

Derived from: DOE CG-W5

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

SECRET
CLASSIFICATION MARKINGS FOR TRAINING PURPOSES ONLY

Figure 4-10. Sample of Marking a Document Where the Cover Memo is Unclassified but the Attachments are Classified

Sample of Marking Foreign Government Information

CLASSIFICATION MARKINGS FOR TRAINING PURPOSES ONLY
SECRET

SUBJECT: Sample of Marking Foreign Government Information (FGI)(U)

1. (U) The U.S. Government affords protection to information provided by foreign governments. Care must be taken to identify the source of the information.

2. (FGI-C) Mark the portions that contain the foreign government information to indicate the country of origin and the classification level. Substitute the words "Foreign Government Information" or "FGI" where the identity of the specific government must be concealed. The identity of the concealed foreign source in this example must be maintained with the record copy and adequately protected.

3. (UK-S) This paragraph contains information marked "Secret" by the government of the United Kingdom. The "Derived From" citation should cite the title of the document provided. Declassification date, event, or exemption category is carried forward, if known.

Derived From: FGI Source Document or
identify the foreign government
source document dated *(fill in the date)*
Declassify On: X5, FGI

SECRET
CLASSIFICATION MARKINGS FOR TRAINING PURPOSES ONLY

Figure 4-11. Sample of Marking Foreign Government Information

Sample of Marking Working Papers

CLASSIFICATION MARKINGS FOR TRAINING PURPOSES ONLY
CONFIDENTIAL
WORKING PAPERS
Created: 1 April 1999

Subject: Sample of Marking Working Papers (U)

1. (C) This page is UNCLASSIFIED and is marked CONFIDENTIAL for training purposes only. IMPORTANT: *You must be an Original Classification Authority to originally classify a document.* Working papers are documents and material accumulated or created in the preparation of finished documents and material. Working papers containing classified information will be: Dated when created; conspicuously marked as "Working Papers" or "DRAFT" on the first page of the document in letters larger than the text; marked with the highest classification of any information contained in the material; protected in accordance with the assigned classification; destroyed when no longer needed; and accounted for, controlled, and marked in the manner prescribed for a finished document of the same classification. See paragraph 6-24, of this regulation for further information. This sample memo only pertains to those relatively few cases in which an OCA is generating a document that the OCA is originally classifying and is considered "Working Papers" until completed.

2. (C) In this example, the OCA is an official that has been delegated Original Classification Authority for a particular intelligence program. The OCA has selected reason 1.5(e) (scientific, technological, or economic matters relating to the national security). Instead of a date or event for declassification within 10 years, the OCA has authorized exemption category X8 (Violate a statute, treaty, or international agreement) for protection beyond 10 years.

Y.I. Never
Director, Security Awareness

Classified by: BG I. Didit, Chief of Intelligence Programs, Army Security Command
Reason: 1.5(c)
Declassify on: X8
Date of source: 26 March 1999
WORKING PAPERS
CONFIDENTIAL
CLASSIFICATION MARKINGS FOR TRAINING PURPOSES ONLY

Figure 4-12. Sample of Marking Working Papers

Equivalent Foreign Security Classification

This is a direct reprint from DODD 5200.1-R.

COUNTRY	TOP SECRET	SECRET	CONFIDENTIAL	OTHER
Albania	TEPER SEKRET	SEKRET	IMIREBESUESHEM	I KUFIZUAR
Argentina	ESTRICTAMENTE SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
Australia	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Austria	STRENG GEHEIM	GEHEIM	VERSCHLUSS	
Balkans	STROGO POVERLJIVO State SECRET DRZAVA TAJNA	TAJNO Military SECRET VOJNA TAJNA	POVERLJIVO	
Belgium (French)	TRES SECRET	SECRET	CONFIDENTIEL	DIFFUSION RESTREINTS
(Flemish)	ZEER GEHEIM	GEHEIM	VERTROUWELIJK	BEPERTKE VERSPREIDING
Bolivia	SUPERSECRETO or MUY SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
Brazil	ULTRA SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
Bulgaria	STROGO SEKRENTO SEKRETNO	SEKRETEN or POVERITELNO NEPOZVOLEN (Illicit) ZABRANEN (Forbidden)	POVERITELEN or (as in Limited)	OGRANICHE

Figure 4-13. Equivalent Foreign Security Classification

COUNTRY	TOP SECRET	SECRET	CONFIDENTIAL	OTHER
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	
Croatia	NAJVECI TAJNITAJNI	TAJNI	POVERLJIV	OGRANCIEN
Denmark	YDERST HEMMELIGT	HEMMELIGTFORTROLIGT	TIL TJENESTEBRUG	
Ecuador	SECRETISIMO	SECRETO	CONFIDENCIAL	RESERVADO
El Salvador	ULTRA SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
Ethiopia	YEMIÀZ BIRTOU MISTIR	MISTIR	KILKIL	
Finland	ERITTAIN SALAINEN			
France	TRES SECRET	SECRET DEFENSE	CONFIDENTIEL DIFFUSION RESTREINTE	
Germany	STRENG GEHEIM	GEHEIM	VS-VERTRAULICH	
Greece	AKRWS APORRHTON	APORRHTON CRHSEWS	EMPISTEUTIKON	PERIWRISMENHS

Figure 4-13. Equivalent Foreign Security Classification—Continued

COUNTRY	TOP SECRET	SECRET	CONFIDENTIAL	OTHER
Guatemala	ALTO SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
Haiti	SECRET	CONFIDENTIAL		
Honduras	SUPER SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
Hong Kong	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Hungary	SZIGOR'UAN TITKOS	TITKOS	BIZALMAS	
Iceland	ALGJORTI	TRUNADARMAL		
India	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Indonesia	SANGAT RAHASIA	RAHASIA	TERBATAS	
Iran	BENKOLI SERRI	SERRI	KHEILI MAHRAMANEH	MAHRAMANEH
Iraq (English Translation)	ABSOLUTELY SECRET	SECRET	LIMITED	
Ireland (Gaelic)	AN-SICREIDEACH	SICREIDEACH	RUNDA	SRIANTA
Israel	SODI BEYOTER	SODI	SHAMUR	MUGBAL
Italy	SEGRETISSIMO	SEGRETO	RISERVATISSIMO	RISERVATO
Japan	KIMITSU	GOKUHI	HI	TORIATSUKAICHUI
Jordan	MAKTUM JIDDAN	MAKTUM	SIRRI MAHDUD	
Kazakstan	*USE RUSSIAN EQUIVALENT*			

Figure 4-13. Equivalent Foreign Security Classification—Continued

COUNTRY	TOP SECRET	SECRET	CONFIDENTIAL	OTHER
Korea	‖ KUP PI MIL	‖ ‖ KUP PI MIL	‖ ‖ ‖ KUP PI MIL	
Kyrgystan	*USE RUSSIAN EQUIVALENT*			
Laos	TRES SECRET	SECRET	SECRET/CONFIDENTIEL	DIFFUSION RESTREINTE
Lebanon	TRES SECRET	SECRET	CONFIDENTIEL	
Moldavian	ULTRASECRET *(May also use Russian Equivalent)*	SECRET	CONFIDENTIAL OR SECRET	RETRINS
Mexico	ALTO SECRETO	SECRETO	CONFIDENCIAL	RESTRINGIDO
Netherlands	ZEER GEHEIM	GEHEIM	CONFIDENTIEEL or VERTROUWELIJK	DIENSTGEHEIM
New Zealand	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Nicaragua	ALTO SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
Norway	STRENGT HEMMELIG	HEMMELIG	KONFIDENSIELL	BEGRENSET
Pakistan	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Paraguay	SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
Peru	ESTRICTAMENTE SECRETO	SECRETO	CONFIDENCIAL	RESERVADO

Figure 4-13. Equivalent Foreign Security Classification—Continued

COUNTRY	TOP SECRET	SECRET	CONFIDENTIAL	OTHER
Philippines	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Poland	TAIJNY SPECJALNEGO	TAHJY	POUFNY	
Portugal	MUITO SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
Romania	ULTRASECRET	SECRET	CONFIDENTIAL or SECRET	RESTRINS
Russian	COBEOWEHHO	CEKPETHO		
Saudi Arabia	SAUDI TOP SECRET	SAUDI VERY SECRET	SAUDI SECRET	SAUDI SECRET
Spain	MEXIMO SECRETO	SECRETO	CONFIDENCIAL	DIFFUSION LIMITADA
Sweden (Red Borders)	HEMLIG	HEMLIG		
Switzerland *(Three languages. TOP SECRET has a registration number to distinguish it from SECRET and CONFIDENTIAL)*				
French	TRES SECRET	SECRET DEFENSE	CONFIDENTIEL DEFENSE	DIFFUSION RESTREINTE
German	STRENG GEHEIM	GEHEIM	VERTRAULICH	
Italian	SEGRETISSIMO	SEGRETO	RISERVATISSIMO	RESERVATO
Taiwan	*(No translation in English characters)*			
Tajikstan	*USE RUSSIAN EQUIVALENT*			

Figure 4-13. Equivalent Foreign Security Classification—Continued

COUNTRY	TOP SECRET	SECRET	CONFIDENTIAL	OTHER
Thailand	LUP TISUD	LUP MAAG	LUP	POK PID
Turkey	COK GIZLI	GIZLI	OZEL	HIZMET OZEL
Turkmenistan	*USE RUSSIAN EQUIVALENT*			
Ukraine	TSILKOM SEKRETNE	SEKRETNO	KONFIDENTSIAL'NO	DYLA
Union of South Africa	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Afrikaans	UITERS GEHEIM	GEHEIM	VERTROULIK	BEPERK
Unit Arab Republic (Egypt)	TOP SECRET	VERY SECRET	SECRET	OFFICIAL
United Kingdom	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Uruguay	ULTRA SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
Uzbekistan	*USE RUSSIAN EQUIVALENT*			
Viet Nam	TRES SECRET	SECRET DEFENSE	CONFIDENTIEL	DIFFUSION
(French)		DEFENSE	RESTREINTE	
(Vietnamese)	TOI-MAT	MAT	KIN	TU MAT

NOTE: The classifications given above represent the nearest comparable designation that are used to signify degrees of protection and control similar to those prescribed for the equivalent U.S. classification.

Figure 4-13. Equivalent Foreign Security Classification—Continued

Chapter 5
Controlled Unclassified Information

Section I
For Official Use Only Information

5–1. General

a. The requirements of the information security program apply only to information that requires protection in order to prevent damage to the national security and has been classified in accordance with EO 12958 or its predecessors. There are other types of information that require application of controls and protective measures for a variety of reasons. In accordance with DODD 5200.1–R this information is known as Controlled Unclassified Information (CUI). Since classified information and CUI exist side by side in the work environment, often in the same documents, this chapter is provided as an attempt to avoid confusion and promote proper handling. It covers several types of CUI, and provides basic information about the nature of this information and the procedures for identifying and controlling it. In some cases, the chapter refers to other DOD directives that provide more detailed guidance.

b. The types of information covered in this chapter include "For Official Use Only" information, "Sensitive But Unclassified" (formerly "Limited Official Use") information, "DEA Sensitive Information," "DOD Controlled Unclassified Nuclear Information," "Sensitive Information" as defined in the Computer Security Act of 1987, and information contained in technical documents.

5–2. Description

a. For Official Use Only (FOUO) is a designation that is applied to unclassified information which is exempt from mandatory release to the public under the Freedom of Information Act (FOIA) (see AR 25–55 for more details). The FOIA specifies nine categories of information which can be withheld from release if requested by a member of the public. They are:

(1) Information which is currently and properly classified.

(2) Information which pertains solely to the internal rules and practices of the agency. This exemption has two profiles, "high" and "low." The "high" profile permits withholding of a document which, if released, would allow circumvention of an agency rule, policy, or statute, thereby impeding the agency in the conduct of its mission. The "low" profile permits withholding, if there is no public interest in the document, and it would be an administrative burden to process the request.

(3) Information specifically exempted by a statute establishing particular criteria for withholding. The language of the statute must clearly state that the information will not be disclosed.

(4) Information, such as trade secrets and commercial or financial information obtained from a company on a privileged or confidential basis, which, if released, would result in competitive harm to the company, impair the government's ability to obtain like information in the future, or protect the government's interest in compliance with program effectiveness.

(5) Intra–agency memoranda which are deliberative in nature; this exemption is appropriate for internal documents which are part of the decision making process and contain subjective evaluations, opinions and recommendations.

(6) Information, the release of which could reasonably be expected to constitute a clearly unwarranted invasion of the personal privacy of individuals.

(7) Records or information compiled for law enforcement purposes that:

(a) Could reasonably be expected to interfere with law enforcement proceedings.

(b) Would deprive a person of a right to a fair trial or impartial adjudication.

(c) Could reasonably be expected to constitute an unwarranted invasion of personal privacy of others.

(d) Disclose the identity of a confidential source.

(e) Disclose investigative techniques and procedures.

(f) Could reasonably be expected to endanger the life or physical safety of any individual.

(8) Certain records of agencies responsible for supervision of financial institutions.

(9) Geological and geophysical information concerning wells.

b. Information which is currently and properly classified can be withheld from mandatory release under the first exemption category (subparagraph (1) above). FOUO is applied to information which is exempt under one of the other eight categories (subparagraphs (2) through (9) above). So, by definition, information must be unclassified in order to be designated FOUO. If an item of information is declassified, it can be designated FOUO if it qualifies under one of those other eight categories. This means that:

(1) Information cannot be classified and FOUO at the same time; and

(2) Information which is declassified can be designated FOUO, but only if it fits into one of the last eight exemption categories (categories (2) through (9) above).

c. The FOIA provides that, for information to be exempt from mandatory release, it must fit into one of the qualifying categories and there must be a legitimate government purpose served by withholding it. Simply because information is marked FOUO does not mean it automatically qualifies for exemption. If a request for a record is received, the information must be reviewed to see if it meets this dual test. On the other hand, the absence of the FOUO marking does not automatically mean the information must be released. Some types of records (for example, personnel records) are not normally marked FOUO, but can still qualify for withholding under the FOIA. Only personnel officially appointed as a Release Authority can release Army information.

5–3. Marking

a. Information which has been determined to qualify for FOUO status should be indicated, by markings, when included in documents and similar material. Markings should be applied at the time documents are drafted, whenever possible, to promote proper protection of the information.

b. Wholly unclassified documents and material containing FOUO information will be marked as follows:

(1) Documents will be marked "FOR OFFICIAL USE ONLY," in letters larger than the rest of the text, where practical, at the bottom of the front cover (if there is one), the title page (if there is one), the first page, and the outside of the back cover (if there is one).

(2) Pages of the document which contain FOUO information will be marked "FOR OFFICIAL USE ONLY" at the bottom.

(3) Material other than paper documents, for example, slides, computer media, films, etc., will bear markings which alert the holder or viewer that the material contains FOUO information.

(4) FOUO documents and material, transmitted outside the Department of Defense, must bear an expanded marking on the face of the document so that non–DOD holders understand the status of the information. A statement similar to this one should be used: This document contains information Exempt from mandatory disclosure under the FOIA. Exemption(s) (indicate the exemption(s)) apply.

c. Classified documents and material containing FOUO information will be marked as required by chapter 4 of this regulation, with FOUO information identified as follows:

(1) Overall markings on the document will follow the procedures in chapter 4. No special markings are required on the face of the document because it contains FOUO information.

(2) Portions of the document will be marked with their classification as required by chapter 4. If there are unclassified portions which contain FOUO information, they can be marked with "FOUO" in parentheses at the beginning of the portion. Since FOUO information is, by definition, unclassified, the "FOUO" is an acceptable substitute for the normal "U."

(3) Pages of the document which contain classified information will be marked as required by chapter 4 of this regulation. Pages which contain FOUO information but no classified information will be marked "FOR OFFICIAL USE ONLY" at the top and bottom.

d. Transmittal documents which have no classified material attached, but do have FOUO attachments, will be marked with a statement similar to this one: "FOR OFFICIAL USE ONLY ATTACHMENT."

e. Each part of electronically transmitted messages containing FOUO information will be marked appropriately. Unclassified messages containing FOUO information will contain the abbreviation "FOUO" before the beginning of the text.

5–4. Access to FOUO information

FOUO information can be disseminated within DOD components and between officials of Army components and Army contractors, consultants, and grantees, as necessary, in the conduct of official business. FOUO information can also be released to officials in other departments and agencies of the Executive and Judicial Branches in performance of a valid government function. Special restrictions can apply to information covered by the Privacy Act. Release of FOUO information to members of Congress is covered by DODD 5400.4, and to the General Accounting Office by DODD 7650.1.

5–5. Protection of FOUO information

a. During working hours, reasonable steps should be taken to minimize risk of access by unauthorized personnel. After working hours, FOUO information can be stored in unlocked containers, desks or cabinets if U.S. Government or U.S. Government–contract building security is provided, or in locked desks, file cabinets, bookcases, or similar items.

b. FOUO documents and material can be transmitted via first class mail, parcel post, or, for bulk shipments, fourth class mail. Electronic transmission of FOUO information by voice, data, facsimile or similar means, should be by approved secure communications systems whenever possible.

c. Record copies of FOUO documents will be disposed of in accordance with AR 25–400–2. Non–record FOUO documents can be destroyed by shredding or tearing into pieces and discarding the pieces in regular trash containers.

5–6. Further guidance
Further guidance on safeguarding personal information is contained in DOD 5400.11–R.

Section II
Sensitive But Unclassified and Limited Official Use Information

5–7. Description
Sensitive But Unclassified (SBU) information is information originated within the Department of State which warrants a degree of protection and administrative control and meets the criteria for exemption from mandatory public disclosure under the Freedom of Information Act. Prior to 26 January 1995, this information was designated and marked Limited Official Use (LOU). The LOU designation will no longer be used.

5–8. Marking
The Department of State does not require that SBU information be specifically marked, but does require that holders be made aware of the need for controls. When SBU information is included in DOD documents, the documents will be marked as if the information were FOUO. There is no requirement to remark existing material containing LOU information.

5–9. Access to SBU information
Within the Department of the Army, the criteria for allowing access to SBU information are the same as those required for FOUO information (see paragraph 5–4).

5–10. Protection of SBU information
Within the Department of the Army, SBU information will be afforded the same protection as that required for FOUO information (see paragraph 5–5).

Section III
Drug Enforcement Administration Sensitive Information

5–11. Description
Drug Enforcement Administration (DEA) sensitive information is unclassified information which is originated by DEA and requires protection against unauthorized disclosure in order to protect sources and methods of investigative activity, evidence, and the integrity of pretrial investigative reports. The administrator, and certain other officials, of the DEA have been authorized to designate information as "DEA SENSITIVE". The Department of Defense has agreed to implement protective measures for the following DEA sensitive information in its possession.

a. Information and material that is investigative in nature.

b. Information and material to which access is restricted by law.

c. Information and material which is critical to the operation and mission of the DEA.

d. Information and material in which the disclosure of such would violate a privileged relationship.

5–12. Marking
a. Unclassified documents containing DEA sensitive information will be marked "DEA SENSITIVE," in letters larger than the rest of the text, where practical, at the top and bottom of the front cover (if there is one), the title page (if there is one), and the outside of the back cover (if there is one).

b. In unclassified documents, each page containing DEA sensitive information will be marked "DEA SENSITIVE" top and bottom. Classified documents containing DEA sensitive information will be marked as required by chapter 4, except that pages containing DEA sensitive information, but no classified information, will be marked "DEA SENSITIVE" top and bottom.

c. Portions of DA documents which contain DEA sensitive information will be marked "(DEA)" at the beginning of the portion. This applies to classified, as well as unclassified documents. If a portion of a classified document contains both classified and DEA sensitive information, the "DEA" marking will be included along with the parenthetical classification marking. For example, a document containing DEA sensitive information along with SECRET information will be marked "(S)(DEA)."

5–13. Access to DEA sensitive information
Access to DEA sensitive information will be granted only to persons who have a valid need–to–know for the

information. A security clearance is not required. DEA sensitive information in the possession of the Department of Defense, cannot be released outside the DOD without prior authorization by the DEA.

5–14. Protection of DEA sensitive information

a. DEA sensitive material can be transmitted within Continental U.S. (CONUS) by first class mail. Transmission outside CONUS must be by a means approved for transmission of SECRET material. Non–U.S. Government package delivery and courier services will not be used. The material will be enclosed in two opaque envelopes or containers, the inner one marked "DEA SENSITIVE" on both sides. Electronic transmission of DEA sensitive information within CONUS should be over secure communications circuits whenever possible; transmission outside CONUS must be over approved secure communications circuits.

b. Reproduction of DEA sensitive information and material will be limited to that required for operational needs.

c. DEA sensitive material will be destroyed by a means approved for the destruction of CONFIDENTIAL material.

Section IV
DOD Unclassified Controlled Nuclear Information

5–15. Description

DOD Unclassified Controlled Nuclear Information (UCNI) is unclassified information on security measures, including security plans, procedures, and equipment, for the physical protection of DOD Special Nuclear Material (SNM), equipment, and facilities. Information is designated DOD UCNI only when it is determined that its unauthorized disclosure could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security, by increasing significantly, the likelihood of the illegal production of nuclear weapons or the theft, diversion, or sabotage of DOD SNM, equipment, or facilities. Information can be designated DOD UCNI by the SECARMY and individuals to whom they have delegated the authority.

5–16. Marking

a. Unclassified documents and material containing DOD UCNI will be marked as follows:

(1) The face of the document and the outside of the back cover, if there is one, will be marked "DOD CONTROLLED UNCLASSIFIED NUCLEAR INFORMATION" in letters larger than the rest of the text, where practical.

(2) Portions of the document which contain DOD UCNI will be marked with "(DOD UCNI)" at the beginning of the portion.

b. Classified documents and material containing DOD UCNI will be marked in accordance with chapter 4, except that:

(1) Pages with no classified information but containing DOD UCNI will be marked "DOD CONTROLLED UNCLASSIFIED NUCLEAR INFORMATION" at the top and bottom.

(2) Portions of the document which contain DOD UCNI will be marked with "(DOD UCNI)" at the beginning of the portion in addition to the classified marking, where appropriate.

c. Material other than paper documents, for example, slides computer media, films, etc., will bear markings which alert the holder or viewer that the material contains DOD UCNI.

d. Documents and material containing DOD UCNI and transmitted outside the Department of Defense must bear an expanded marking on the face of the document so that non–DOD holders understand the status of the information. The following statement will be used: Department of Defense — Controlled Unclassified Nuclear — Information exempt from mandatory disclosure (5 USC 552(b)(3), as authorized by 10 USC 128)

e. Transmittal documents which have DOD UCNI attachments will bear a statement: The attached document contains DOD Unclassified — Controlled Nuclear Information (DOD UCNI).

5–17. Access to DOD UCNI

Access to DOD UCNI will be granted only to persons who have a valid need–to–know for the information and are specifically eligible for access under the provisions of DODD 5210.83.

5–18. Protection of DOD UCNI

a. During working hours, reasonable steps should be taken to minimize risk of access by unauthorized personnel. After working hours, DOD UCNI can be stored in unlocked containers, desks or cabinets if U.S. Government or U.S. Government–contract building security is provided, or in locked buildings, rooms, desks, file cabinets, bookcases, or similar items.

b. DOD UCNI can be transmitted by first class mail in a single, opaque envelope or wrapping. Except in emergencies, electronic transmission of DOD UCNI will be over approved secure communications circuits.

c. Record copies of DOD UCNI documents will be disposed of in accordance with the Federal Records Act (44

USC 33) and component records management directives. Non–record DOD UCNI documents can be destroyed by shredding or tearing into pieces and discarding the pieces in regular trash containers.

Section V
Sensitive Information (Computer Security Act of 1987)

5–19. Description

a. The Computer Security Act of 1987 established requirements for protection of certain information in federal government Automated Information Systems (AIS). This information is referred to as "sensitive" information, defined in the Act as: "Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, USC (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy."

b. Two aspects of this definition deserve attention. First, the Computer Security Act of 1987 applies only to unclassified information which deserves protection. Second, unlike most other programs for protection of information, the Computer Security Act of 1987 is concerned with protecting the availability and integrity, as well as, the confidentiality of information. Much of the information which fits the Computer Security Act of 1987's definition of "sensitive" falls within the other categories of information discussed in this chapter.

5–20. Marking

There is no specific marking authorized for the designation of "sensitive" information. If the information fits within one of the other categories of information described in this chapter, the appropriate marking requirements apply.

5–21. Access to sensitive information

If sensitive information falls within one of the other categories of information described in this chapter, the specific limitations on access for the appropriate category will be applied. If it does not, access to the information will be limited only to those with a valid need for such access in order to perform a legitimate organizational function, as dictated by common sense principles of security management, learned through a proper and thorough security education program.

5–22. Protection of sensitive information

Information on a DA AIS, which is determined to be "sensitive," within the meaning of the Computer Security Act of 1987, will be provided protection which is:

a. Determined after thorough consideration of the value and sensitivity of the information and the probable adverse impact of loss of its availability, integrity or confidentiality.

b. In compliance with applicable DA policy and requirements for security of information within automated systems.

c. Commensurate with the degree of protection required for the category of information described in this chapter to which it belongs (if any).

d. Based on sound application of risk management techniques and procedures.

5–23. Further guidance

Further guidance is found in appendix E of this regulation, AR 380–19, DODD 5200.28, and other related publications.

5–24. Technical documents

DODD 5230.24 and AR 70–11 require distribution statements to be placed on technical documents no matter if they are classified or unclassified (See figure 5–1). These statements facilitate control, distribution and release of these documents without the need to repeatedly refer questions to the originating activity. The originating office can, of course, make case–by–case exceptions to distribution limitations imposed by the statements.

Distribution Statements for Technical Documents

Distribution Statement A
Approved for public release; distribution is unlimited.

Distribution Statement B
Distribution authorized to U.S. Government Agencies only; *[reason]*; *[date]*.
Other requests for this document will be referred to *[controlling DOD office]*.

Distribution Statement C
Distribution authorized to U.S. Government Agencies and their contractors; *[reason]*; *[date]*.
Other requests for this document will be referred to *[controlling DOD office]*.

Distribution Statement D
Distribution authorized to the DoD and U.S. DoD contractors only; *[reason]*; *[date]*.
Other requests for this document will be referred to The*[controlling DOD office]*.

Distribution Statement E
Distribution authorized to DoD Components only; *[reason]*; *[date]*
Other requests for this document will be referred to The*[controlling DOD office]*.

Distribution Statement F
Further distribution only as directed by *[controlling DOD office]* or higher DoD authority; *[date]*

Distribution Statement X
Distribution authorized to U.S. Government Agencies and private individuals or enterprises eligible to obtain export-controlled technical data in accordance with DoD Directive 5230.24; *[date]*.
Controlling DoD office is *[controlling DOD office]*.

Figure 5-1. Distribution Statements for Technical Documents

Chapter 6
Access, Control, Safeguarding, and Visits

Section I
Access

6–1. Responsibilities

DA personnel are responsible, both personally and officially, for safeguarding classified information for which they have access. This responsibility includes ensuring they do not permit access, to sensitive or classified information, by unauthorized personnel. Any person who does not have a need–to–know and who is not cleared or granted access to information at that level, in accordance with the policy established in AR 380–67, is considered unauthorized personnel. Both the clearance/access authorization and the need–to–know must be present before access is authorized. The holder of the information, not the potential recipient, must confirm valid need–to–know and must verify the level of security clearance or access authorization. This responsibility, of preventing access by unauthorized personnel, pertains to any means of access, including auditory and visual means. Care will be exercised to make sure that classified conversations are not made within hearing distance of unauthorized personnel. Collecting, obtaining, recording, or removing, for any personal use whatsoever, of any material or information classified in the interest of national security, is prohibited.

6–2. Nondisclosure Agreement

a. Prior to granting access to classified information, DA personnel will receive a briefing outlining their responsibility to protect classified information and will sign the SF 312 (Classified Information Nondisclosure Agreement (NDA)). Cleared personnel who have signed an earlier nondisclosure agreement, the SF 189 (Classified Information Nondisclosure Agreement) (replaced by SF 312), and have not already signed the SF 312, do not need to sign the SF 312. They may, however, elect to replace the old SF 189 with a newly signed SF 312. National policy requires that SF 312 and SF 189 NDAs be retained for 50 years from the date of signature. Execution of the NDA is mandatory for all personnel as a condition of access to classified information. It will be signed once unless verification of previous execution of the form indicates that the form cannot be located, in which case the form will be signed again and filed as if it were an original. In order to preclude duplicate NDAs, reasonable effort will be made to verify an existing NDA prior to asking for a second form to be signed. The purpose of the NDA is to make sure that personnel requiring access to classified information are advised of their responsibility to protect that classified information.

b. Contractor personnel will execute the NDA through their company and not through the sponsoring DA command. Non–U.S. Government personnel, who have been hired under Civil Service procedures as consultants to the Department of the Army, and granted a DA security clearance or access authorization, in accordance with AR 380–67, will follow the same procedure, for execution of the SF 312, as civilian personnel. When in exceptional situations in which access to specific classified information is approved for uncleared non–government personnel, under the provisions of AR 380–67, the execution of the NDA will follow the same policy as stated for civilian personnel, as amended.

6–3. Signing and filing the NDA

The command will have proof of clearance prior to execution of the NDA. Proof of security clearance will be the receipt of the completed DA Form 873 (Certificate of Clearance and/or Security Determination). Other means of verifying the clearance can come from the Department of the Army Central Clearance Facility (CCF), a review of individual's personnel file and verification that it contains the DA Form 873, or the issuance of an interim security clearance. Upon proof of clearance, a command official, typically the command security manager, will brief the individual on the responsibilities to protect classified information. After verification from a picture identification card, the individual will read, date, and sign the NDA. The command official will witness the execution of the NDA by signing and dating the form immediately after the individual's signature. The same official, or another official in the command, that witnesses the form, can serve as the accepting official.

a. Civilian Personnel.

(1) *Intelligence Related Position:*

Copies of nondisclosure agreements, such as SF 312 or SF 189 or similar forms, signed by civilian personnel, including employees of contractors, licensees, or grantees, with access to information that is classified under standards put forth by Executive Orders governing security classification, fall into this category. These forms should be maintained separately from personnel security clearance files. Agreements for civilian employees working for elements of the intelligence community must be maintained separately from the official personnel folder. These forms, that are maintained separately from the individual's official personnel folder, will be destroyed when 70 years old.

(2) *All Others.* The accepting official will forward the original NDA to the supporting local or regional Civilian

Personnel Office (CPO), to be filed in the individual's Official Personnel File (OPF). The form will be filed on the permanent side of the OPF as an adjunct to the DA Form 873. NDAs for civilian employees transferring from one duty station to another, to include transferring to another U.S. Government agency, will transfer as part of their OPF. The NDA will not be removed from the OPF. If a command receives an NDA executed by a current employee while that employee was assigned to another command or agency, the command official receiving the form will forward the NDA to the applicable local or regional supporting CPO for insertion into the OPF as an adjunct to the DA Form 873. When a civilian employee transfers from one duty station to another, the designated command civilian personnel official will ensure that the Standard Form 75 (Request for Preliminary Employment Data) verifies that a completed NDA is on file. These forms, that are maintained in the individual's official personnel folder, will apply the disposition instructions for the official personnel folder.

b. Military Personnel. For military personnel, a copy of the NDA will be kept on file by the command security manager, or other designated command official, for verification that the individual has executed the NDA. Copies of nondisclosure agreements, such as SF 312 or SF 189 or similar forms, signed by military personnel, with access to information that is classified under standards put forth by Executive Orders governing security classification, should be maintained separately from personnel security clearance files. This copy will remain in the command file until the individual transfers or is separated from the U.S. Army. Upon the soldier's arrival at the new duty station, the command security manager will maintain a copy of the original, newly signed NDA on file pending the next transfer. The accepting official will forward the original NDA to the address below, where it will be converted to microfiche and filed with the soldier's official records. Upon notification of transfer, the command security manager, or other designated command official, will send the copy of the NDA to the gaining organization's command security manager either by mail or in the possession of the transferring individual.

(1) Active Army Commissioned and Warrant Officers: Commander, U.S. Total Army Personnel Command, ATTN: TAPC–MSR Alexandria, VA 22332–0400.

(2) Active Army Enlisted Personnel: Commander, U.S. Army Enlisted Records and Evaluation Center, ATTN: PCRE–FS, 8899 East 56th Street, Fort Benjamin Harrison, IN 46249–5301.

(3) Reservists: Commander, U.S. Army Reserve Personnel Center, ATTN: DARP–PRD–MP, 9700 Page Avenue, St. Louis, MO 63132–5200. When a cleared Individual Ready Reserve (IRR) member is ordered to active duty for training that will involve access to classified information and previous execution of the NDA cannot be verified, an NDA will be completed at the training site and the original forwarded to the U.S. Army Reserve Personnel Center.

(4) National Guard Commissioned and Warrant Officers: Army National Guard Personnel Division, ATTN: NGB–ARD–C, 111 South George Mason Drive, Arlington, VA 22204–1382.

(5) For National Guard enlisted soldiers: Forward to the soldier's State Adjutant General, ATTN: POMSO.

c. Department of the Army Consultants and Other Non–U.S. Government Personnel. If a consultant to the Department of the Army is hired under Civil Service procedures, as opposed to contracting with a company for consultant services, the NDA will be executed and filed with the DA Form 873. If the consultant's OPF is not retired, the command is obligated to retain the NDA for the required 50–year retention period. Consultant NDAs cannot be used by or transferred to another activity. They only authorize access to classified information under a specific agreement and an access termination form must be executed when the agreement has ceased or when classified access is no longer required, whichever occurs first. In special situations where non–U.S. Government uncleared personnel have been granted classified access to specific information in accordance with the policy established in AR 380–67, the NDA will be attached to the exception to policy memorandum or other appropriate written authorization which authorized the individual's access to classified information and will be retained in the command's files for 50 years.

6–4. Refusal to execute the NDA

If a person refuses to sign the NDA, the individual will be advised of the applicable portions of the NDA, SF 312. The individual will be given five calendar days to reconsider and will not be permitted access to classified information during that time. At the end of the five–day period, the individual will again be requested to sign the NDA. If at that point the individual still refuses to sign the NDA, their classified access, if it had been previously granted, will be formally suspended, the individual will not be permitted any access to classified information, the Department of the Army's Central Clearance Facility will be notified concerning clearance revocation or denial action, and the matter will be reported as required by AR 380–67.

6–5. Debriefing and termination of classified access

a. Classified information is not the personal possession of any DA personnel, regardless of rank, title, or position. Classified information will not be removed to nonofficial or unapproved locations, such as personal residences, upon the termination of employment or military service of any person, including the custodian of that material.

b. All DA personnel who are retiring, resigning, being discharged, or will no longer have access to classified information, will out–process through the command security manager's office or other designated command office. During this out–processing the individual will be informed that security clearance and access to classified information has terminated and that the individual still has an obligation to protect any knowledge they have of classified information. DA personnel will sign a debriefing statement during out–processing. The debriefing statement will either

be the NDA Security Debriefing Acknowledgement section of the SF 312, or DA Form 2962 (Security Termination Statement). The debriefing, as a minimum, will consist of informing the individual of the continuing obligation to protect classified information accessed, the admonition that discussion or other revelation of classified information to unauthorized persons is prohibited, provide instructions for reporting any unauthorized attempt to gain access to classified information, advise the individual of the prohibition against retaining classified material when leaving the command, and remind the individual of the potential civil and criminal penalties for failure to fulfill these continuing responsibilities. The same procedures will be followed for DA personnel still employed and still in service whose security clearance has been withdrawn, denied (after interim access was granted), or revoked either for cause or for administrative reasons due to lack of need for future access to classified information. In these cases both civilian and military DA personnel will execute the debriefing statement.

c. Unless exempted by the senior security official at the MACOM, security out–processing is required for all cleared personnel transferring to another DA command or to a Federal Government agency. Transfers will not require the execution of the type of debriefing statement described in subparagraph b, above. This does not preclude the command from requesting the transferring individual sign or initial a form or statement indicating, in substance, that the individual has been advised of the continuing responsibility to protect classified information and/or has completed the security out–processing. Personnel transferring will be briefed on the responsibilities stated in subparagraph b, above. Additionally, personnel transferring will be advised that classified information previously created, or in the custody of, the individual, including that gained while attending training or conferences, does not belong to the individual and does not transfer to the gaining command without appropriate approval by both the gaining and losing commands. Such approval will be based upon the losing command's assessment of the need–to–know for the information by the gaining command. Out–processing can also be used as a means to ensure that the appropriate command security officials are aware of the departure of personnel to ensure combinations and passwords are changed, keys are returned, accountable documents and property are under new custody, etc. Where out–processing is not required for transfers, the command will establish procedures to ensure that the command security manager is advised of such transfers.

d. For all DA military personnel, retiring, resigning, or separating from military service, the DA Form 2962, or the termination portion of the NDA, will be executed and maintained on file by the command security manager, or other designated command official, at the soldier's last duty station, for a period of two years, in accordance with AR 25–400–2.

e. All Army civilian personnel who are retiring or resigning from government service, must out–process through the activity's security office. The security official will debrief the civilian employee about the continuing obligation to protect the classified information accessed during government service. The civilian employee should sign a DA Form 2962 or the NDA Debriefing Acknowledgement, which will be retained by the activity. Signing the NDA Debriefing Acknowledgement is the individual's option upon final separation from the government service, however, the individual will be informed that security clearance and access to classified information has terminated and that the individual still has a legal obligation to protect classified information. The original NDA, for civilian employees, who retire or resign from government service, will remain in the employee's OPF and will be retired as part of the OPF. The NDA (SF 189 or SF 312) for civilian employees who retired or resigned prior to 1993 and are currently filed in an inactive file will be forwarded to: National Personnel Records Center, Civilian Personnel Records, 111 Winnebago Street, St. Louis, MO 63118.

f. Refusal to sign the DA Form 2962 or the termination portion of the NDA, SF 312, will be considered a lack of personal commitment to protect classified information. Personnel who refuse to sign a termination statement will not be granted further access to classified information and their security clearance may be revoked or denied in accordance with AR 380–67.

6–6. Communication and cooperation between command officials

Commanders will establish policy and procedures to ensure that other command officials and personnel advise the command security manager of any information affecting an individual's access to classified information. Personnel officials will make sure that transfer and recruitment documents, including vacancy announcements, indicate if a security clearance is required for the position.

6–7. Access to restricted data, formerly restricted data, and critical nuclear weapons design information

a. Access to RD (less CNWDI) and FRD by DA personnel, at Army facilities, will be under the same conditions as for all other classified information, based on the appropriate security clearance and access, need–to–know for the information, and in accordance with DODD 5210.2. See paragraph 6–17 for the requirement for DA certification to access classified information, including RD and FRD, held by Department of Energy (DOE) personnel and for classified visits to DOE certified facilities. Because of the sensitivity of nuclear information, the need–to–know criteria will be strictly enforced for all access to RD and FRD information.

b. Critical Nuclear Weapons Design Information (CNWDI) is a category of SECRET and TOP SECRET restricted data. Access to and dissemination of CNWDI is of particular concern to national security. Access to CNWDI will be limited to U.S. citizens with final TOP SECRET or SECRET, as appropriate to the information being accessed,

security clearance, and will be limited to the minimum number of personnel who require such access to accomplish assigned duties. Access to CNWDI will be limited to personnel whose need–to–know has been justified to, and verified by, an official authorized to sign DOE Form 5631.20 (Request for Visit or Access Approval), or by a representative appointed by that official. Once the need–to–know for CNWDI access has been justified and verified, personnel who have a need for access to CNWDI will be briefed on its sensitivity before access is granted. See paragraph 9–13, for suggested CNWDI briefing. CNWDI access authorizations will be reflected in appropriate security records. Records of CNWDI briefings and access authorizations will be maintained in a manner that will ease verification by certifying officials.

c. Access to CNWDI is strictly limited to U.S. citizens. In rare cases an exception to the U.S. citizenship requirement will be made if a non–U.S. citizen possesses a unique or very unusual talent or skill that is essential to the U.S. Government, and it is not possessed, to a comparable degree, by an available U.S. citizen. In such cases, the determination can be made that it is in the overall best interest of the United States to permit access to CNWDI. This determination will be made by the Secretary of Defense based upon the recommendation of the Secretary of the Army. Such requests will be forwarded through command channels to DAMI–CH.

6–8. Access by persons outside the Executive Branch

Classified information can 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 U.S. Government will derive a benefit or advantage, and that such release is not prohibited by the originating department or agency. MACOM Commanders and the Administrative Assistant to the Secretary of the Army are designated as Department of the Army Release Authorities. They are authorized to determine, subject to OCA approval and before the release of classified information, the propriety of such action in the interest of national security and the assurance of the recipient's trustworthiness and need–to–know. This authority can be further delegated, if required.

a. Congress

(1) Congressional staff members requiring access to DOD classified information will be processed for a security clearance in accordance with DODD 5142.1 and the provisions of AR 380–67. The Director, Washington Headquarters Services (WHS), will initiate the required investigation (initial or reinvestigation) to DIS, adjudicate the results and grant, deny or revoke the security clearance, as appropriate. The Assistant Secretary of Defense (Legislative Affairs) will be notified by WHS of the completed clearance action.

(2) The Assistant Secretary of Defense (Legislative Affairs) as the principal staff assistant to the Secretary of Defense for DOD relations with the members of Congress, will provide for DOD processing of personal security clearances for members of Congressional staffs.

(3) Personnel testifying before a Congressional committee, in executive session, in relation to a classified matter, will obtain the assurance of the committee that individuals present have a security clearance commensurate with the highest classification of information that is to be presented.

b. Government Printing Office (GPO) Documents. Governmentt Printing Office (GPO) Documents and material of all classification may be processed by the GPO, which protects the information in accordance with the DOD/GPO Security Agreement of February 20, 1981.

c. General Accounting Office representative. Representatives of the General Accounting Office (GAO) Representatives of the GAO can be granted access to classified information, originated by and in the possession of the Department of the Army and DOD, when such information is relevant to the performance of the statutory responsibilities of that office, as set forth in DODD 7650.1. Certifications of security clearance, and the basis thereof, will be accomplished pursuant to arrangements between GAO and the concerned command. Personal recognition or presentation of official GAO credential cards are acceptable for identification purposes.

d. Historical Researchers and Former Presidential Appointees (See DODD 5200.1–R, Chapter 6) MACOM commanders, the Administrative Assistant to the Secretary of the Army, and the DCSINT are authorized to execute the provisions of DODD 5200.1–R pertaining to historical researchers and former presidential appointees. This authority cannot be further delegated. Investigative personnel security requirements contained in AR 380–67 will be followed and the NDA must be executed and maintained for the required period of time.

e. Judicial Proceedings DODD 5405.2 governs the release of classified information in litigation.

f. Other Situations When necessary, in the interests of national security, MACOM commanders and the Administrative Assistant to the Secretary of the Army can authorize access by persons outside the federal government, other than those identified above, to classified information. This is accomplished only upon determining that the recipient is trustworthy, as determined by AR 380–67 requirements, for the purpose of accomplishing a national security objective, and that the recipient can and will safeguard the information from unauthorized access. This authority will not be further delegated. Once the approval official has determined need–to–know, and that the recipient can and will safeguard the information from unauthorized disclosure, the provisions of AR 380–67 will be followed, regarding the personnel security investigative requirements to be met, prior to granting access to classified information. The approval authority will ensure that an NDA is executed prior to access and maintained for the required period of time.

Section II
Control Measures and Visits

6–9. Responsibilities for maintaining classified information.

a. Commands will maintain a system of control measures that ensures that access to classified information is limited only to authorized persons. The control measures will be appropriate to the environment in which the access occurs and the nature and volume of the information. The system will include technical, where appropriate, physical, administrative, personal, and personnel control measures.

b. DA personnel granted access to classified information are responsible for protecting classified information of which they have knowledge or that is in their possession or control. DA personnel are personally responsible for taking proper precautions to ensure that unauthorized persons do not gain access to classified information. Classified information will be protected at all times, either by storage in an approved security container, or having it under the personal observation and physical control of an authorized individual.

6–10. Care during working hours

a. Classified material removed from storage will be kept under constant surveillance and control by authorized personnel. Classified document cover sheets, Standard Forms 703 (TOP SECRET Cover Sheet), 704 (SECRET Cover Sheet), and 705 (CONFIDENTIAL Cover Sheet), will be placed on classified documents or files not in security storage. All items containing classified information, such as drafts, carbons, notes, floppy disks, typewriter and printer ribbons, plates, stencils, worksheets, etc., will be destroyed immediately after they have served their purpose, or protected as required for the level of classified information they contain.

b. SF 702 (Security Container Check Sheet) 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 a 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 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 person who locked the safe, will check the container to make sure it is properly secured. The person doing the checking will record the time the container was checked and initial the form. The person who locked the safe will see that the check is made.

(3) Containers not opened during a workday will be checked and the action recorded as in subparagraph (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) The SF 702 will be retained at least 24 hours following the last entry.

c. 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.

d. 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 (Security Container Information), 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.

e. 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.

6–11. End–of–Day security checks

a. Commands that access, process, or store–classified information will establish a system of security checks at the close of each working day to ensure that all classified material is properly secured. Standard Form 701 (Activity

Security Checklist), will be used to record these checks. An integral part of the security check system will be the securing of all vaults, secure rooms, and containers used for the storage of classified material; SF 702 will be used to record such actions. In addition, Standard Forms 701 and 702 will be annotated to reflect after–hours, weekend, and holiday activity.

b. 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.

6–12. Emergency planning

Commands will develop plans for the protection, removal, and destruction of classified material in case of fire, flood, earthquake, other natural disasters, civil disturbance, terrorist activities, or enemy action, to minimize the risk of its compromise. The level of detail in the plan and the amount and frequency of testing of the plan is at the command option, subject to MACOM approval, and should be based upon an assessment of the risk which might place the information in jeopardy. In this regard, special concern will be given for locations outside the United States. In preparing emergency plans, consideration must be given to reducing the amount of classified material on hand, including the transfer of information to microforms or removable computer media to reduce bulk, and the storage of less frequently used material at more secure locations. AR 380–40 contains policy for the emergency protection, including emergency destruction under no–notice conditions, of COMSEC material.

6–13. Telephone conversations

a. Classified discussions are not permitted in personal residences, in public, in public transportation conveyances (airplane, taxi, etc.), or in any area outside approved spaces on a U.S. Government or cleared contractor facility. Classified information will only be discussed, in telephone conversations, over secure communication equipment, such as a STU–III, and circuits approved for transmission of information at the level of classification being discussed. When discussing classified information, the ability of others in the area, who are not appropriately cleared or do not have a need–to–know, will be taken into consideration to make sure that classified information is not compromised by being heard or otherwise accessed by unauthorized personnel. This includes instances where the installation of STU–III telephones are authorized in personal residences. Non–secure telephones will have DD Form 2056 (Telephone Monitoring Notification Decal) affixed, advising the user that the telephone is subject to monitoring at all times and that use constitutes consent to this. Further guidance on monitoring can be found in AR 380–53.

b. As an exception to the policy on classified discussions in certain situations requiring immediate contact and discussion of classified information in off–duty hours, the installation of a secure telephone unit (such as STU–III) can be authorized in personal residences to the extent that MACOM policy permits, up to, and including, the SECRET level. Only the SECARMY is authorized to permit TOP SECRET communications, via approved secure methods, and document storage, in personal residences. The MACOM commander is authorized to permit SECRET communications, via approved secure methods, and document storage in personal residences. This will not be authorized for personal convenience. Where such communications units are permitted, care must be exercised in ensuring that unauthorized personnel, to include family members, are not within hearing distance when classified discussions take place, and that the control key for the communications unit is either personally retained or stored in a discrete location separate from the unit. In such cases, it can be necessary for the custodian of the unit to make notes regarding the classified discussion that occurs over the security telephone. Where this occurs, such classified notes can be retained in the personal residence only until the next duty day. If the next duty day falls during a period of more than one day, leave, Temporary Duty (TDY), or other absence, the material will be delivered for storage to a U.S. Government or cleared contractor facility prior to such absence. While in a personal residence, such classified notes will be safeguarded and under the personal, physical control of the authorized, cleared holder of the notes, at all times.

6–14. Speakerphone guidance

a. There has been a lot of questions and debates over the use of speakerphones in Sensitive Compartmented Information Facilities (SCIF) and other open–storage areas. According to Director of Central Intelligence Directives (DCID)1/21 speakerphones are restricted from common–use areas where sensitive conversations might be picked up inadvertently.

b. NSA S412 approves the installation/enablement of speakerphones on National Secure Telephone Systems (NSTS) and Secure Telephone Unit (STU)–III instruments. These systems will only be used in sole–use offices, conference rooms, and similar areas, and all room occupants are required to be aware of the conversations taking place, such as rooms used for contingency planning. The intent of speakerphone approval, rests with the room occupant assuming responsibility for taking the necessary precautions to ensure that the classified discussion is not overheard. STU–IIIs must be configured in such a manner as to prevent speaker enablement in the non–secure mode. Approval for use of non–secure speakerphones on NSTS and STU–III instruments will be granted by NSA S412 on a case–by–case basis.

In some configurations, Integrated Services Digital Network (ISDN) technology allows outsiders the capability to activate the speaker on the telephone without the individual's knowledge.

c. NSA S412 representatives conduct random reviews as part of their SCIF inspections to ensure speakerphones are being utilized IAW prescribed policy. NSA also maintains records of current speakerphone locations, which may be verified as required. Therefore, after NSA grants approval for use of a speakerphone in a selected sole–office or conference room, you should not move the speakerphone unless you submit to NSA S412 a new request for speakerphone use.

d. NSA speakerphone security guidance for SCIF areas include the following:

(1) Sole–use offices.

(a) The telephone instrument must be located in a sole–use office that affords sound attenuation.

(b) The office door must be closed prior to engaging in a speakerphone conversation.

(c) The user must be aware of any uncleared individuals in the vicinity and exercise sound judgement in determining when it is appropriate to engage in a speakerphone discussion.

(2) Conference rooms.

(a) The telephone instrument must be used in a conference room that affords sound attenuation.

(b) All conference room occupants must be appropriately cleared and have a "need–to–know" regarding the conversation.

(c) Entrance into the conference room must be controlled to ensure that only appropriately cleared individuals are present.

e. Any speakerphone mishap involving a possible security compromise or violation must be reported to NSA S412. See DCID 1/21 for further guidance.

6–15. Removal of Classified Storage and Information Processing Equipment

Storage containers and information processing equipment, which had been used to store or process classified information, will be inspected by cleared personnel, before removal from protected areas, and/or before unauthorized persons are allowed unescorted access to them. The inspection will ensure that no classified information remains within or on the equipment. Items to be inspected include security containers, reproduction equipment, facsimile machines, micrographic readers and printers, AIS equipment and components, equipment used to destroy classified material, and other equipment used for safeguarding or processing classified information. A written record of the inspection will be completed and maintained in accordance with paragraph 7–11.

6–16. Visits

Commands will establish procedures to control access to classified information by visitors. See AR 380–10 for the policy on foreign visitors.

a. Except when a continuing, frequent working relationship is established, through which a current security clearance and need–to–know are determined, DA personnel visiting other Army commands, other U.S. Government agencies, and U.S. Government contractors, will provide advance notification of any pending visit that is anticipated to involve access to classified information. The visit request will provide certification of the visitor's security clearance and the date(s) and purpose of the visit. Visit requests will be signed by an official other than the visitor and that official will be in a position to verify the visitor's security clearance. It can be approved, denied, or rescheduled at the option of the command being visited. As a general rule, unless otherwise indicated or contrary to command policy, visit requests sent to DA commands will be considered to be approved unless notification to the contrary is received. It is a recommended procedure to verify that the request was received and accepted. Visit requests can remain valid for up to one year.

b. Unless informed to the contrary, by the activity to be visited, visit requests involving DA personnel will include the following:

(1) Visitor's full name, date and place of birth, social security number, and rank or grade.

(2) Certification of visitor's security clearance and any special access authorizations required for the visit.

(3) Full address of visitor's command, and telephone number of a point of contact at that command. Point of contact is generally the person signing the visit request or the command security manager or other official who can verify the clearance status of the visitor.

(4) Name and address of the activity to be visited and name of person(s) to be contacted at the visited activity.

(5) Purpose of the visit, in sufficient detail to establish an assessment of need–to–know, and necessity of the visit.

(6) Date and duration of proposed visit. Intermittent visits on the same visit request can be authorized, where clearly stated on the request and approved by the command being visited, for up to one year.

c. Each agency outside of the Department of the Army has its own criteria for what constitutes the required elements on a visit request. Most are similar to, but may not be exactly the same as, the above. For example, contractors, under the terms of the National Industrial Security Program (NISP) Operating Manual (NISPOM), are not required to furnish the visitor's social security number. In such cases in which personnel, particularly non–DA personnel, are visiting an Army command, the command can decide whether or not the visit request is adequate and/or

request more information if necessary. Care is to be exercised in requiring additional personal information if it is not specifically relevant. For instance, if it is the policy of another agency to exclude the social security number, or the rank/grade, or the date/place of birth of the visitor, that information cannot be relevant, at least to that agency, if all the other elements of the visit request are satisfied. However, the visited Command will make the final determination as to what is required on the visit request.

6–17. Classified visits by Department of Energy personnel and to DOE facilities

a. Certification of security clearances. DA commands will accept certification of security clearances granted by other components of DOD and all other Federal Government departments and agencies, including clearances granted to contractors of the Federal Government. The DOE and Nuclear Regulatory Commission (NRC) use a different terminology in granting clearances. DA commands will accept DOE and NRC clearances for access to classified information as shown below.

(1) *DOE clearances.*

(a) Q sensitive. TOP SECRET Restricted Data/Formerly Restricted Data, and all other TOP SECRET information (exclusive of RD and FRD).

(b) Q non–sensitive. SECRET Restricted Data, TOP SECRET Formerly Restricted Data, and all other TOP SECRET information (exclusive of RD).

(c) TOP SECRET. No access to RD. Access authorized to TOP SECRET FRD and all other TOP SECRET information (exclusive of RD).

(d) L CONFIDENTIAL RD, SECRET FRD. L CONFIDENTIAL RD, SECRET FRD, and all other SECRET information (exclusive of RD).

(e) SECRET. No access to RD. Access authorized to SECRET FRD, and all other SECRET information (exclusive of RD).

(2) *NRC clearances.*

(a) Q (F) and (0). TOP SECRET RD/FRD, and all other TOP SECRET information.

(b) L (contractor). SECRET information (exclusive of RD and FRD), and CONFIDENTIAL FRD.

(c) L (employee). No access to RD or FRD. Access authorized to SECRET information (exclusive of RD and FRD).

(3) *Company CONFIDENTIAL clearances.* DOD or NISP approved Company CONFIDENTIAL clearances are not valid for access to RD.

b. Visits to DOE facilities and other requests for access to RD held by DOE.

(1) Requests for access to RD held by DOE or other U.S. federal agencies outside of DOD that are designated by DOE, will be made on DOE Form 5631.20, which replaced DOE Form DP–277. The form will be signed by an official that is authorized, no lower than brigade commander level or equivalent, or that official's representative, designated in writing for security matters. The list of authorized officials will be approved and compiled by DAMI–CH and forwarded to the DOE. An information copy of the list will be forwarded, by DAMI–CH, to, and held at, the office of the senior security official at each MACOM, and for the HQDA activities, the office of the senior security official in the office of the Administrative Assistant to the Secretary of the Army. Additions, changes, or deletions to the list of certifying officials will be forwarded through command channels to DAMI–CH, and will include the complete name and address of the command, title of the command certifying official, phone number of the office that will make the certification, and the justification.

(2) The request will state that the individual requires repeated access to the same type of information, or continuing visits to a facility, under the cognizance of the same approving authority, if applicable. Generally, arrangements for continuing access can be made for a period not to exceed one year, subject to approval by DOE. In such cases, the DOE facility requires advance notification of each visit. This notification procedure will be verified with the approving office. Access by military personnel can be arranged for the specified period of their assignment. If access to CNWDI is required, a statement to that affect will be listed on the form. It is recommended that the point of contact, at the site to be visited, be contacted to obtain the correct office location for submission of the form. Without any specific information to the contrary, the DOE Form 5631.20 will be submitted as follows:

(a) Direct to DOE, Director of Safeguards and Security, Washington, D.C. 20585, for information at DOE.

(b) To the U.S. Nuclear Regulatory Commission, Division of Security, Washington, D.C. 20555, for requests that pertain to the Army and Navy Research Reactor Program and when the RD is held by federal government agencies other than DOD.

(c) To the managers of the Albuquerque or San Francisco DOE operations offices, or officials designated by them, for data that pertains to weapons programs.

(d) To the DOE headquarters division that has responsibility for the subject matter involved, regarding information in the custody of DOE personnel in situations other than those described above.

(3) DOE personnel will accept oral requests for access to RD in emergencies. In such cases, the same information that is requested on DOE Form 5631.20 will be provided and an appropriate written confirmation will be forward as

soon as possible. DOE personnel authorized to approve requests for access to, or release of, RD will make determinations of emergency situations.

6–18. Classified meetings and conferences

Meetings, conferences, classes, seminars, symposia, and similar activities, at which classified information is to be presented or discussed, are considered "classified meetings." The classified portions of these meetings present special vulnerabilities to unauthorized disclosure and will be limited to persons possessing an appropriate clearance and access and the need–to–know for the specific information involved. Security requirements contained elsewhere in this regulation and other applicable security regulations apply, without exception, to classified meetings.

a. For purposes of this regulation, classified meetings are divided into two categories: in–house classified meetings, and association–related classified meetings.

(1) *In–House Classified Meetings.* In–house classified meetings involve routine gatherings of U.S. Government officials, classes conducted at U.S. Government schools, meetings between U.S. Government personnel and current or potential contractor personnel, other than that which is association–related, on a matter related to a specific government contract, program, or project, or gatherings of U.S. Government personnel and foreign government and/or foreign contractor representatives on a matter related to a specific government contract, program, or project. There are no special requirements for in–house classified meetings. Security and foreign disclosure procedures specified elsewhere in this and other applicable regulations, such as AR 380–10, apply, including the requirement to hold the classified portions of the meeting in approved spaces on a U.S. Government installation or cleared contractor facility.

(2) *Association–Related Classified Meetings.* A meeting which involves a non–U.S. Government association or organization is considered, for the purposes of this regulation, to be an association–related meeting. Examples of association–related meetings are conferences, symposia, seminars, or other meetings of organizations such as the American Society of Military Engineers, the Association of Old Crows, Association of the U.S. Army, American Defense Preparedness Association, Aerospace Industries Association, etc. The need–to–know concept must be strictly adhered to when considering classified sessions at an association–related meeting. The mere fact that an individual is cleared and is a member of the association does not in any way constitute a need–to–know for the classified information to be presented at the meeting. Wide dissemination of classified information at the type of general meeting, represented in association–related meetings, increases the potential risk of unauthorized access to, and compromise of, classified information. Presentation of classified information at such meetings requires complete justification to ensure that dissemination of the information, to the association membership, is in the U.S. Government's interests, and, where presentation is justified, requires careful attention to security requirements. When an association wishes to hold a classified meeting or classified sessions at its general meeting for its members and other invited guests, it must obtain the agreement of a U.S. Government agency to act as the U.S. Government security control for the meeting. DA Commands will not accept security control for association–related classified meetings until approval has been obtained from the DCSINT, through DAMI–CH.

b. Approval authority. Security control by a DA command for any association–related classified meeting, and any meeting which involves foreign participation, and does not fall within the criteria of "in–house" classified meeting, as stated in subparagraph a above, will require the approval of the DCSINT. Once approved, a specific, detailed security plan must be put in place to ensure that classified information is safeguarded and is not accessed by unauthorized persons, those without a clearance, or cleared but without a need–to–know for the specific information. The plan will be developed by the command and approved by the MACOM. HQDA approval for security control will be considered only when all of the following conditions are met:

(1) The meeting will serve a specific U.S. Government purpose.

(2) The use of other appropriate channels for dissemination of classified information will not serve the purpose.

(3) The meeting location will be under the security control of a DA command, other U.S. Government activity, or a U.S. contractor with an appropriate facility security clearance.

(4) Adequate security procedures have been developed and will be implemented to minimize risk to the classified information involved.

(5) Screening for verification of security clearance and need–to–know of potential attendees is specifically addressed and followed.

(6) Classified sessions will be segregated from unclassified sessions whenever possible.

(7) Any participation by foreign nationals or foreign representatives complies with the requirements of DODI 5230.20 and DODD 5230.11. For example, assurance is obtained, in writing, from the responsible U.S. Government foreign disclosure office(s) that the information to be presented has been cleared for foreign disclosure.

(8) Announcement of the classified meeting will be unclassified and limited to a general description of topics expected to be presented, names of speakers, logistical information, and administrative and security instructions.

(9) Non–government organizations may assist in organizing and provide administrative support for a classified meeting, but all security requirements remain the specific responsibility of the DA MACOM sponsoring the meeting.

(10) Procedures must ensure that classified documents, recordings, audiovisual material, notes, and other materials created, distributed, or used during the meeting are controlled, safeguarded, and transported as required by other

provisions of this regulation. Note taking or electronic recording during classified sessions will be permitted only when it is determined that such action is necessary to fulfill the U.S. Government purpose for the meeting.

c. Obtaining authorization. When a DA command wishes to be authorized to serve as the security sponsor for an association–related classified meeting, they will make the request, through command channels, to DAMI–CH. It must be received at least 120 days in advance of the meeting. The request will contain adequate justification or explanation for all points in subparagraph b above and an overall description of the classified information to be presented. In addition, if the association is intending to invite citizens of foreign countries, the command will request approval for the disclosure of specified classified information to the countries or foreign nationals expected to attend (see AR 380–10). Foreign nationals, of approved countries, can then submit visit requests, through their embassies, as provided in AR 380–10.

d. Command and MACOM responsibilities. The decision on the approval or disapproval of security sponsorship, of an association–related classified meeting, will be communicated by DAMI–CH, to the command and its MACOM. If HQDA approval has been obtained, the command authorized as the security sponsor can inform the association that the announcements for the location of the meeting can be sent to its members. Announcements mentioning the location of the meeting or stating that a DA command has accepted security sponsorship can be made only after HQDA approval has been obtained. Announcements of classified meetings will be unclassified and limited to a general description of topics expected to be presented, names of speakers, logistical information, and administrative and security instructions. The command sponsoring the meeting will take the following actions:

(1) Appoint a security manager for this project. Only DA personnel can be appointed as the security manager for the meeting. Other U.S. Government or cleared contractor personnel can assist with the implementation of security requirements under the direction of the appointed security manager. Other association personnel can assist in the organization of, and administrative support to, the meeting.

(2) Develop a security plan. The command's MACOM must approve the final security plan to be implemented at the meeting. The security plan will describe the procedures that will be used to ensure that proper security measures for the access, control, storage, and dissemination of the classified information have been developed and will be implemented.

(3) Make sure that all personnel attending have the appropriate security clearance, access, and need–to–know for the specific information to be presented. The mere fact that an individual is cleared and is a member of the association does not in any way constitute a need–to–know for the classified information to be presented at the meeting. A visit request will be required for all U.S. Government personnel. If the U.S. Government personnel attending the meeting are in a duty status, as opposed to being in a leave status, the visit request can serve as certification of need–to–know and a specific statement of need–to–know will not be required. A visit request with U.S. Government contracting officer certification of need–to–know, will be required for contractor personnel. The certification of need–to–know for contractor personnel will be in writing, will specify the applicable contract number, or project or program if pre–contract activity serves as justification, and will be made by the U.S. Government contracting officer for the particular contract pertaining to the need–to–know for the information presented or discussed at the meeting.

(4) Make sure that participation or attendance by foreign nationals or foreign representatives complies with the requirements of AR 380–10. Foreign personnel can be invited to participate only after HQDA approval and the requirements of AR 380–10 are met.

(5) Make sure that all classified papers to be used, and all classified presentations, have been approved, in writing, by the originators of the information, for release to the cleared association members. Written foreign disclosure authorization will be required if there are to be foreign attendees at the meeting (see AR 380–10).

(6) Make sure that the classified sessions are segregated from the unclassified sessions at all times and that the classified sessions are held only at a U.S. Government installation or a cleared contractor facility. The location must allow proper control of physical, auditory and visual access to the classified information.
Note: No Department of the Army official is authorized to waive the requirement to hold such classified meetings at a U.S. Government installation or cleared contractor facility.

(7) Make sure that all classified material created, distributed, or used during the meeting are controlled, accounted for, safeguarded, and transmitted as required by other provisions of this regulation. Note–taking or electronic recording during the classified sessions will be permitted only if, in approving the plan, the MACOM approving official makes a specific determination that it is necessary to do so in order to fulfill the U.S. Government purpose for the meeting. If such approval is requested, the command will specifically state such in the security plan, or in the cover letter, for the MACOM request for approval of the plan.

6–19. Information processing equipment

There are a variety of non–COMSEC–approved equipment that are used to process classified information. This includes copiers, facsimile machines, computers, notebooks and other AIS equipment and peripherals, electronic typewriters, word processing systems, hand–held personal data managers, etc. Commands will identify those features, parts, or functions of equipment used to process classified information that can retain all or part of the information. Command security procedures will prescribe the appropriate safeguards to prevent unauthorized access to that information, and replace, control, and/or destroy equipment parts, pursuant to the level of the classified material contained

therein, when the information cannot be removed from them. Alternatively, the equipment can be designated as classified and appropriately protected at the retained information's classification level (for instance, by being installed in a vault approved for the storage of classified information at that classification level).

6–20. Receipt of classified material

Commands will develop procedures to protect incoming mail, bulk shipments, and items delivered by messenger, until a determination is made whether classified information is contained in the mail. Screening points will be established to limit access to classified information.

Section III
Accountability and Administrative Procedures

6–21. TOP SECRET information

Material containing TOP SECRET information will be provided continuous control and accountability. Commands will establish procedures, tailored to the individual situation, in accordance with the principles of risk management, for the control and accountability of the TOP SECRET material they hold. These procedures will provide the means of facilitating oversight and management of TOP SECRET access controls, assessment and management of holdings, and identification of material at risk, in cases of potential unauthorized disclosure. In developing these procedures, the following minimum requirements will be met.

a. TOP SECRET Control Officers (TSCO) will be designated within offices which handle or maintain TOP SECRET material. They will be responsible for receiving, dispatching, and maintaining accountability and access records for TOP SECRET material. Such individuals will be selected on the basis of experience and reliability, and as a general rule, will already possess the appropriate clearance and access level equal to or higher than the information to be handled, and be a minimum grade of GS–07 or rank of E–7. Grade/rank can be waived by the commander, subject to MACOM policy on this matter. One or more alternate TSCOs will also be designated. There is no grade/rank preference for alternate TSCOs. TSCOs need not be appointed in those instances where there is no likelihood of processing TOP SECRET documentation. In such circumstances, the command will record the fact that a TSCO has not been appointed. TSCOs will maintain a current, accurate system of accountability within the command for all TOP SECRET documents and other material. TSCOs will record the receipt, dispatch, downgrading, movement from one command element to another, current custodian, and destruction of all TOP SECRET material. Automated information systems can be used to maintain these records.

b. TOP SECRET material will be accounted for by a continuous chain of receipts. Receipts will be maintained for five years. TOP SECRET registers (for example, DA Form 455 (Mail and Document Register) or equivalent) and TOP SECRET accountability record forms (for example, DA Form 3964 (Classified Document Accountability Record) or equivalent) will reflect sufficient information to identify adequately the TOP SECRET document or material. As a minimum, it will include the title or short title, date of the document, identification of the originator, copy number, and disposition. TOP SECRET material will be numbered serially and marked to indicate its copy number (for example, copy 1 of 2 copies) and accounted for accordingly.

c. TOP SECRET material will be inventoried at least once annually. The inventory will reconcile the TOP SECRET accountability register and records with 100 percent of the TOP SECRET material held. The inventory will be conducted by two properly cleared individuals. One will be the TSCO or alternate, and the other will be a properly cleared, disinterested party, that is neither a TSCO, alternate, or subordinate to either official. The inventory will consist of a physical sighting of the material or written evidence of authorized disposition, such as certificate of destruction or receipt of transfer. At the time of the inventory, each TOP SECRET document or material will be physically examined for completeness and the TSCO will ensure that the accountability record accurately reflects the material held. Discrepancies found during the inventory will be resolved immediately, or, where they cannot be immediately resolved, referred to the command security manager for further investigation.

d. In activities that store exceptionally large volumes of TOP SECRET material, MACOMs can authorize the inventory of TOP SECRET material to be limited to documents and material to which access has been granted within the past year (use the TSCO's accountability records), and 10 percent of the remaining inventory. The 10 percent will be randomly selected. MACOMs will document these authorizations and retain such documentation for as long as the authorization remains. In such cases, MACOM oversight will include a spot inventory of randomly selected TOP SECRET material during Advice and Assistance Visits (AAV), inspections, or other security reviews. Note: MACOMs cannot authorize the exception to the 100 percent inventory for TOP SECRET Special Access Programs information (see DODD 5220.22–M). Requests for an exception to the 100 percent annual inventory for TOP SECRET Special Access Programs information will be completely justified and submitted through command channels to DAMI–CH (SAPs).

e. Before leaving the command, the TSCO or alternate will conduct a joint inventory with the new TSCO or alternate of all TOP SECRET material for which they have custodial responsibility. In addition, a 100 percent inventory of all TOP SECRET material held by the command is advised, but not required. However, the new TSCO or alternate will be held accountable for all TOP SECRET material for which they have custodial responsibility.

f. As stated above, commands will establish procedures that provide a means of making easier the oversight and management of TOP SECRET access controls, assessment and management of holdings, and the identification of material at risk, in cases of potential unauthorized disclosure. Disclosure records can be used as a means to help meet these requirements. Disclosure records, such as DA Form 969 (Top Secret Document Record) or a similar form, provide a means to record the name of the individual(s) to whom the information/material has been disclosed, and the date(s) of the disclosure. They are a means that commands can choose to use in the execution of the above–cited responsibilities.

6–22. SECRET and CONFIDENTIAL information

Commands will establish procedures to control all SECRET and CONFIDENTIAL information and material originated, received, distributed, or routed to sub–elements within the command, and all information disposed of by the command by transfer of custody or destruction. The control system for SECRET and CONFIDENTIAL information is to be determined by a practical balance of security and operating efficiency.

6–23. NATO and Foreign Government material

Accountability requirements for NATO material are contained in AR 380–15. See paragraph 6–29 for recording the destruction of foreign government and NATO material.

6–24. Working papers

a. Working papers are documents and material accumulated or created in the preparation of finished documents and material. Working papers containing classified information will be:

(1) Dated when created.

(2) Conspicuously marked as "DRAFT" or "WORKING PAPERS" on the first page of the document in letters larger than the text.

(3) Marked with the highest classification of any information contained in the material.

(4) Protected in accordance with the assigned classification.

(5) Destroyed when no longer needed.

(6) 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 command or transmitted electronically or through message center channels within the activity (exclusive or through a local area network or other automated system when the transmission does not go beyond the command).

(b) Retained for more than 180 days from the date of origin.

(c) Filed permanently.

(d) TOP SECRET information is contained therein.

b. MACOMs can grant exceptions for accountability, control, and marking requirements for working papers containing TOP SECRET information on a case–by–case basis provided a determination is made that:

(1) The conditions set forth in subparagraphs a6(a), (b), or (c), above, will remain in effect.

(2) The Command seeking an exception 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 command's mission or operations.

(3) Access to areas where TOP SECRET working papers are handled is restricted to personnel who have a TOP SECRET clearance, and other safeguarding measures are adequate to prevent the possibility of unauthorized disclosure.

Section IV
Reproduction of Classified Material

6–25. Policy

Documents and other material containing classified information will be reproduced only when necessary for the accomplishment of the command's mission or for compliance with applicable statutes or directives. Reproduction equipment and the reproduction process involve substantial risk. Therefore, commands will establish and enforce procedures for the reproduction of classified material which limit reproduction to that which is mission essential and will make sure that appropriate countermeasures are taken to negate or minimize any risk. All copies of classified documents reproduced for any purpose, including those incorporated in working papers, are subject to the same safeguards and controls prescribed for the document from which the reproduction is made. Reproduced material will be clearly identified as classified at the applicable level. TOP SECRET material will be numbered serially and marked to indicate its copy number (for example, copy 1 of 2 copies) and accounted for accordingly. Waste products generated during reproduction will be properly safeguarded as appropriate to the level of classification contained within, and destroyed in a manner approved for the destruction of classified information at that classification level.

a. Stated prohibition against reproduction of information at any classification level will be prominently displayed and strictly observed (for example, notices stating "Reproduction Only by Permission of Originator").

b. Except for the controlled initial distribution of information processed or received electronically, or that containing COMSEC or SCI which are governed by separate requirements, reproduction of TOP SECRET information, either portions of documents or whole documents, will be strictly controlled. Written authorization, by the TSCO or other command official who has been designated in writing as having this authority (TOP SECRET reproduction control official) is required. The command official can only authorize the local reproduction of TOP SECRET material with permission of the originator or higher authority (see paragraph 6–26). Once copies are made, the TSCO will be advised of the reproduction and will place the copied material under the command accountability system.

c. Specific equipment will be designated for the reproduction of classified information. Such equipment cannot be designated for classified reproduction if it leaves latent images in the equipment or on other material. Exceptions are that the equipment is in a vault or other area approved for the storage of classified information, the equipment is protected as classified material, and the material on which the image resides is destroyed as classified waste. Rules for reproduction of classified information will be posted on or near the designated equipment. Personnel who operate reproduction equipment will be made aware of the risks involved with the specific equipment, the command procedures concerning the protection, control and accountability of reproduced information as well as the destruction of classified waste products. Information on security hazards associated with various types of reproduction equipment can be obtained from the Intelligence Materiel Activity (IMA), Intelligence Materiel Management Center, Fort Meade, MD, 20755–5315. Notices prohibiting reproduction of classified information will be posted on equipment used only for the reproduction of unclassified information.

6–26. Approval for reproduction

a. Commands will establish procedures which ensure that appropriate approval is granted before classified material is reproduced. As a minimum, these procedures will—

(1) Require approval of the originator or higher authority before reproducing TOP SECRET documents and material.

(2) Ensure compliance with reproduction limitations placed on documents by originators and special controls applicable to Special Access Programs and other special categories of information.

(3) Make easier the oversight and control of reproduction of classified material.

b. A written record will be maintained verifying the approval authorization for reproduction of TOP SECRET information and, where required, for information addressed in subparagraph a(2), above. This record will be maintained for the life of the copy and filed with the destruction certificate when the copy is destroyed.

c. The provisions of subparagraphs a(l) and a(2), above, will not restrict the reproduction of documents for the purpose of facilitating declassification review. After review for declassification, those reproduced documents that remain classified must be destroyed in accordance with section V of this chapter.

Section V
Disposition and Destruction of Classified Material

6–27. Policy

a. Classified documents and other material will be retained only if they are required for effective and efficient operation of the command or if their retention is required by law or regulation. Requests from contractors for retention of classified material will only be approved if they meet the same criteria and approvals are in the best interests of the government. See AR 380–49 for more guidance on contractor retention.

b. Documents which are no longer required for operational purposes will be disposed of in accordance with the provisions of the Federal Records Act (44 USC chapters 21 and 33) as implemented by AR 25–400–2. Classified information is subject to the same retention criteria as unclassified information. Special care will be exercised in the placing of classified information in files designated under AR 25–400–2 as "permanent". Such files can, and many are, eventually accessioned into the National Archives. These files are subject to any automatic, systematic, and mandatory declassification systems that exist now or will in the future. Resources, at present, cannot permit a careful review of all of the material prior to declassification. In order to conserve resources, the declassification review personnel can rely heavily on the markings on the front of the document and on the SF 135 for those cases in which the boxes cannot be opened prior to a decision to employ bulk declassification based upon a description of the contents of the file box. Resources cannot permit a careful review for unclassified, "For Official Use Only (FOUO)," information unless the FOUO markings are conspicuous on the front of the document and on the portions to which they apply, and are included in the SF 135 description. Command personnel must be aware that the current policy, as stated in the recent EO 12958, with amendments, refers to the declassification of information contained in permanent records that have been determined to have permanent historical value, by the Archivist of the U.S., under Title 44, U.S. Code. Therefore, once the classified material has been placed in a file designated under MARKS (AR 25–400–2) as "permanent," the

information in the files will be subject to the automatic declassification provisions of the prevailing EO, whether or not reviewed for declassification by DA personnel.

c. Commands will review classified files designated as "permanent," under AR 25–400–2, prior to forwarding to a Federal Records Center, where the files are maintained pending ultimate destruction or accession into the National Archives. Each classified document in the files will be reviewed to ensure that:

(1) The classified material is a necessary part of the file as described in AR 25–400–2.

(2) That only the record copy is placed in the file and that duplicate copies are destroyed.

(3) That the classified material has been reviewed for downgrading and declassification instructions and is properly remarked if downgraded or declassified.

(4) That any For Official Use Only information, that is contained in the document, is properly marked and a notice, that the document contains FOUO information, is displayed on the front cover and title page, or the first page when there is no cover or title page. Also, that it is marked on the applicable portions of the document. It is recommended that unclassified documents in the file that contain FOUO information be checked at the same time to make sure they are properly identified on the documents, on the file, and on the SF 135. This is because the National Archives can permit access to the public of unclassified information in permanent files if it is not clearly apparent that the information contains FOUO information.

(5) That the subject of the classified information is adequately described on the file label.

(6) That Restricted Data and Formerly Restricted Data and foreign government information are not intermingled with other information, and it is clearly marked on the file and accompanying forms (see AR 25–400–2, paragraph 9–2).

(7) That TOP SECRET information is not included unless it meets the criteria stated in AR 25–400–2, paragraph 9–2.

(8) That the subject of the classified information is adequately and completely described in the accompanying documentation, the SF 135 and SF 135–A (Continuation) as required by AR 25–400–2. Paragraph 9–5 of AR 25–400–2 requires that the SF 135, or SF 135–A, describe records in enough detail to permit quick retrieval of specific documents. This is true for all files whether classified or unclassified. However, particular attention to this requirement must be paid when the file is designated as "permanent" and contains classified material.

d. Commanders will make sure that the management of the retention of classified material is included in oversight and evaluation of program effectiveness.

e. Material which has been identified for destruction will continue to be protected as appropriate for its classification until it is actually destroyed. Destruction of classified documents and material will be accomplished by a means which eliminate risk of reconstruction of the classified information and will follow the criteria stated in this regulation.

6–28. Methods and standards for destruction

a. Classified documents and materials will be destroyed by burning, or, when meeting the standards contained in chapter 3, of this regulation, by melting, chemical decomposition, pulping, pulverizing, cross–cut shredding, or mutilation, sufficient to preclude recognition or reconstruction of the classified information. Strip shredders, those that do not have a half–inch cross cut feature, do not sufficiently destroy the information and are not authorized for use. MACOMs can approve the use of strip shredders, in exceptional cases, for use in the destruction of classified material at the SECRET level and below, under the following conditions: if the equipment was purchased prior to June, 1986, there are no other means of destruction available to the command, and additional precautions, such as shredding at least 20 pages of similar material, not blank paper, at the same time, are utilized to minimize risk of reconstruction of the material. MACOMs must consider efforts to replace the strip shredders as soon as possible.

b. Technical assistance and guidance on the application of the standards described above can be obtained from the Intelligence Materiel Activity, Intelligence Materiel Management Center, Fort Meade, MD 20755–5315.

c. Systems which involve the collection of classified material for later destruction, for example, the use of burn bags, will include provisions for minimizing the risk of compromise of the material while it awaits destruction.

6–29. Records of destruction

a. Records of destruction are required for TOP SECRET documents and material. The record will be executed when the material is actually destroyed, or when it is torn and placed in a burn bag or similar container. Two persons will sign the destruction record as witnessing the destruction. DA Form 3964 (Classified Document Accountability Record) may be used for this purpose. Destruction records are not required for waste materials (scratch notes, typewriter and printer ribbons, carbon paper, etc.) containing TOP SECRET information, unless that material has been placed on an accountability record.

b. Records of destruction are not required for SECRET material, except for NATO and foreign government documents. For NATO or foreign government SECRET material, two signatures are required on the record of destruction. Records of destruction are not necessary for CONFIDENTIAL material unless required by the originator.

c. Records of destruction will be maintained for 5 years from the date of destruction. For guidance on requirements for NATO classified material, to include retention standards, see AR 380–15.

Section VI
Waivers

6–30. General
Waivers to the requirements in sections III through V of this Chapter can be authorized by MACOM commanders, and for HQDA activities, by the Administrative Assistant to the Secretary of the Army. This authority will not be further delegated and does not apply to any other section, Chapter, or appendix of this regulation. Waiver approval will follow the policy discussed in this Chapter. Waivers pertaining to SAPs will be submitted in accordance with appendix I, of this regulation, and AR 380–381.

6–31. Unique situation and compensatory measures
a. A waiver will be granted only on a case–by–case basis and when the approval authority has determined that:

(1) A unique or an unusual situation or factor exists requiring deviation from the established policy; and

(2) A system of alternative compensatory measures adequately addresses the protection of classified information.

b. The alternative compensatory measures will be tailored to make sure that the intent of the protection requirement has been fulfilled by the application of other measures not addressed in the established policy. The alternative compensatory measures must show the protection afforded classified information is sufficient to reasonably deter and detect the loss or compromise of the classified information. Deviations to established requirements will be based on the consideration of risk management factors such as: criticality, sensitivity, and value of the information, analysis of the threat both known and anticipated, vulnerability to exploitation, and countermeasures benefits versus cost (both monetary and cost to national security). Waivers to requirements for records that must be maintained, concerning foreign government information, are not authorized.

6–32. Duration
Waivers are normally granted for a limited, specific duration, but can be approved for an indefinite period, if deemed appropriate, by the approval authority. In either case, a waiver must be revalidated no less than every five years. The revalidation will require rejustification of the unique or unusual circumstances that supports the request for a waiver and a current assessment to make sure the alternative compensatory measures do afford the protection to the classified information and that they are sufficient to reasonably deter and detect loss or compromise and meet the intent of the established policy being waived.

6–33. Documentation
Waivers will be documented and furnished upon request to other agencies with whom classified information or secure facilities are shared. The waiver documentation will describe the alternative compensatory measures and contain an assessment of how those alternative compensatory measures fulfill the intent of the protection requirement of the policy being waived. The continuing need for waivers will be a factor in the command inspection program. The record of waiver will be made available to inspection personnel and will be maintained for as long as the waiver is in effect.

6–34. Prior waivers
Waivers granted prior to the effective date of this regulation are canceled no later than one year after the effective date of this regulation. See paragraph 1–19 for waivers pertaining to any requirement beyond those contained in sections III through V of this Chapter.

Section VII
Inspections

6–35. Self Inspection
Heads of DA MACOMs, units, activities, and agencies will establish and maintain a self–inspection program based on program needs and the degree of involvement with classified information. The purpose of the program shall be to evaluate and assess the effectiveness and efficiency of the Command's implementation of the Army Information Security Program. Commands that originate significant amounts of classified information should be inspected at least annually.

6–36. Entry Exit Inspection Program and Two Person Integrity for TOP SECRET Information
The previous edition of this regulation required all commands to establish a program to inspect for the unauthorized removal of classified information. Although this program, known as the Entry/Exit Inspection Program (EEIP) is, effective by this regulation, no longer a Department of the Army–wide requirement, it does remain an effective tool that can be used in command security programs to deter and detect the unauthorized removal of classified information.

When effectively implemented the EEIP provides visibility and emphasis to the command security program. Its use is a command option. The Two Person Integrity (TPI) Program is, effective by this regulation, no longer a Department of the Army–wide requirement. Personnel are reminded that the unauthorized disclosure of TOP SECRET information can result in exceptionally grave damage to national security. TPI is a tool that can be used to better protect this high level of classification and should be considered for inclusion in command security programs. Its use is also a command option. Two persons are required, however, for the destruction of TOP SECRET material as stated in paragraph 6–29, and may be required for SAPs (see AR 380–381).

Chapter 7
Storage and Physical Security Standards

Section I
General

7–1. Policy
Classified information will be secured under conditions adequate to prevent access by unauthorized persons and meeting the minimum standards specified in this regulation. An assessment of the threat to the material, the location of the command, and the sensitivity of the information, will be considered when determining if the minimum requirements of this Chapter require enhancement, as determined by the local command. Based upon an assessment of the threat, the command will institute appropriate security measures designed to make unauthorized access so difficult that an intruder will hesitate to attempt to try to gain access or enhance the likelihood of discovery and apprehension if an unauthorized access is attempted.

7–2. Physical security policy
a. Physical security is intended to be built upon a system of defense, or security in depth, to provide accumulated delay time. AR 190–13, AR 190–16, and Field Manual (FM) 19–30, provide additional information on the principals of physical security. For technical assistance concerning classified material physical security storage standards, commands can contact the Army Intelligence Materiel Activity (IMA), Intelligence Materiel Management Center, Fort George G. Meade, MD 20755–5315.

b. AR 190–13 prescribes minimum uniform standards and procedures in the use of security identification cards and badges to control personnel movement into, and movement within, restricted areas. These standards and procedures are established to safeguard facilities against espionage, sabotage, damage, and theft. Security identification cards and badges may be used to control access to installations and activities. They will be used in addition to other required identification cards to military personnel, civilian DOD and contractor employees, and visitors entering installations, activities, or restricted areas, as determined by the commander concerned.

Section II
Storage Standards

7–3. Standards for storage equipment
General Services Administration (GSA) establishes and publishes minimum standards, specifications, and supply schedules for containers, vault doors, modular vaults, alarm systems, and associated security devices suitable for the storage and protection of classified information.

7–4. Storage of classified information
a. Classified information that is not under the personal control and observation of an authorized person, is to be guarded or stored in a locked security container, vault, room, or area, pursuant to the level of classification and this regulation by one or more of the following methods:

(1) TOP SECRET information will be stored as identified below:

(a) A GSA–approved security container with one of the following supplemental controls:

1. The location that houses the security container will be subject to continuous protection by cleared guard or duty personnel.

2. Cleared guard or duty personnel will inspect the security container once every two hours, but not in a way that indicates a pattern.

3. An Intrusion Detection System (IDS), meeting the requirements of section III of this Chapter, with personnel responding to the alarm, arriving within 15 minutes of the alarm annunciation.

4. Security–in–depth when the GSA–approved container is equipped with a lock meeting Federal Specification FF–L–2740A. See appendix J for a definition of security–in–depth.

(b) A vault, modular vault, or security room constructed in accordance with section III of this Chapter, and equipped

with an IDS with the personnel responding to the alarm within 15 minutes of the alarm annunciation if the area is covered by security–in–depth, or a 5 minute alarm response time if it is not. Other rooms that were approved under former policy for the storage of TOP SECRET in the U.S. can continue to be used.

(c) New purchases of combination locks for GSA–approved security containers, vault doors and secure rooms will conform to Federal Specification FF–L–2740A. Existing, non–FF–L–2740A mechanical combination locks will not be repaired. If they should fail, they will be replaced with locks meeting FF–L–2740A. See section IV for information on retrofitting locks (replacing locks with those meeting Federal Specification FF–L–2740A) on existing containers where the lock is not in need of repair.

(d) Under field conditions, during military operations, commanders can prescribe the measures deemed adequate to meet the storage standard contained in subparagraphs 1 and 2 above.

(2) SECRET information will be stored—

(a) In the same manner as prescribed for TOP SECRET.

(b) In a GSA–approved security container or vault without supplemental controls.

(c) In secure rooms that were approved for the storage of SECRET or CONFIDENTIAL information by the 28 February 1988 edition of this regulation, provided that the approval for storage occurred prior to 1 October 1995.

(d) Until 1 October 2002, in a non–GSA–approved container having a built–in combination lock, or in a non–GSA–approved container secured with a rigid metal lock–bar and a GSA–approved padlock with one or more of the following supplemental controls.

1. The location that houses the container is subject to continuous protection by cleared guard or duty personnel.

2. Cleared guard or duty personnel will inspect the security container once every four hours, using random times.

3. An IDS with the personnel responding to the alarm arriving within 30 minutes of the alarm. In order to reduce the risk of the lock being swapped while the container is opened, the padlock will be secured to the hasp in the locked position, or the padlock will be locked and placed inside the cabinet. Commands are encouraged to replace the non–GSA–approved cabinets with GSA–approved security containers as soon as feasible, prior to the mandatory replacement date of 1 October 2002. New lock–bar cabinets will not be fabricated from either existing or new containers, nor will any existing lock–bar container, that was not previously used for the protection of classified information, be put into use for that purpose.

(3) CONFIDENTIAL information will be stored in the same manner as prescribed for TOP SECRET and SECRET information except that supplemental controls are not required. Where lock–bar cabinets are used, in order to reduce the risk of the lock being swapped while the container is open, the padlock will be secured to the hasp in the locked position, or the padlock will be locked and placed inside the cabinet. Commands are encouraged to replace the non–GSA–approved cabinets with GSA–approved security containers as soon as feasible prior to the mandatory replacement date of 1 October 2002. New lock–bar cabinets will not be fabricated from either existing or new containers, nor will any existing lock–bar container, that was not previously used for the protection of classified information, be put into use for that purpose.

b. Specialized security equipment.

(1) GSA–approved field safes and special purpose, one and two drawer, light–weight, security containers, approved by the GSA, are used primarily for storage of classified information in the field and in military platforms, and will be used only for those or similar purposes. Such containers will be securely fastened to the structure or under sufficient surveillance to prevent their theft or compromise.

(2) GSA–approved map and plan files are available for storage of odd–sized items such as computer media, maps, charts, and classified equipment.

(3) GSA–approved modular vaults, meeting Federal Specification AA–V–2737, can be used to store classified information as an alternative to vault requirements described in section III of this Chapter.

c. Replacement of combination locks. The mission and location of the command, the classification level and sensitivity of the information, and the overall security posture of the activity, are factors used in determining the priority for replacement of existing combination locks. All system components and supplemental security measures, including electronic security systems (e.g., intrusion detection systems, automated entry control subsystems, and video assessment subsystems), and level of operations, must be evaluated by the command when determining the priority for replacement of security equipment. Section IV of this Chapter provides a matrix illustrating a prioritization scheme for the replacement of existing combination locks on GSA–approved security containers and vault doors, and can be used as a guide for this purpose. The prioritization scheme can be tailored to specific environments and sensitivity of information stored. Priority 1 requires immediate replacement. Replacement is generally considered to be accomplished when the equipment is obtained and installed within the framework of the command budget constraints, but in no event will exceed two years from the effective date of this regulation.

d. Storage areas. Storage areas, for bulky material containing SECRET or CONFIDENTIAL information, can have access openings secured by GSA–approved, changeable, combination padlocks (Federal Specification FF–P–110 series) or high security, key–operated padlocks (Military Specification MIL–P–43607). Other security measures are required, in accordance with paragraph 7–4a(1), above, for TOP SECRET material, and are strongly recommended for all other levels of classified material.

(1) Commands will establish administrative procedures for the control and accountability of keys and locks whenever key–operated, high–security padlocks are utilized. The level of protection provided such keys will be equivalent to that afforded the classified information being protected by the padlock. As a minimum, the following procedures will be implemented.

(a) A key and lock custodian will be appointed in writing to ensure proper custody and handling of keys and locks.

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

(c) Keys and locks will be audited at least quarterly.

(d) Keys will be inventoried with each change of custodian. Keys will not be removed from the premises.

(e) Keys and spare locks will be protected in a security container or other secure container;

(f) In order to reduce the risk of the padlock being swapped while the container is opened, the padlock and the key will be either placed in the security container, or the padlock will be locked to the hasp and the key either personally retained, retained at a central location, or placed inside the unlocked container.

(g) Since there is a lesser degree of risk of compromise with key operated locks, they will be changed or rotated at a minimum of once every two years, and will be immediately replaced upon loss or compromise of their keys.

(2) Section 1386 of Title 18, United States Code, makes unauthorized possession of keys, key–blanks, key–ways or locks adopted by any part of the Department of Defense for use in the protection of conventional arms, ammunition, or explosives, special weapons, and classified equipment, a criminal offense punishable by fine or imprisonment for up to 10 years, or both.

7–5. Procurement of New Storage Equipment

a. New security storage equipment will be procured from those items listed on the GSA Federal Supply Schedule. Exceptions can be made by the MACOM commander, will be fully justified, and will be reported to DAMI–CH, who must notify the Office of the Secretary of Defense (ASD(C31)) of the details of the exception.

b. As stated in paragraph 7–4a(3) above, new lock–bar containers used to store classified material will not be fabricated from either existing or new cabinets, and existing lock–bar containers will be phased out and no longer authorized for use after 1 October 2002.

c. Nothing in this Chapter will be construed to modify existing federal supply class management assignments made under DODD 5030.47.

7–6. Residential storage

Classified information will not be stored in a personal residence, on or off a military installation. Classified information will not be stored in any location outside an approved location at a U.S. Government or cleared contractor facility. Exceptions are:

a. In extreme and exceptional situations, a MACOM commander, or the Administrative Assistant to the Secretary of the Army for HQDA activities, can approve the temporary storage of SECRET and CONFIDENTIAL material only, in a personal residence, either on or off a military installation, or in another location that is not a U.S. Government or cleared contractor facility. This authority will not be further delegated. A validated operational requirement must exist for consideration of such requests and requests will not be approved for personal convenience. Authorization for such temporary storage must be in writing and will include written procedures for the protection of the information. The material will be stored in a GSA–approved security container and protected with an intrusion detection (alarm) system (IDS). Other methods of supplemental control can be used in place of an IDS, where the other methods provide substantially the same assurance of protection. Physical security standards, beyond the requirement for storage in a GSA–approved security container protected with an IDS, will be determined by the approving official.

b. The Secretary of the Army is the only DA official that can authorize the removal of TOP SECRET information and/or material from designated work areas for temporary storage outside a government or cleared contractor facility, to include the storage at a personal residence on a government facility. MACOM commanders can authorize the removal SECRET, and below, information and/or material from designated work areas for temporary storage outside a government or cleared contractor facility, to include the storage at a personal residence on a government facility. Where such approval is granted, to temporarily store classified information and/or material outside a designated work area at a government or cleared contractor facility, a GSA–approved security container will be furnished for storage. The container will be protected by an (IDS) as prescribed in section III of this Chapter, and written procedures addressing the appropriate protection of the information will be provided to the holder of the material. Other methods of supplemental control can be used in place of an IDS where the other methods provide the same assurance of protection. As a minimum, the written procedures concerning the storage of any level of classified information, will require the material to be under personal control, of the authorized individual, at all times when it is not secured in a GSA–approved security container. Also included will be the identification and signature receipt of the material temporarily stored, the reconciliation of the material upon its return, and the requirement that the material be returned as soon as possible after the operational requirement has ended. All authorizations, irrespective of classification level of material involved, will specify a specific expiration date.

c. Classified discussions are not permitted in personal residences, in public, in public transportation conveyances (airplane, taxi, etc.), or in any area outside approved spaces on a U.S. Government or cleared contractor facility. As an exception to this policy, and in certain situations requiring immediate contact and discussion of classified information in off–duty hours, the installation of a secure telephone unit (such as STU–III) can be authorized in personal residences to the extent that MACOM policy permits, up to, and including, the SECRET level. Only the SECARMY is authorized to permit TOP SECRET communications and document storage in personal residences. This will not be authorized for personal convenience. Where such units are permitted, care must be exercised in ensuring that unauthorized personnel, to include family members, are not within hearing distance when classified discussions take place, and that the control key for the unit is either personally retained or stored in a discrete location separate from the unit. In such cases, it can be necessary for the custodian of the unit to make notes regarding the classified discussion that occurs over the security telephone. Where this occurs, such classified notes can be retained in the personal residence only until the next duty day. If the next duty day falls during a period of more than one day, leave, Temporary Duty (TDY), or other absence, the material will be delivered for storage to a U.S. Government or cleared contractor facility prior to such absence. While in a personal residence, such classified notes will be safeguarded and under the personal, physical control of the authorized, cleared holder of the notes, at all times.

7–7. Safeguarding of U.S. Classified Information Located in Foreign Countries

Except for classified information released to a foreign government or international organization, and under the safeguarding of that country or organization, U.S. classified material will be retained in foreign countries only when necessary to satisfy specific U.S. Government requirements. Commanders will take into consideration the additional risk associated with storing, discussing, and processing classified information outside the United States in establishing procedures to implement this regulation. Particular attention will be paid to the foreign release requirements of AR 380–10, making sure that classified material is not accessed by foreign personnel not authorized access to the information, keeping classified holdings to the minimum required, making sure that classified material no longer required is frequently and completely destroyed, making sure that classified discussions and processing are protected from unauthorized access from personnel working in the area, that classified discussions are conducted on secure communications equipment, and requiring that the emergency destruction plan is rehearsed and is practical for execution. U.S. classified material in foreign countries will be stored at:

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

b. A U.S. Government activity located in a building used exclusively by U.S. Government tenants, provided the building is under 24–hour control by U.S. Government and U.S. citizen personnel.

c. A U.S. Government activity located in a building not used exclusively by 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 and U.S. citizen personnel.

d. 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 authorized U.S. personnel have access. The room or area will be secured with a 3–position dial combination lock meeting Federal Specification FF–L–2740A (electro–mechanical lock). MACOMs can approve the use of an existing non–FF–L–2740A lock until the lock meeting Federal Specification FF–L–2740A is installed.

7–8. Equipment Designations and Combinations

a. There will be no external mark revealing the level of classified information authorized to be stored in a given container or vault. Priorities for emergency evacuation and destruction will not be marked or posted on the exterior of storage containers, vaults, or secure rooms. For identification and/or inventory purposes, each vault or container will bear, externally, an assigned number or symbol not relating to any known security markings. This, along with the SF 702 and the "OPEN–CLOSED" or "OPEN–LOCKED" signs, are the only items permitted on the exterior of the security container. The top of the security container will not be used as a "bookshelf" or paper storage area. Storage of various non–authorized items on the top of storage containers, could lead to classified material being inadvertently left unsecured and/or mixed in with other miscellaneous material.

b. Combinations to security containers, vaults, and secure rooms will be changed only by individuals assigned that responsibility in writing (for example, the command security manager) and the appropriate security clearance. Combinations will be changed:

(1) When placed in use.

(2) Whenever an individual knowing the combination no longer requires access.

(3) When the combination has been subject to possible compromise.

(4) At least once annually.

(5) When taken out of service. When taken out of service, built–in combination locks will be reset to the standard combination 50–25–50; combination padlocks will be reset to the standard combination 10–20–30.

(6) Annually, per U.S. Central Registry, when NATO information is stored in the security container, vault, or secure room.

c. A record will 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) will be used for this purpose. A current record for all security containers, vault doors, and padlock combinations will be kept on SF 700.

(1) 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.

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

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

(4) 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 is not required. Because of the design of the SF 700, 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).

(5) 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.

d. The combination of a container, vault or secure room used for the storage of classified information will be treated as information having a classification equal to the highest classification level of the classified information to be stored inside. Such written records are classified and will be stored in containers approved for the storage of classified information, at the appropriate classification level, at the next higher headquarters. Written records of combinations will not be personally retained in wallets, purses, briefcases, desk drawers, on calendars or note pads, or written "in code" or foreign languages and stored in unapproved locations.

e. Access to the combination of a vault or container used for the storage of classified information will be granted only to those individuals who are authorized access to the classified information that is to be stored inside.

f. Entrances to secure rooms or areas, will be either under visual control at all times during duty hours, to preclude entry by unauthorized personnel, or the entry will be equipped with electric, mechanical, or electro–mechanical access control devices to limit access during duty hours. Section III, of this Chapter, provides standards for these access control devices. Electronically actuated locks (for example, cipher and magnetic strip card locks) and other such locking devices used primarily for duty–hours access control do not afford by themselves the required degree of protection for classified information and must not be used either during or after duty hours as a substitute for the locks prescribed in paragraph 7–4b.

7–9. Repair of Damaged Security Containers

Neutralization of lock–outs, or repair of any damage, that affects the integrity of a security container approved for storage of classified information, will be accomplished only by authorized persons who have been the subject of a trustworthiness determination, in accordance with AR 380–67, or are continuously escorted while so engaged.

a. With the exception of frames bent through application of extraordinary stress, a GSA–approved security container manufactured prior to October 1991 (identified by a silver GSA label with black lettering affixed to the exterior of the container) is considered to have been restored to its original state of security integrity as follows:

(1) All damaged or altered parts, for example, the locking drawer, drawer head, or lock, are replaced.

(2) The safe has been drilled immediately adjacent to or through the dial ring to neutralize a lock–out, a replacement lock meeting FF–L–2740A is used, 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 will remain at each end of the rod a willow recess not less than ⅛–inch nor more than &frac316;–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 must 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.

b. In the interests of cost efficiency, the procedures identified in subparagraph a(2) above, should not be used for GSA–approved security containers purchased after October 1991, distinguished by a silver GSA label with red lettering affixed to the outside of the container control drawer, until it is first determined whether warranty protection still applies. To make this determination, it will be necessary to contact the manufacturer and provide the serial number and date of manufacture of the container. If the container is under warranty, a lockout will be neutralized using the procedures described in the Federal Standard FED–STD–809 (Neutralization and Repair of GSA Approved Containers), dated 1 April 1998.

c. Unapproved modification or repair of security containers and vault doors is considered a violation of the container or door's integrity and the GSA label will be removed. Thereafter, these safes will not be used to protect classified information except as otherwise authorized in this regulation.

d. For technical assistance concerning classified material physical security storage standards, commands can contact the Interagency Advisory Committee on Security Equipment (IACSE). The designated DA representatives to the

IACSE, Security Equipment and Locking Systems (SEALS) subcommittee can be reached through the Army Intelligence Materiel Activity, Intelligence Materiel Management Center, Fort George G. Meade, MD 20755–5315.

7–10. Maintenance and Operating Inspections

MACOMs will establish procedures concerning repair and maintenance of classified material security containers, vaults, and secure rooms, to include a schedule for periodic maintenance. The following guidelines pertain to spotting repair and maintenance problems that will be addressed outside the regular maintenance schedule.

a. Security containers are usually serviceable for at least 25 years, if properly maintained. The life span of the container 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 their early stages, and definite symptoms can warn of a developing problem. Users should be alert for these symptoms, and if any of them are detected, the users should immediately contact their supporting maintenance activity for help. It is important to 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 depended upon to open again. Should that occur, the user can be faced with a lockout.

b. Users should watch for the following signs of trouble:

(1) A dial that is unusually loose or difficult to turn.

(2) Any jiggling movement in the dial ring. This is often detected when a twist motion is applied to the dial.

(3) Difficulty in dialing the combination or opening the container. Examples are:

(a) The need to dial the combination more than once, when human error is not at fault.

(b) The need to dial on numbers that are slightly above or below the correct number in the combination.

(4) Difficulty with the control drawer or other drawers. Examples are:

(a) Drawers rubbing against container walls. This can be caused if the container is not leveled, or the tracks or cradles are not properly aligned.

(b) 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.

(5) Difficulty in locking the control drawer. Examples are:

(a) The control drawer handle or latch will not return to the locking position when the drawer is shut.

(b) On Sargent and Greenleaf (S&G) or other similar 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 zero.

(c) The locking bolts move roughly, slip, or drag, or the linkage is burred or deformed.

c. Commands will periodically remind users of containers about the above guidelines.

7–11. Turn–in or Transfer of Security Equipment

In addition to having combinations reset before turn–in (see paragraph 7–8b(5)), 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 make sure that all papers and other material are removed and that the container is completely empty. Vaults, secure rooms, incinerators, shredders, or other classified material destruction devices, as well as the rooms in which they are located, will be thoroughly inspected to make sure that no classified material remains. A written, signed record certifying that this inspection has been accomplished and that no classified material remains, will be furnished to the command security manager and filed for two years.

Section III
Physical Security Standards

7–12. General

This section provides the general construction standards for areas approved for the open storage of classified information, general standards for intrusion detection (alarm) systems (IDS) used in areas in which classified information is stored, access control standards, and priorities for the replacement of locks on security containers. Classified material will be stored to the maximum extent feasible in GSA–approved security containers. Open storage areas will only be approved when storage in other approved security containers is not feasible due to the size, shape, or volume of material stored.

7–13. Vault and Secure Room (Open Storage Area) Construction Standards

a. Vault.

(1) Floor and Walls Eight inches of concrete reinforced to meet current standards. Walls are to extend to the underside of the roof slab above.

(2) Roof Monolithic reinforced concrete slab of thickness to be determined by structural requirements, but not less than the floors and walls.

(3) Ceiling The roof or ceiling must be reinforced concrete of a thickness to be determined by structural requirements, but not less than the floors and walls.

(4) Door and Frame Vault door and frame unit will conform to Federal Specification AA–D–2757 Class 8–vault door, or Federal Specification AA–D–600 Class 5 vault door.

b. Secure room

(1) *Floor, Walls, and Roof.* The walls, floor, and roof construction of secure rooms must be of permanent construction materials, i.e., plaster, gypsum wallboard, metal panels, hardboard, wood, plywood, or other materials offering resistance to, and evidence of, unauthorized entry into the area. Walls will be extended to the true ceiling and attached with permanent construction materials, with mesh or 18 gauge expanded steel screen.

(2) *Ceiling.* The ceiling will be constructed of plaster, gypsum, wallboard material, hardware, or other similar material that the command security manager judges to be of equivalent strength.

(3) *Doors.* The access door to the room will be substantially constructed of wood or metal. The hinge pins of out–swing doors will be pinned, brazed, or spot–welded to prevent removal. The access door will be equipped with a built–in GSA–approved combination lock meeting Federal Specification FF–L–2740A. For open storage areas approved under previous standards, the lock can be the previously approved GSA combination lock. However, upon retrofit, the door must be fitted with a lock meeting Federal Specification FF–L–2740A (See paragraph 7–21 for priorities for replacement of such locks). Doors, other than the access door, will be secured from the inside. For example, by using a dead bolt lock, panic dead bolt lock, or rigid wood or metal bar which extends across the width of the door, or by any other means that will prevent entry from the outside. Key operated locks that can be accessed from the exterior side of the door are not authorized.

(4) *Windows.* Windows which are less than 18 feet above the ground when measured from the bottom of the window, or are easily accessible by means of objects directly beneath the windows, will be constructed from or covered with materials which will provide protection from forced entry. The protection provided to the windows need be no stronger than the strength of the contiguous walls.

(5) *Openings.* Utility openings, such as ducts and vents, will be kept at less than a person–passable, 96 square inches, opening. Openings larger than 96 square inches will be hardened in accordance with Military Handbook 1013/1A, which provides guidance to ensure that appropriate physical security considerations are included in the design of facilities.

7–14. Intrusion Detection System Standards

a. An Intrusion Detection System (IDS), often referred to as an alarm, must detect an unauthorized penetration in the secured area. An IDS complements other physical security measures and consists of the following:

(1) Intrusion Detection Equipment (IDE).

(2) Security forces.

(3) Operating procedures.

b. System functions. IDS components operate as a system with the following four distinct phases:

(1) Detection.

(2) Communications.

(3) Assessment

(4) Response.

c. These elements are equally important, and none can be eliminated if an IDS is to provide an acceptable degree of protection.

(1) Detection. The detection phase begins as soon as a detector or sensor reacts to stimuli it is designed to detect. The sensor alarm condition is then transmitted over cabling located within the protected area to the Premise Control Unit (PCU). The PCU may service many sensors. The PCU, and the sensors it serves, comprise a “zone” at the monitor station. This will be used as the definition of an alarmed zone for purposes of this regulation.

(2) Reporting. The PCU receives signals from all sensors in a protected area and incorporates these signals into a communication scheme. Another signal is added to the communication for supervision, to prevent compromise of the communication scheme by tampering or injection of false information by an intruder. The supervised signal is sent by the PCU through the transmission link to the monitor station. Inside the monitor station either a dedicated panel or central processor monitors information from the PCU signals. When an alarm occurs, an annunciator generates an audible and visible alert to security personnel. Alarms result normally from intrusion, tampering, component failure, or system power failure.

(3) Assessment The assessment period is the first phase that requires human interaction. When alarm conditions occur, the operator assesses the situation and dispatches the response force, as necessary.

(4) Response The response phase begins as soon as the operator assesses an alarm condition. A response force must immediately respond to all alarms. The response phase must also determine the precise nature of the alarm and take all measures necessary to safeguard the secure area.

7–15. Selection of equipment

a. As determined by the commander, and in accordance with the minimum standards established by this regulation, all areas that reasonably afford access to the container, or where classified data is stored, are to be protected by IDS unless continually occupied. Prior to the installation of an IDS, commanders, or their designated personnel, will consider the threat, the vulnerabilities, and any in–depth security measures, and will perform a risk analysis to determine if IDS is appropriate to the situation.

b. Acceptability of Equipment. All IDE must be UL–listed, or equivalent, and approved by the Department of the Army or authorized U.S. Government contractor. Government installed, maintained, or furnished systems are acceptable.

7–16. IDS Transmission

a. Transmission Line Security. When the transmission line leaves the facility and traverses an uncontrolled area, Class I or Class II line supervision will be used.

(1) *Class I.* Class I line security is achieved through the use of Data Encryption Standard (DES) or an algorithm based on the cipher feedback or cipher block chaining mode of encryption. Certification by the National Institute of Standards (NIST) or another independent testing laboratory is required.

(2) *Class II.* Class II line supervision refers to systems in which the transmission is based on pseudo random generated tones or digital encoding using an interrogation and response scheme throughout the entire communication, or UL Class AA line supervision. The signal will not repeat itself within a minimum six–month period. Class II security will be impervious to compromise using resistance, voltage, current, or signal substitution techniques.

b. Internal Cabling. The cabling between the sensors and the PCU must be dedicated to the IDS and must comply with national and local code standards.

c. Entry Control Systems. If an entry control system is integrated into an IDS, reports from the automated entry control system must be subordinate in priority to reports from intrusion alarms.

d. Maintenance Mode. When an alarm zone is placed in the maintenance mode, the condition will be signaled automatically to the monitor station. The signal must appear as an alarm or maintenance message at the monitor station and the IDS will not be securable while in the maintenance mode. The alarm or message must be continually visible at the monitor station throughout the period of maintenance. A standard operating procedure will be established to address appropriate actions when maintenance access is indicated at the panel. All maintenance periods will be archived in the system. A self–test feature will be limited to one second per occurrence.

e. Annunciation of Shunting or Masking Condition. Shunting or masking of any internal zone or sensor must be appropriately logged or recorded in archive. A shunted or masked internal zone or sensor must be displayed as such at the monitor station throughout the period the condition exists whenever there is a survey of zones or sensors.

f. Indications. Indications of alarm status will be revealed at the monitoring station and optionally within the confines of the secure area.

g. Power Supplies Primary power for all IDE will be commercial AC or DC power. In the event of commercial power failure at the protected area or monitor station, the equipment will change power sources without causing an alarm indication.

(1) Emergency Power Emergency power will consist of a protected independent backup power source that provides a minimum of 4 hours operating power battery and/or generator power. When batteries are used for emergency power, they will be maintained at full charge by automatic charging circuits. The manufacturers periodic maintenance schedule will be followed and results documented.

(2) Power Source and Failure Indication An illuminated indication will exist at the PCU of the power source in use (AC or DC). Equipment at the monitor station will indicate a failure in power source, a change in power source, and the location of the failure or change.

h. Component Tamper Protection IDE components located inside or outside the secure area will be evaluated for a tamper protection requirement. If access to a junction box or controller will enable an unauthorized modification, tamper protection will be provided.

7–17. System Requirements

a. Independent Equipment When many alarmed areas are protected by one monitor station, secure room zones, areas in which classified information is stored, must be clearly distinguishable from the other zones to ensure a priority response. All sensors will be installed within the protected area.

b. Access and/or Secure Switch and PCU No capability is to exist to allow changing the access status of the IDS from a location outside the protected area. All PCUs must be located inside the secure area and are to be located near the entrance. Only assigned personnel will initiate changes in access and secure status. Operation of the PCU can be restricted by the use of a device or procedure that verifies authorized use. In the secure mode, any unauthorized entry into the space will cause an alarm to be transmitted to the monitor station.

c. Motion Detection Protection Secure areas that reasonably afford access to the container or where classified data is stored, are to be protected with motion detection sensors, e.g., ultrasonic and/or passive infrared. Use of dual

technology is authorized when one technology transmits an alarm condition independently from the other technology. A failed detector will cause an immediate and continuous alarm condition.

d. Protection of Perimeter Doors Each perimeter door will be protected by a Balanced Magnetic Switch (BMS) that meets the standards of UL 634.

e. Windows All readily accessible windows (within 18 feet of ground level) will be protected by an IDS, either independently or by the motion detection sensors in the space.

f. IDS Requirements for Continuous Operations Facility A continuous operations facility may not require an IDS. This type of secure area should be equipped with an alerting system if the occupants cannot observe all potential entrances into the room. Duress devices could also be required depending upon the situation.

g. False and/or Nuisance Alarm Any alarm signal transmitted in the absence of detected intrusion, or identified as a nuisance alarm, is a false alarm. A nuisance alarm is the activation of an alarm sensor by some influence for which the sensor was designed, but which is not related to an intrusion attempt. All alarms will be investigated and the results documented. The maintenance program for the IDS must make sure that incidents of false alarms do not exceed one in a period of 30 days per zone.

7–18. Installation, Maintenance and Monitoring

a. IDS Installation and Maintenance Personnel Alarm installation and maintenance will be accomplished by U.S. citizens who have been subjected to a trustworthiness determination, in accordance with AR 380–67 (See also DODD 5200.2–R).

b. Monitor Station Staffing The monitor station is to be supervised continuously by U.S. citizens who have been subjected to a trustworthiness determination in accordance with the regulations noted in subparagraph a, above.

7–19. Access Controls While Material is Not Secured in Security Containers

This section applies to open storage areas such as vaults and secure rooms. It can also apply, at the MACOM's option, to other areas of security interest, such as areas in which significant amounts of classified material or especially sensitive material are routinely accessed. This section does not apply to open storage of SAPs material. See appendix I and AR 380–381 regarding open storage of SAPs material and information.

a. The perimeter entrance will be under visual control at all times during working hours so as to deny entry to unauthorized personnel. This can be accomplished by several methods, such as an employee work station, guard, closed circuit television (CCTV), or a day access combination lock when there are persons present in the area but the entrance is not under visual control. Regardless of the method used, an access control system will be used on the entrance. Note: Uncleared persons will be escorted within the facility by a cleared person, who is familiar with the security procedures at the facility, and an announcement, either auditory or visual, will be used to alert others of the uncleared person's presence.

b. An automated entry control system (AECS) can be used to control admittance during working hours instead of visual or other methods of control. That AECS must meet the criteria stated below. Further guidance can be obtained from IACSE, SEALS subcommittee, at Fort Meade, MD (see paragraph 7–9d for contact information). The automated entry control system must identify an individual and authenticate the person's authority to enter the area through the use of one of the following:

(1) ID Badges or Key Cards The identification (ID) badge or key card must use embedded sensors, integrated circuits, magnetic stripes, or other means of encoding data that identifies the facility and the individual to whom the card is issued.

(2) Personal Identity Verification Personal identity verification (biometrics devices) identifies the individual requesting access by some unique personal characteristic, such as:

(a) Fingerprinting.

(b) Hand geometry.

(c) Handwriting.

(d) Retina scans.

(e) Voice recognition. A biometrics device can be particularly appropriate for access to areas in which highly sensitive information is located.

c. In conjunction with subparagraph (2), above, a personal identification number (PIN) can be required. The PIN must be separately entered into the system by each individual using a keypad device and will consist of four or more digits, randomly selected, with no known or logical association with the individual. The PIN must be changed or discontinued when it is believed to have been compromised, subjected to compromise, or the individual no longer requires access.

d. Authentication of the individual's authorization to enter the area must be accomplished within the system by inputs from the ID badge/card, the personal identity verification device, or the keypad with an electronic database of individuals authorized to enter the area. Procedures will be established, in writing, for removal of the individual's authorization to enter the area upon reassignment, transfer, or termination, or when the individual's access is suspended, revoked, or downgraded to a level lower than the required access level.

e. Protection must be established and maintained for all devices or equipment which constitute the entry control system. The level of protection can vary depending upon the type of device or equipment being protected. This can be accomplished by the following:

(1) Location where authorization data and personal identification or verification data is entered or inputted, stored, or recorded, is protected.

(2) Card readers, keypads, communication or interface devices located outside the entrance to a controlled area will have tamper resistant enclosures and be securely fastened to the wall or other permanent structure. Control panels located within a controlled area will require only a minimal degree of physical security protection sufficient to preclude unauthorized access to the mechanism.

(3) Keypad devices will be designed or installed in such a manner that an unauthorized person in the immediate vicinity cannot observe the selection of input numbers.

(4) Systems that use transmission lines to carry access authorizations, personal identification data, or verification data between devices or equipment located outside the controlled area will have line supervision (see paragraph 7–16 for explanation of line supervision).

(5) Electric strikes used in access control systems will be of heavy duty, industrial grade.

f. Access to records and information concerning encoded ID data and PINs will be restricted. Access to identification or authorizing data, operating system software or any identifying data associated with the entry control system will be limited to the fewest number of personnel as possible. Such data or software will be kept secure when unattended.

g. Records will be maintained reflecting active assignment of ID badge/card, PIN, level of access, and similar system–related records. Records concerning personnel removed from the system will be retained for 90 days. Records of entries will be retained for at least 90 days or until any investigations of system violations and incidents have been investigated, resolved and recorded.

h. Personnel who are the first to enter or last to leave an area will be required to secure the entrance or exit point. Authorized personnel who permit another individual to enter the area are responsible for confirmation of clearance, need–to–know, and access. Commanders can approve the use of standardized AECS which meet the criteria specified below. MACOMs and the Administrative Assistant to the Secretary of the Army, for HQDA activities, can approve deviations to these standards, based upon compensatory measures that provide a commensurate level of assurance of access control. Criteria for standardized AECS is as follows:

(1) For a Level 1 key card system, the AECS must provide a .95 probability of granting access to an authorized user providing the proper identifying information within three attempts. In addition, the system must ensure an unauthorized user is granted access with less than 0.05 probability after three attempts to gain entry have been made.

(2) For a Level 2 key card and PIN system, the AECS must provide a .97 probability of granting access to an authorized user providing the proper identifying information within three attempts. In addition, the system must ensure an unauthorized user is granted access with less than .010 probability after three attempts to gain entry have been made.

(3) For a Level 3 key card and PIN and biometrics identifier system, the AECS must provide a .97 probability of granting access to an unauthorized user providing the proper identifying information within three attempts. In addition, the system must ensure an authorized user is granted access with less than .005 probability after three attempts to gain entry have been made.

i. Electric, Mechanical, or Electromechanical Access Control Devices. Electric, mechanical, or electromechanical devices which meet the criteria stated below, may be used to control admittance to secure areas during duty hours, if the entrance is under visual or other command approved system of control by cleared authorized personnel located in the area. These devices are also acceptable to control access to selected or otherwise compartmented areas within a secure area. Nothing in this statement is intended to modify the policy stated in AR 380–28 for the protection of sensitive compartmented information. Access control devices will be installed in the following manner:

(1) The electronic control panel containing the mechanical mechanism by which the combination is set is to be located inside the area. The control panel, located within the area, will require only minimal degree of physical security designed to preclude unauthorized access to the mechanism.

(2) The control panel will be installed in such a manner, or have a shielding device mounted, so that an unauthorized person in the immediate vicinity cannot observe the setting or changing of the combination.

(3) The selection and setting of the combination will be accomplished by an individual cleared at the same level as the highest classified information controlled within.

(4) Electrical components, wiring included, or mechanical links (cables, rods and so on) should be accessible only from inside the area, or, if they traverse an uncontrolled area they should be secured within protecting covering to preclude surreptitious manipulation of components.

7–20. Minimum standards for deviations to construction standards for open storage areas

Where deviations to the general open storage areas, vaults and strong rooms, are approved by the MACOM or the Administrative Assistant to the Secretary of the Army, for HQDA activities, the following standards, as a minimum,

will be satisfied and the areas will be certified as being designed to sufficiently deter, detect, or delay entry, to unauthorized persons from gaining access to the classified information stored therein.

a. Construction: The perimeter walls, floors, and ceiling will be permanently constructed and attached to each other. All construction will be done in a manner as to provide visual evidence of unauthorized penetration.

b. Doors: Doors will be constructed of wood, metal, or other solid material. Entrance doors will be secured with a built–in GSA approved three–position combination lock. Other doors will be secured from the inside with either a combination lock, panic hardware, a dead bolt, or a rigid wood or metal bar which extends across the width of the door. Any door that permits entry from the outside must be secured with a GSA approved three position built–in combination lock. In unusual circumstances in which a built–in combination lock is not feasible, the designated official can approve a GSA approved three–position combination padlock. Where such padlocks are used, they will be secured in a security container or approved open storage area or kept in the locked position on the hasp during hours in which the area is opened. Key operated or cipher locks are not permitted on any door that provides access from the exterior of the open storage area.

c. Vents, Ducts, and Miscellaneous Openings: All vents, ducts, and similar openings in excess of 96 square inches, and/or over six inches in its smallest dimension, that enter or pass through an open storage area, will be protected with either bars, expanded metal grills, or an intrusion detection system. Sound baffles will be used if classified discussions occur in an area in which the sound carries outside the range of authorized personnel.

d. Windows:

(1) All windows which might reasonably afford visual observation of classified activities within the facility will be made opaque or equipped with blinds, drapes, or other coverings.

(2) Windows at ground level will be constructed from or covered with materials which provide protection from forced entry. The protection provided to the windows will be as strong as the strength of the contiguous walls.

(3) Approved open storage areas which are located within an Army command, located on an Army installation or other Army controlled compound, may eliminate the requirement for forced entry protection if the windows are made inoperable either by permanently sealing them or equipping them on the inside with a locking mechanism. In either situation, sealing or locking, the windows must be covered by an IDS, either independently or by the motion detection sensors within the area.

e. IDS. An IDS must be used (see standards in paragraph 7–12) to provide complete coverage of the entire open storage area. Minimum response time for any area storing classified information is contained in paragraph 7–4a. Locations outside the United States and all areas that store information which is of special risk of theft or espionage, or in areas of high risk, must seriously consider reducing the minimum response time.

Section IV
Lock Replacement Priorities

7–21. Priorities for Replacement of Locks

All newly purchased GSA approved security containers are equipped with the electromechanical GSA–approved combination lock meeting Federal Specification FF–L–2740A. New purchases of combination locks for GSA–approved security containers, vault doors and secure rooms will conform to Federal Specification FF–L–2740A. Existing mechanical combination locks that do not meet this specification will not be repaired. If they do fail, they will be replaced with locks meeting FF–L–2740A. Army commands will be advised by HQDA of the policy concerning the retrofitting of existing security containers with the new electromechanical locks meeting Federal Specification FF–L–2740A. This section contains the recommended general priorities for the lock retrofit program (See figure 7–1). In accordance with the Army Intelligence Materiel Activity (AIMA), it is to be implemented upon notification, or as command funds become available and upgrading of locks is assessed as a component of the command security program. Where individual situations are assessed as requiring a modification to the general priorities, they can be made at command option, unless otherwise instructed by HQDA. An individual situation could include a risk assessment of such factors as amount of material held, sensitivity of the information, threat to the information, environment in which the container is located, and depth of other security features that control access to the container or area. Priorities range from 1 to 4, with 1 being the highest and 4 the lowest.

Lock Replacement Priorities

In the United States and Its Territories

ITEM	TS/SAPs	TS	S/SAPs		S-C
Vault Doors	1	1	3[1]	4[1]	
Containers (A)*		3[2]	4[2]	4[2]	4[2]
Containers (B)**		1	1	1	2
Crypto1	1	2	2		

Outside the United States and Its Territories

ITEM	TS/SAPs	TS	S/SAPs		S-C
Vault Doors	1	1	2[1]	2[1]	
Containers (A)*		2	2	3[2]	3
Containers (B)**		1	1	1	2[2]
Crypto1	1	2[2]	2[2]		
High Risk Areas		1	1	1	1

*A - Located in a controlled environment where the Department of the Army, or other element of the Department of Defense, has the authority to prevent unauthorized disclosure of classified information. The command can control or deny access to the space, post guards, require identification, challenge presence, inspect packages, program elevators, or take other reasonable measures necessary to deny unauthorized access.

**B - Located in an uncontrolled area without the perimeter security measures identified in *A, above.

---

[1] If the vault door lock is the only GSA approved three-position combination lock that secures the material, the priority will be designated as 1. A lower priority is assigned based on command assessment in situations in which the material is secured in an approved container with a GSA approved three position combination lock that is located within the vault.

[2] The higher priority will be used at command option based upon a weighing of the factors involved, such as: the sensitivity of the material stored, volume of material, threat to the information, and environment in which the container is located.

Figure 7-1. Lock Replacement Priorities

Chapter 8
Transmission and Transportation

Section I
Methods of Transmission and Transportation

8–1. Policy
Classified information will be transmitted and transported only as specified in this Chapter. COMSEC information will be transmitted in accordance with AR 380–40. Special Access Programs material will be transmitted and transported in accordance with appendix I of this regulation, AR 380–381, and applicable SAPs procedure guides. Commands will establish local procedures to meet the minimum requirements to minimize risk of compromise while permitting use of the most effective transmission or transportation means. External, street side, collection boxes, for instance, U.S. Mail boxes, will not be used for the dispatch of classified information. Commands will develop procedures to protect incoming mail, bulk shipments, and items delivered by messenger, until a determination is made whether classified information is contained therein. Screening points will be established to limit access of classified information to only cleared personnel.

8–2. TOP SECRET Information
TOP SECRET information will be transmitted only by:

a. A cryptographic system authorized by the Director, NSA, or a protected distribution system designed and installed to meet approved NSA standards. This applies to voice, data, message, and facsimile transmissions.

b. The Defense Courier Service (DCS) (see DODD 5200.33–R).

c. Authorized command courier or messenger services.

d. The Department of State Diplomatic Courier Service.

e. Cleared U.S. military personnel and U.S. Government civilian employees, traveling by surface transportation, or traveling on a conveyance owned, controlled, or chartered by the U.S. Government or DOD contractors.

f. Cleared U.S. military personnel and U.S. Government civilian employees on scheduled commercial passenger aircraft.

g. Cleared DOD contractor employees within and between the United States and its territories, when the transmission has been authorized, in writing, by the appropriate Cognizant Security Agency (CSA), or a designated representative. For DA contractors, the CSA is generally the Defense Security Service (DSS).

8–3. SECRET information
SECRET information can be transmitted by:

a. Any of the means approved for the transmission of TOP SECRET information.

b. U.S. Postal Service registered mail, within and between the 50 States, the District of Columbia, and the Commonwealth of Puerto Rico.

c. U.S. Postal Service express mail, within and between the 50 States, the District of Columbia, and the Commonwealth of Puerto Rico. The "Waiver of Signature and Indemnity" block on the U.S. Postal Service express mail label 11–B, will not be executed under any circumstances. The use of external, street side, express mail collection boxes is prohibited.

d. U.S. Postal Service registered mail, through Army, Navy, or Air Force Postal Service facilities, for instance, APO/FPO, outside the United States and its territories, so 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. United States Postal Service and Canadian registered mail, with registered mail receipt between U.S. Government and Canadian Government installations in the U.S. and Canada.

f. As an exception, in urgent situations requiring next–day delivery, an overnight or next–day delivery service, that is a current holder of a GSA contract for overnight delivery of material for the Executive Branch, provided that the delivery service is U.S. owned and operated and provides automated in–transit tracking of the material. These companies are not required to be cleared and generally are to be considered uncleared. Their employees are not cleared and are not required to be U.S. citizens, and the companies are not required to meet the storage requirements contained in this regulation. For the purpose of this section of the regulation, an urgent situation exists when the classified material must be received by the next day, there is no other authorized means to make the delivery, excluding the

handcarrying by authorized personnel, the delivery company assures delivery by the required date, and the transmission complies with the provision of Title 39, U.S. Code (USC), section 320.6, Postal Services, as amended. The sender will comply with the requirement contained in paragraph 8–10, to address the package to the command or activity, and not address it to an individual. Since delivery services usually require the building number and name of recipient, the sender will contact the recipient to ensure that an authorized and appropriately cleared person will be available to sign for the material, and they will verify the authorized address to make sure that it is displayed correctly on the package label. Unless it is not possible, for example, if the material is needed on a weekend and the mailroom is not in operation then, the package label will be addressed to a supporting mailroom. The release signature block on the receipt label will not be executed under any circumstances. Executing the release signature block, ensures that someone, but not necessarily the addressee, if the addressee is unavailable when the package is delivered, signs for the package. These precautions are required because uncleared, commercial overnight delivery services can deliver the package directly to the person named, and building identified, on the label, or to whomever signs for the material, if the addressee is unavailable when the material is delivered. U.S. Postal Service mail is delivered or picked–up by a centralized command mailroom where personnel who open mail are cleared and the material is properly safeguarded until opened. The use of external, street side, commercial delivery service collection boxes is prohibited. Note: In many situations, the United States Postal Service express mail can meet the next day delivery standards and should be used, as noted in subparagraph c, above.

g. Carriers authorized to transport SECRET information by way of a Protective Security Service (PSS) under the National Industrial Security Program (NISP). This method is authorized only within the United States boundaries when other methods are impractical.

h. Appropriately cleared contractor employees, provided that the transmission meets the requirements specified in DODD 5220.22–R and DODD 5220.22–M (NISPOM).

i. U.S. Government and U.S. Government contract vehicles, including aircraft, ships of the U.S. Navy, civil service–operated U.S. Navy ships, and ships of United States 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 will protect the shipment at all times, through personal observation or authorized storage, to prevent inspection, tampering, pilferage, or unauthorized access. Observation of the shipment is not required during flight or sea transit, provided it is loaded into a compartment that is not accessible, to any unauthorized persons, or in a specialized secure, safe–like container. The escort will, if possible, observe the loading of the shipment.

8–4. CONFIDENTIAL information

CONFIDENTIAL information may be transmitted by:

a. Means approved for the transmission of SECRET information. However, U.S. Postal Service registered mail will be used for CONFIDENTIAL material only as indicated below:

(1) NATO CONFIDENTIAL information. If NATO CONFIDENTIAL material is sent between U.S. Government activities, within the Continental United States, its territories, and the District of Columbia, it can be sent by first class mail. The caveat, "POSTMASTER: RETURN SERVICE REQUESTED" will be affixed to the outer wrapper.

(2) Other CONFIDENTIAL material sent to and from FPO or APO addressees, located outside the U.S. and its territories.

(3) Other CONFIDENTIAL material when the originator is uncertain that the addressee's location is within U.S. boundaries or knows the addressee's location is outside U.S. boundaries.

b. United States Postal Service certified mail (or registered mail, if required above) for material addressed to DOD contractors or non–DOD agencies.

c. United States Postal Service first class mail between DOD component locations anywhere in the U.S., its territories, and the District of Columbia. The use of external, street side, postal collection mailboxes is prohibited. The outer envelope or wrappers will be endorsed, where possible, in letters larger than the text on the address of the envelope: "POSTMASTER: RETURN SERVICE REQUESTED."

d. Within United States boundaries, commercial carriers that provide a Constant Surveillance Service (CSS).

e. In the custody of commanders or masters of ships of United States registry, who are United States citizens. CONFIDENTIAL information shipped on ships of U.S. registry, cannot pass out of United States control. The commanders or masters must sign a receipt for the material 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.

(2) Maintain control of the cargo until a receipt is obtained from an authorized representative of the consignee.

8–5. NATO restricted material

NATO restricted material can be transmitted within the United States and to designated APO/FPO addresses, by U.S. first class mail, single wrapped with a notation on the envelope, "POSTMASTER: RETURN SERVICE REQUESTED." When to or from areas outside the United States and APO/FPO addresses, NATO restricted material will be sent, double–wrapped, to NATO addressees through United States or NATO member postal systems.

Section II
Transmission of Classified Material to Foreign Governments

8–6. General

Classified information or material approved for release to a foreign government, in accordance with AR 380–10, will be transferred between authorized representatives of each government in compliance with the provisions of this Chapter. Each contract, agreement, or other arrangement, that involves the release of classified material to foreign entities, will either contain detailed transmission instructions, or require that a separate transportation plan be approved, by the appropriate security and transportation officials and the recipient government, prior to release of the material. Transportation plan requirements are outlined in paragraph 8–7h. (See DOD TS–5105.21–M–2 for further guidance regarding SCI.)

8–7. Procedures

a. Classified information or material to be released directly to a foreign government representative will be delivered or transmitted only to a person who has been designated in writing by the recipient government to sign for and assume custody and responsibility on behalf of said government (referred to as the designated government representative). This written designation will 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. The foreign government can designate a freight forwarder as their representative for receipt of freight.

b. Classified material that is suitable for transfer by courier or postal service, in accordance with this regulation, and which cannot be transferred directly to a foreign government's designated representative, will be transmitted to:

(1) An embassy, consulate, or other official agency of the recipient government having extraterritorial status in the United States.

(2) A U.S. embassy or a U.S. military organization in the recipient country or in a third–party country for delivery to a designated representative of the recipient government.

c. The shipment of classified material as freight by truck, rail, aircraft, or ship, will be in compliance with the following:

(1) Army officials authorized to approve a Foreign Military Sales (FMS) transaction that involves the delivery of U.S. classified material to a foreign purchaser will, at the beginning of negotiations or consideration of a proposal, consult with DOD transportation authorities (Military Traffic Management Command, Military Sealift Command, Air Mobility Command, as appropriate) to determine whether secure shipment from the CONUS point of origin to the ultimate foreign destination is feasible. Normally, the U.S. will use the Defense Transportation System (DTS) to deliver classified material to the recipient government. A transportation plan will be developed by the shipper that prepares the Letter of Offer in coordination with the purchasing government. MACOM security officials, of the MSC or agency that prepares the Letter of Offer, will evaluate and approve the transportation plan, and may delegate this authority as they deem necessary. This does not, however, relieve the MACOM of the ultimate responsibility for oversight.

(2) Classified shipments resulting from direct commercial sales must comply with the same security standards that apply to FMS shipments. To develop and obtain approval of the required transportation plan, defense contractors will consult with the purchasing government and the Defense Security Service Regional Security Office prior to signing of a commercial contract that will result in the shipment of classified material.

(3) Delivery of classified material to a foreign government at a point within the U.S., its territories, or its possessions, will be accomplished at:

(a) An embassy, consulate, or other official agency under the control of the recipient government.

(b) The 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 agency official who transfers custody will make sure the recipient is aware of secure means of onward movement of the classified material to its final destination, consistent with the approved transportation plan.

(c) A military or commercial port of embarkation (POE) that is a recognized point of departure from the U.S., its territories or possessions, for on–loading aboard a ship, aircraft, or other carrier. In these cases, the transportation plan will provide for U.S. controlled secure shipment to the CONUS transshipment point and the identification of a secure storage facility, either government or commercial, at or near the POE. An agency official authorized to transfer custody is to supervise or observe the on–loading of the FMS material being transported, when physical and security custody of the material has yet to be transferred formally to the foreign recipient. In the event that the transfer of physical security

and custody cannot be accomplished promptly, the agency official will make sure that the classified material is either returned to a secure storage facility of the U.S. shipper, segregated and placed under constant surveillance of a duly cleared U.S. security force at the POE, or held in the secure storage facility designated in the transportation plan.

(d) An appropriately cleared freight forwarder facility identified by the recipient government as its designated representative. 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.

d. Delivery outside the United States, its territories, or possessions:

(1) Classified U.S. material to be delivered to a foreign government within the recipient country, will be delivered on arrival in the recipient country to a U.S. Government representative, who will 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 can be delivered directly to the recipient government's designated representative upon arrival.

(2) Classified material to be delivered to a foreign government representative within a third country will be delivered to an agency or installation of the U.S., 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 will be designated locally to receive the shipment upon arrival and deliver it to the recipient government's designated representative.

e. Overseas shipments of U.S. classified material will be made only via ships, aircraft, or other carriers that are owned, or chartered by the U.S. Government or under U.S. registry, owned or chartered by, or under the registry of, the recipient government, or otherwise authorized by the head of the command or agency having classification jurisdiction over the material involved. Overseas shipment of classified material will be escorted, prepared for shipment, packaged, and stored, onboard as prescribed elsewhere in this regulation, DODD 5220.22–R, and DODD 5220.22–M.

f. Only freight forwarders that have been granted an appropriate security clearance by the DOD or the recipient government are eligible to receive, process related security documents, 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 classified material, and is not required to perform security–related functions, will not be cleared.

g. Foreign governments can return classified material to a U.S. contractor for repair, modification, or maintenance. At the time the material is initially released to the foreign government the approved methods of return shipment will be specified in the Letter of Offer and Acceptance (LOA) for Foreign Military Sales, the security requirements section of a direct commercial sales contract, or in the original transportation plan. The contractor, upon notification of a return shipment, will give advance notice of arrival to the applicable user agency or the Defense Security Service, and arrange for secure inland shipment within the U.S. if such shipment has not been prearranged.

h. Transportation plan requirements are as follows:

(1) Preparation and coordination is as follows:

(a) Foreign Military Sales. U.S. classified material to be furnished to a foreign government or international organization under FMS transactions, will normally be shipped via the Defense Transportation System and delivered to the foreign government within its own territory. The U.S. Government can permit other arrangements for such shipments when it determines that the recipient foreign government has its own secure facilities and means of shipment from the point of receipt to ultimate destination. In any FMS case, the agency or command having security cognizance over the classified material involved is responsible, in coordination with the foreign recipient, for developing a transportation plan. When the point of origin is a U.S. contractor facility, the contractor and Defense Security Service will be provided a copy of the plan by the agency or command.

(b) Commercial transactions. The contractor will prepare a transportation plan for each commercial contract, subcontract, or other legally binding arrangement providing for the transfer of classified freight to foreign governments, to be moved by truck, rail, aircraft, or ship. The requirement for a transportation plan applies to U.S. and foreign contracts.

(c) The transportation plan will describe arrangements for secure shipment of the material from the point of origin to the ultimate destination. It must identify recognized points of embarkation from the U.S., its territories, or possessions for transfer to a specified ship, aircraft, or other authorized carrier. It must identify a government or commercial secure facility in the vicinity of the points of embarkation and debarkation that can be used for storage if transfer or onward movement cannot take place immediately. Except as described in paragraph 8–7d, a U.S. Government official authorized to transfer custody and control, must supervise the on–loading of classified material when the material has yet to be officially transferred. The plan must provide for security arrangements in the event custody cannot be transferred promptly.

(d) Upon transfer of title to the purchasing foreign government, classified material can be delivered to a freight forwarder that is designated, in writing, by the foreign government, as its representative for that shipment, and is cleared to the level of the classified material to be received. The freight forwarder will be provided a copy of the transportation plan and agree to comply.

(2) The transportation plan will, as a minimum, will include—

(a) A description of the material to be shipped and a brief narrative description indicating where and under what circumstances transfer of custody will occur.

(b) Identification, by name and title, of the designated representative (or alternate) of the recipient government or international organization who will receipt for and assume security responsibility for the classified material.

(c) Identification and specific location(s) of delivery point(s) and security arrangements while the material is located at the delivery points.

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

(e) Identification of any storage or processing facilities and transfer points to be used, certification that such facilities are authorized by competent government authority to receive, store, or process the level of classified material to be shipped, and a description of security arrangements while the material is located at the facilities.

(f) Routes and, if applicable, security arrangements for overnight stops or delays enroute.

(g) Arrangements for dealing with port security and customs officials.

(h) The identification, by name or title, of couriers, escorts, or other responsible officials (e.g. Captain or Crew Chief) to be used, including social security number, government identification or passport number, security clearance, and details concerning their responsibilities.

(i) Description of the shipping methods to be used and the identification of the foreign or domestic carriers.

(j) Description of packaging requirements, seals and storage during shipment.

(k) A requirement for the recipient government or international organization to examine shipping documents upon receipt of the classified material in its own territory and notify DSS or the agency or command having security cognizance over the classified material if the material has been transferred enroute to any carrier not authorized by the transportation plan.

(l) Requirement for the recipient government or international organization to inform DSS or the agency or command having security cognizance over the classified material promptly and fully of any known or suspected compromise of classified material.

(m) Arrangements for return shipments if necessary for repair, modification or maintenance.

8–8. Shipment of freight

Where applicable, commands will establish procedures for shipment of bulk classified material as freight, to include provisions for shipment in closed vehicles, when required, appropriate notice to the consignee concerning the shipment, procedures at transshipment activities, and action to be taken in case of non–delivery or unexpected delay in delivery. DA Form 1965 (Delivery and Pick Up Service) may be used as a manifest for delivery by courier or messenger of sealed containers. The Top Secret and Secret contents will have an attached receipt form to be completed by the recipient and returned to the originator.

Section III
Preparation of Material for Transmission

8–9. Envelopes or containers

a. When classified information is transmitted, it will be enclosed in two opaque, sealed envelopes, wrappings, or containers, durable enough to properly protect the material from accidental exposure and to ease in detecting tampering. The following exceptions apply:

(1) If the classified material is an internal component of a packageable item of equipment, the outside shell or body can 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, the outside or body of the item can be considered to be a sufficient enclosure provided observation of it does not reveal classified information.

(3) If the classified material is an item or piece of equipment that is not easily packageable and the shell or body is classified, it will be concealed with an opaque covering that will hide all classified features.

(4) Specialized shipping containers, including closed cargo transporters, can be considered the outer wrapping or cover when used.

(5) When classified material is handcarried outside an activity, a locked briefcase can serve as the outer wrapper. In such cases, the addressing requirements for the outer wrapper, as stated in paragraph 8–10a, below, do not apply.

(6) NATO restricted material does not have to be double–wrapped when it is transmitted within the United States. The marking "NATO RESTRICTED" will not appear on the outermost wrapper.

b. Classified material will be prepared for shipment, packaged, and sealed in ways that minimize the risk of accidental exposure or undetected deliberate compromise. Documents will be packaged so that the classified text is not in direct contact with the inner envelope or container. For documents that do not have an unclassified cover or cover

transmittal letter or form, this can be accomplished by inserting an opaque sheet or cardboard sheet on top of the classified text in the inner envelope.

8–10. Addressing

a. The outer envelope or container for classified material will be addressed to an official government activity or to a DOD contractor with a facility clearance and appropriate storage capability. It will show the complete return address of the sender. The outer envelope will not be addressed to an individual. Office codes or phrases such as "Attention: Research Department" may be used.

b. The inner envelope or container will show the address of the receiving activity, the address of the sender, the highest classification of the contents, including, where appropriate, any special markings such as "RESTRICTED DATA" or "NATO," and any other special instructions. The inner envelope may have an "attention line" with a person's name.

c. The outer envelope or single container will not bear a classification marking or any other unusual marks that might invite special attention to the fact that the contents are classified.

d. Classified information intended only for U.S. elements of international staffs or other organizations, must be addressed specifically to those elements.

8–11. Mail channels with the Department of Energy

Other federal government agencies can require special certification or special procedures before forwarding classified information to another agency. Where that is the case, DA commands will comply with the requirements of those agencies. Specifically, the Department of Energy (DOE) requires that a "mail channel" be established prior to the transmission of certain classified information from a DOE facility to another activity. The mail channel, or material channel for transmission of material other than mail, will be certified by a designated DA certification official, will be made on DOE Form 5631.20 and will include the certified classified mailing address. The certification official will be one of the officials authorized to sign DOE Form 5631.20. See paragraph 6–17, of this regulation, for policy on personnel authorized to sign the DOE Form 5631.20. The DOE Form 5631.20 replaced DOE Form DP–277. It is recommended that the DOE facility that holds the material be contacted for the proper address and information to be completed on the form. Unless notified to the contrary by the DOE facility, the mail or material channel may not exceed one year, subject to renewal of the form.

Section IV
Escort or Handcarrying of Classified Material

8–12. General provisions

a. Appropriately cleared personnel may be authorized to escort or handcarry classified material between locations when other means of transmission or transportation cannot be used. Handcarrying of classified material will be limited to situations of absolute necessity and will be carried out to make sure it does not pose an unacceptable risk to the information. Generally, two–way handcarrying, carrying the material both to and from the destination, is not authorized unless specific justification has been provided and both situations involving the handcarrying meet the requirements stated in this section. Handcarrying will be authorized only when:

(1) The information is not available at the destination and is required by operational necessity or a contractual requirement.

(2) The information cannot be sent by a secure facsimile transmission or by other secure means, for example, U.S. Postal Service express mail.

(3) The handcarry has been authorized by the appropriate official. For handcarrying within and between the United States, its territories, and Canada, the authorizing official will be determined by the commander, subject to MACOM approval. For all other areas, approval is at the MACOM level and can be further delegated in writing by the MACOM. Where delegated, the MACOM will exercise oversight, during inspections and/or assistance visits, by requiring copies of approvals, or by other means, to ensure the requirements of this section are met.

(4) The handcarry is accomplished aboard a U.S. carrier, or a foreign carrier if no U.S. carrier is available, and the information will remain in the custody and physical control of the U.S. escort at all times.

(5) Arrangements have been made for secure storage during overnight stops and similar periods. The material will not be kept in hotels, personal residences, vehicles, or any other unapproved storage location.

(6) A receipt for the material, for all classification levels, is obtained from an appropriate official at the destination and the receipt is returned to the appropriate official at the traveler's command.

b. Many of the principles contained in paragraph 8–14, of this regulation, apply to all situations involving the handcarrying of classified information and are not restricted to those situations involving classified material handcarried outside the United States. Commands will consider the principles stated in paragraph 8–13 in developing command

procedures concerning the handcarrying of classified material and incorporate those that are deemed applicable to the handcarrying of classified material within the United States.

8–13. Documentation

a. Responsible officials will provide a written statement to all individuals escorting or carrying classified material authorizing such transmission.

b. The DD Form 2501 (Courier Authorization Card) may be used to identify appropriately cleared DA personnel who have been approved to handcarry classified material in accordance with the following, except that in the case of travel aboard commercial aircraft, the provisions of paragraph 8–15 of this regulation apply:

(1) The individual has a recurrent need to handcarry classified information;

(2) The form is signed by an appropriate official in the individual's servicing security office;

(3) Stocks of the form are controlled to preclude unauthorized use.

(4) The form is issued for no more than two years at a time. The requirement for authorization to handcarry will be reevaluated and/or revalidated on at least an biennial basis, and a new form issued, if appropriate.

(5) The use of the DD Form 2501 for identification and/or verification of authorization to handcarry Sensitive Compartmented Information or Special Access Programs information, will be in accordance with policies and procedures, established by the official having security responsibility for such information or programs.

8–14. Security requirements for temporary duty travel outside the United States

a. As stated above, the handcarrying of classified information is not a routine method of transmission and will only be approved when fully justified. Handcarrying classified material outside the United States subjects the information to increased risk. When classified material is handcarried, for delivery to a foreign government representative, or when classified information is discussed with, or otherwise disclosed to, foreign national personnel, the requirements of AR 380–10 will be strictly followed.

b. The DOD requires that a request for travel outside the United States contain a written statement by the traveler that classified information will or will not, as applicable, be disclosed during the trip. If the foreign disclosure of classified information is involved, there will be an additional written statement that disclosure authorization has been obtained in accordance with DODD 5230.11. For DA commands, AR 380–10 applies. The statement also will specify whether authorization has been obtained to carry classified material, in compliance with the provisions of this regulation.

c. If the traveler has been authorized to carry classified material, a copy of the written authorization will accompany the justification for the temporary duty travel (TDY). This authorization, the courier orders, will be provided by the traveler's Special Security Officer (SSO) or Command Security Manager (CSM). They will be kept in a secure place and will not be presented unless circumstances dictate.

d. Because of Operations Security (OPSEC) concerns, Block 16 of DD Form 1610 (Request and Authorization for TDY Travel of DOD Personnel) will not contain statements that identify the traveler as carrying classified information.

e. Travelers who are authorized to carry classified material on international flights, or by surface conveyance if crossing international borders, must have courier orders. The DD Form 2501 is not a valid form of courier authorization for travel overseas. A memorandum on command letterhead is required and will, as a minimum, provide the information specified in subparagraph (11), below. Travelers will be informed of, and acknowledge, their security responsibilities. The latter requirement may be satisfied by a briefing or by requiring the traveler to read written instructions that, as a minimum, contain the information listed below.

(1) The traveler is liable and responsible for the material being escorted.

(2) Throughout the journey, the classified material will stay in the personal possession of the traveler, except when it is in authorized storage.

(3) The material will not be opened en route except in the circumstances described in subparagraph (9), below.

(4) The classified material is not to be discussed or disclosed in any public place.

(5) The classified material is not, under any circumstances, to be left unattended. During overnight stops, U.S. military facilities, embassies, or cleared contractor facilities will be used. Classified material will not be stored in vehicles, hotel rooms or safes, personal residences, or any other unauthorized storage facility or location.

(6) The traveler will not deviate from the authorized travel schedule, unless such deviation is beyond the traveler's control, such as cancellation of a flight. The traveler will immediately notify their command of any delays.

(7) In cases of emergency, the traveler will take appropriate measures to protect the classified material, and will notify their command as soon as possible.

(8) The traveler is responsible for ensuring that personal travel documentation, such as passport, courier authorization, and medical documents, etc., are complete, valid, and current.

(9) There is no assurance of immunity from search by the customs, police, and/or immigration officials of the various countries whose border the traveler may be crossing. Therefore, should such officials inquire into the contents of the consignment, the traveler will present the courier orders and ask to speak to the senior customs, police and/or immigration official. This action should normally suffice to pass the material through unopened. However, if the senior

customs, police, and/or immigration official demands to see the actual contents of the package, it should be opened only in his/her presence, and must be done in an area out of sight of the general public, if possible. If the traveler is permitted to pass, notification to his/her command will be done at the earliest possible time.

(a) Precautions must be taken to show officials only as much of the contents as will satisfy them that the package does not contain any other item. The traveler should ask the official to repack or assist in repackaging of the material immediately upon completion of the examination.

(b) The senior customs, police, and/or immigration official, should be requested to provide evidence of the opening and inspection of the package, by sealing and signing it when closed, and confirming on the shipping documents, if any, or courier certificate, that the package has been opened.

(c) If the package has been opened under such circumstances as those mentioned above, the traveler will inform, in writing, the addressee and the dispatching security officer of this fact.

(10) Prior to travel, classified material to be carried by a traveler will be inventoried and a copy of the inventory retained by the traveler's security office. A copy of the inventory will be placed inside the classified package.

(11) Travel orders (DD Form 1610) will identify the traveler by name, title, organization, and include the traveler's passport or identification number. The travel orders will describe the route to be taken by the traveler, the traveler's itinerary can be attached for this purpose; describe the package to be carried by size, weight, and configuration, but will not contain statements that identify the package as containing classified material; reflect a date of issue and expiration; and contain the name, title, and telephone number of an appropriate official, within the traveler's command, who may be contacted to verify the authorization to escort classified material. Courier orders will contain this same information, in addition to a complete description of the material that is to be carried and expiration of authorization to carry the material. Where possible, the courier authorization should show the phone number of the U.S. embassy or consulate, closest to the area that the traveler will enter the country, in case the assistance of the U.S. State Department is needed in clearing customs. As an alternative, the courier orders should show the name and phone number of a point of contact at the activity located in the foreign country that is to be visited. Courier orders will be signed by the official authorizing the handcarrying of classified material.

(12) Upon return, the traveler will return all classified material, in a sealed package, or produce a receipt, signed by the security officer of the addressee organization, for any material that is not returned.

f. For guidance on handcarrying NATO information, travelers who are authorized to carry NATO classified material on international flights will refer to AR 380–15.

8–15. Handcarrying or escorting classified material aboard commercial passenger aircraft

a. Airport and aircraft operating and security procedures make handcarrying and escorting classified material on commercial passenger aircraft a complex task. Advance coordination with appropriate authorities is essential. See figure 8–1 for listings of the Federal Aviation Administration (FAA) Air Transportation Security Field Offices. During this coordination, specific advice should be sought regarding the nature of documentation that is required. Generally, the following has been found to meet requirements:

(1) The individual designated as courier will be in possession of a DOD military ID card (DD Form 2, (Armed Forces of the United States Geneva Convention Identification Card)) or civilian ID card, or contractor–issued identification card, that includes 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.

(2) The courier will have the original of the authorization letter. A reproduced copy is not acceptable. The traveler will have sufficient authenticated copies to provide a copy to each airline involved. The letter will be prepared on letterhead stationary of the agency authorizing the carrying of classified material and will—

(a) Give the full name of the individual and his or her employing agency or company.

(b) Describe the type of identification the individual will present, for example, Naval Research Laboratory Identification Card N0. 1234; ABC Corporation Identification Card No. 1234.

(c) Describe the material being carried, for example three sealed packages, 9' × 8' × 24', addressee and addresser.

(d) Identify the points of departure, destination, and known transfer(s).

(e) Carry a date of issue and expiration.

(f) Carry the name, title and signature, of the official issuing the letter. Each package or carton to be exempt will be signed on its face by the official who signed the letter.

(g) Carry the name of the person designated to confirm the letter of authorization, and that person's official U.S. Government telephone number.

b. The traveler should process through the airline ticketing and boarding procedure the same as other passengers. The package or the carry–on luggage containing it should be routinely offered for inspection for weapons.

8–16. Consignor/consignee responsibility for shipment of bulky material

The consignor of a bulk shipment will—

a. 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 that 200 pounds in closed vehicles only.

c. Notify the consignees and military transshipping activities of the nature of the shipment, including level of classification, the means of shipment, the serial number of the 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.

d. Advise the first military transshipping activity that, in the event the material does not move on the conveyance originally anticipated, the transshipping activity should advise the consignee with information of the firm date and estimated time of arrival. Upon receipt of the advance notice of a shipment of classified material, consignees and transshipping activities will take appropriate steps to receive the classified shipment and to protect it upon arrival.

e. Annotate the bills of lading to require the carrier to notify the consignor immediately, by the fastest means, if the shipment is unduly delayed in route. Such annotations will 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 POSIBLE AND IMMEDIATELY NOTIFY CONSIGNOR AND CONSIGNEE."

f. 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 the transshipping activity. Upon receipt of such notice, the consignor will immediately trace the shipment. If there is evidence that the classified material was subjected to compromise, the procedures set forth in chapter 10 of this regulation for reporting compromises will apply.

Federal Aviation Administration (FAA) Air Transportation Security Field Offices

City	State
Anchorage	Alaska
Atlanta	Georgia
Baltimore	Maryland
Boston	Massachusetts
Chicago (O'Hare)	Illinois
Cleveland	Ohio
Dallas	Texas
Denver	Colorado
Detroit	Michigan
Honolulu	Hawaii
Houston	Texas
Kansas City	Missouri
Las Vegas	Nevada
Los Angeles	California
Miami	Florida
Minneapolis	Minnesota
Newark	New Jersey
New Orleans	Louisiana
New York (John F. Kennedy)	New York
New York (La Guardia)	New York
Philadelphia	Pennsylvania
Pittsburgh	Pennsylvania
Portland	Oregon
Saint Louis	Missouri
San Antonio	Texas
San Diego	California
San Francisco	California
San Juan	Puerto Rico
Seattle	Washington
Tampa	Florida
Tucson	Arizona
Washington (Dulles)	Washington, D.C.
Washington (National)	Washington, D.C.

Figure 8-1. Federal Aviation Administration (FAA) Air Transportation Security Field Offices

Chapter 9
Security Education

Section I
Policy

9–1. General policy
Commanders will establish security education programs. These programs will be aimed at promoting quality performance of security responsibilities by command personnel, and will be tailored, as much as possible, to the specific involvement of individuals in the information security program and the command's mission. The programs will—

a. Provide necessary knowledge and information to enable quality performance of security functions.

b. Promote understanding of information security program policies and requirements, and their importance to the national security.

c. Instill and maintain continuing awareness of security requirements and the intelligence collection threat.

d. Assist in promoting a high degree of motivation to support program goals.

9–2. Methodology
Security education must be a continuous, rather than periodic, influence on individual security performance. Periodic briefings, training sessions, and other formal presentations will be supplemented with other informational and promotional efforts to ensure maintenance of continuous awareness and performance quality. The use of job performance aids and other substitutes for formal training, for example, video tapes or self–paced computer programs, can be used when they are determined to be the most effective means of achieving program goals. The circulation of directives or similar material on a "read–and–initial" basis will not be considered as fulfilling any of the specific requirements of this Chapter, because there is no basis to gauge effectiveness.

Section II
Briefings

9–3. Initial orientation
All DA personnel, especially those who could be expected to play a role in the information security program, will be given an initial orientation. The purpose of the orientation will be:

a. To ensure personnel are aware of the roles they are expected to play in the information security program;

b. The importance of their fulfilling their responsibilities; and

c. That they have enough information to fulfill those responsibilities.

9–4. Cleared personnel
a. All personnel, especially those granted access or are expected to be granted access to classified information, will be provided an initial orientation to the information security program before being allowed access to any classified or sensitive information. The initial orientation is intended to:

(1) Produce a basic understanding of the nature of classified information and the importance of its protection to the national security;

(2) Place employees on notice of their responsibility to play a role in the security program; and

(3) Provide them enough information to ensure proper protection of classified/sensitive information in their possession. Security educators will, as a minimum, include the following points in their Security Education Programs:

(a) The nature of U.S. and foreign government classified and sensitive information, its importance to the national security, and the degree of damage associated with each level of classification/sensitivity.

(b) How to recognize U.S. and foreign government classified and sensitive information that personnel may encounter, including markings, etc.

(c) The individual's responsibility for protection of classified and sensitive information, and the consequences of failing to do so.

(d) Procedures and criteria for authorizing access to classified and sensitive information.

(e) Procedures for safeguarding and control of classified and sensitive information in the individual's work environment.

(f) Proper reaction to discovery of information believed to be classified/sensitive in the public media.

(g) The security management and support structure within the command, to include sources of help with security problems and questions and proper procedures for challenging classifications believed to be improper.

(h) Penalties associated with careless handling or compromise of classified/sensitive information. See chapter 10 for extracts from the espionage laws and federal statutes for details.

b. Before being granted access to classified information, employees must sign SF 312. See paragraph 6–2 of this regulation, for details regarding the use of the SF 312.

9–5. Briefing upon refusal to sign the NDA, SF 312

Chapter 6 of this regulation contains the policy on the execution of the Classified Information Nondisclosure Agreement (NDA)(SF 312). Individuals who refuse to sign the form will be advised of the following:

a. Execution of the NDA is mandatory for all military and civilian personnel as a condition of access to classified information.

b. The purpose of the NDA is to make sure each individual authorized access to classified information is aware of the duties and responsibilities imposed by law and to ensure that the individual understands the personal commitment to protect classified information.

c. The NDA does not impose any obligation beyond those prescribed by law to protect classified information.

d. In the interests of national security, classified information will be disclosed only to those individuals who are committed personally to protecting such information, have a valid need–to–know, and who have been granted access to classified information. Any individual who shows a reluctance to sign an NDA will be considered to have a lack of personal commitment to protect classified information.

e. An individual who refuses to sign the NDA will not be granted access to classified information. That individual will be granted a period of time, not to exceed 5 calendar days, to re–evaluate their decision. If the individual refuses to sign the NDA at the end of that 5–day period, that individual will be advised that the foregoing action will require termination of their present and future access to classified information. In addition, the individual will be advised that the reluctance to sign the NDA may place their security clearance in jeopardy.

f. There is no prohibition against the individual consulting with an attorney in this matter. However, the individual will be advised that such consultation will be at no additional expense to the government nor will it extend the 5–day re–evaluation time limit.

9–6. Briefing uncleared personnel

Personnel who are not cleared for access to classified information will be included in the security education program. Especially if they will be working in situations where inadvertent access to classified information might occur or they will have access to unclassified/sensitive information which might be of value to intelligence collectors. They will be provided with a brief explanation of the nature and importance of classified and sensitive information and actions they should take if they discover classified information unsecured, note an apparent security vulnerability, or believe they have been contacted by an intelligence collector or other unauthorized individual seeking to gain access to sensitive government information. Security training for all DA personnel is the command's responsibility. Security education training is useful in the understanding of why official information must be protected and, therefore, inclusion of uncleared personnel in certain aspects of the security education program is essential.

9–7. Refresher briefing

Security education programs will include efforts to maintain and reinforce quality performance of security responsibilities. As a minimum, all DA employees, especially those who have access to, create, process, or handle classified/sensitive information, will be provided refresher training in their responsibilities at least once a year. The actual frequency and nature of continuing security education must be determined by the needs of, and outlined in, the command's information security program and the nature of the command personnel involvement in the program. As a minimum, all personnel will receive annual refresher training that reinforces the policies, principles, and procedures, covered in initial and specialized training. Refresher training will also address the threat and the techniques employed by foreign intelligence activities attempting to obtain classified information, and advise personnel of penalties for engaging in espionage activities. Refresher training should also address issues or concerns identified during unit self–inspections. Whenever security policies and procedures change, personnel, whose duties would be impacted by these changes, must be briefed as soon as possible.

9–8. Foreign travel briefing

a. Although foreign travel (personal or official) may be briefly discussed during annual refresher briefings, it is also a requirement to attend a separate foreign travel briefing for all active and reserve soldiers pending travel outside the U.S. and its territories. This is especially true for those that travel frequently. It is in the best interest of the traveler, as well as the command, to ensure the traveler is fully prepared for any particular security or safety concerns that their travel to foreign areas may introduce.

b. A foreign travel briefing used to be only offered to those individuals who had access to classified information. AR 525–13 requires that all DA military and civilian personnel pending travel outside the U.S. and its territories or possessions must attend the Antiterrorism/Force Protection (AT/FP) Level I awareness training, prior to departure from their current duty station. Training must be received within 6 months of departure date to the overseas area. It is the

commander's responsibility to ensure all DA military and civilain personnel are scheduled for and receive this training prior to their departure. All DA military and civilian personnel will not outprocess or depart on PCS, TDY, TCS, leave, or pass to an overseas area without AT/FP training.

c. Upon request, an unclassified version may be given to dependents or others who do not have access. For updated information, regarding foreign travel, contact your command security manager or the U.S. State Department. Examples of briefings and country specific information are available on the State Department's unclassified Internet website at http://www.state.gov/. Individuals with SCI access should be referred to their SSO for foreign travel briefing requirements.

d. Upon return, the traveler should be provided the opportunity to report any incident to their command security manager, no matter how insignificant, that could have security implications.

Section III
Special Requirements

9–9. General policy

DA personnel in positions which require performance of specified roles in the information security program will be provided security education sufficient to permit quality performance of those duties. The training will be provided before, concurrent with, or not later than six months following assumption of those positions.

9–10. Original classifiers

a. Officials who have been granted original classification authority will be educated in their responsibilities before they exercise the delegated authority. They will be provided an understanding of:

(1) The difference between original and derivative classification and the circumstances in which each is appropriate.

(2) Requirements, standards and criteria for original classification of information.

(3) Prohibitions and limitations on classification.

(4) The process and standards for determining duration of classification.

(5) Requirements for creation and maintenance of classification guides.

(6) Agency procedures for challenging classification, and the responsibilities of the original classification authority in responding to challenges.

(7) Declassification decision–making regarding information classified under previous Executive Orders, EO 12958 and amendments, DODD 5200.1–R, and previous editions of this regulation, including mandatory and systematic declassification review.

(8) Aspects of marking, controlling and the safeguarding of classified information (including requirements for automated systems) which could affect classification and declassification decision–making.

(9) Requirements and procedures for safeguarding foreign government information.

b. Security educators may consider the use of job aids or similar techniques, for example, video tapes or self–paced computer training programs, to replace or supplement traditional educational techniques, due to the relatively low frequency of training for original classification authorities. The Defense Security Service Academy may be contacted for advice in obtaining training aids. They can be found on the Internet at http://www.dss.mil/training.

c. DOD Handbook 5200.1–PH can be used as a reference by original classification authorities and personnel that assist these officials. Many of the basic principles of making an original classification decision have not changed since the publication of the handbook, and it may be useful both as a training aid for newly designated original classification authorities, as a reference in making original classification decisions, and developing command level security classification guides. Excerpts from this handbook appear as appendix G of this regulation.

9–11. Derivative classifiers

DA personnel whose responsibilities include derivative classification, will be trained in requirements and procedures appropriate to the information and material they will be classifying, including the proper use of classification guides and source documents. As a minimum, the training will address the following questions:

a. What are the original and derivative classification processes and the standards applicable to each?

b. What are the proper and complete classification markings to be applied to classified information?

c. What are the authorities, methods and processes for downgrading and declassifying information?

d. What are the methods for the proper use, storage, reproduction, transmission, dissemination and destruction of classified information?

e. What are the requirements for creating and updating classification and declassification guides?

f. What are the requirements for controlling access to classified information?

g. What are the procedures for investigating and reporting instances of actual or potential compromise of classified information and the penalties that may be associated with violation of established security policies and procedures?

h. What are the requirements for creating, maintaining, and terminating special access programs, and the mechanisms for monitoring such programs?

i. What are the procedures for the secure use, certification and accreditation of automated information systems and networks which use, process, store, reproduce, or transmit classified information?

j. What are the requirements for oversight of the security classification program, including self–inspections?

9–12. Security Program Management personnel

Security managers, security staff members, and others with significant responsibility for management of the information security program, will be trained/educated to fulfill their roles. The Defense Security Service Academy, formerly the Defense Security Institute (DSI), Baltimore Maryland, should be contacted for advice in obtaining training and/or training aids. They can be found on the Internet at http://www.dss.mil/training/. The training and education should be tailored to suit their expected contributions to the program, and will include at a minimum:

a. Procedures, standards, and processes for original and derivative classification, and for downgrading and declassifying information.

b. Proper marking of classified/sensitive documents and material.

c. Requirements and techniques for controlling access to classified/sensitive information, and for the proper use, storage, reproduction, transmission, transportation, dissemination and destruction of classified and sensitive material.

d. Procedures and requirements for responding appropriately to security violations and other security incidents.

e. Requirements and procedures for securing classified/sensitive information processed, maintained, or stored on automated information systems. It should be noted that command–wide responsibilities for the Information Systems Security (ISS) Program can be delegated to another official as specified in AR 380–19. The security manager and select security staff personnel will be educated in at least the basics of ISS to promote a seamless, integrated security program.

f. Requirements and methods for security education, program oversight, and program management.

9–13. Critical Nuclear Weapons Design Information Briefing

As stated in Chapter 6, DA personnel will be briefed on the sensitivity of Critical Nuclear Weapons Design Information (CNWDI) before access is granted. The following is an example of a sample briefing for CNWDI access, and it, or a version thereof, is suggested for use.

a. CNWDI is that TOP SECRET or SECRET Restricted Data that reveals the theory of operation or design of the components of a thermonuclear or implosion type fission bomb, warhead, demolition munition, or test device. Access to and dissemination of CNWDI is of particular concern to the Army. Because of its extreme sensitivity, access must be limited to the minimum number of persons.

b. You have been nominated for access to CNWDI, certified by the appropriate official as having the required "need–to–know" for that category of information, and determined to have an appropriate clearance for access to be granted.

c. Access to CNWDI entails additional responsibilities as well as special procedures. These are contained in AR 380–5, and include special access, dissemination, and marking requirements. It is particularly emphasized that CNWDI can only be disseminated to those individuals who have been fully authorized for access and have a verified need–to–know. If in doubt, check with (fill in appropriate name/office/telephone number).

d. Any questions regarding procedures governing access to, dissemination of, or safeguarding CNWDI are to be referred to (fill in appropriate name/office/telephone number).

9–14. Others

Commands will include in their security education programs, either in the general program or as part of special briefings to select personnel affected, provisions regarding special education and training for personnel who:

a. Use automated information systems to store, process, or transmit classified/sensitive information (see appendix E of this regulation and AR 380–19).

b. Will be traveling to foreign countries where special concerns about possible exploitation exist or will be attending professional meetings or conferences where foreign attendance is likely. The military intelligence unit providing counterintelligence support to the command, should be contacted for assistance and/or information in this regard.

c. Will be escorting, handcarrying, or serving as a courier for classified/sensitive material.

d. Are authorized access to classified and/or sensitive information requiring special control or safeguarding measures.

e. Are involved with international programs.

f. Regardless of clearance and/or access level held, all DA personnel will receive Subversion and Espionage Directed Against the U.S. Army (SAEDA) training, at a minimum of every two years, pursuant to Interim Change I01, AR 381–12.

Section IV
Termination Briefings

9–15. General Policy
DA commands will establish procedures to make sure that cleared employees, who leave the command or whose clearance is terminated, receive a termination briefing. See paragraph 6–5 of this regulation for more detailed policy on termination briefings. This briefing will—

a. Emphasize the individual's continued responsibility for protection of classified/sensitive information to which they have had access;

b. Provide instructions for reporting any unauthorized attempt to gain access to such information;

c. Advise the individual of the prohibition against retaining classified/sensitive material when leaving the organization; and

d. Remind them of the potential civil and criminal penalties for failure to fulfill their continuing responsibilities (see chap 10).

Section V
Program Oversight

9–16. General policy
DA commanders will ensure that their security education programs are appropriately evaluated during self–inspections and during oversight activities of subordinate commands or organizational units. This evaluation will include assessment of the quality and effectiveness of security education efforts, as well as ensuring appropriate coverage of the target populations. Commands will maintain a record of the programs offered and of the personnel that participated. These records will be maintained for two years and will be available for review during oversight inspections and assistance visits. These evaluations will also be included in block 9 of the SF 311 annual report.

Chapter 10
Unauthorized Disclosure and Other Security Incidents

Section I
Policy

10–1. General policy
a. The compromise of classified information can cause damage to our national security. Loss of classified material is just as serious. If classified material is lost, it cannot be determined if the information has been compromised. When loss or compromise of classified information happens, immediate action is required to minimize any damage and eliminate any conditions that might cause further compromises. To do this, prompt and effective investigation of the situation and prompt reporting of results are critical. Each incident in which classified information or material may have been lost or compromised must be the subject of a preliminary inquiry as described in this Chapter (See figure 10–1 for a sample preliminary inquiry). The purposes of this preliminary inquiry will be to:

(1) Determine whether classified information was compromised and, if so, whether there is damage to the national security.

(2) Determine what persons, situations, and/or conditions were responsible for or contributed to the incident.

b. The provisions of other Department of the Army regulations that require the investigation and reporting of counterintelligence (CI), criminal, or other serious incidents can also apply to incidents discussed in this Chapter. For example, AR 190–40, AR 195–2, AR 381–10, AR 381–12, AR 381–20, and any other Army regulations that implement DODI 5240.4. All applicable Army regulations will be followed in reporting and investigating these matters.

c. Incidents involving cryptographic information will be handled in accordance with National Communications Security Instruction (NACSI) 4006 (See AR 380–40). Details involving the use of DA Form 2134 (Security Violation Report(s)) for reporting COMSEC security violations, discussed in previous editions of this regulation, are covered in AR 380–40. Incidents involving SCI will be handled in accordance with DOD Manual 5105.21–M–1 (see AR 380–28). Incidents involving SAPs information will be handled in accordance with AR 380–381 (See appendix I for more information).

d. The Office of the Under Secretary of Defense (Policy), (USD(P)), will be notified of all losses or compromises of foreign government information. These reports will be made through command channels and DAMI–CH.

10–2. Reaction to discovery of incident

a. Anyone finding classified material out of proper control, will take custody of and safeguard the material, if possible, and immediately notify the appropriate security authorities. In all cases, the individual's immediate supervisor is to be notified.

b. Any person who becomes aware of the possible loss or compromise of classified information will immediately report it to the commander, the command security manager, or other official the commander may direct, for instance, a department head or office chief if indicated by the command security manual or other command directive. If the person believes that the commander, security manager, or other official designated to receive such reports may have been involved in the incident, the person making the discovery will report it to the security authorities at the next higher level of command or supervision.

c. If classified information appears in the public media, personnel will not make any statement or comment that would confirm the accuracy or verify the classified status of the information. See paragraph 4–2, of this regulation, for further guidance.

(1) It is essential that Army personnel are careful to neither confirm nor deny the existence of classified information or the accuracy of that information in the public media. Personnel will report such matters to the command security manager, or other official designated by the commander. The matter will then be reported to the original classification authority for the information.

(2) The news article or other medium will not be marked as classified, however, the written report detailing the discovery of the information in the public media will be classified to the level of the information believed to have been compromised. Personnel will not discuss the matter with anyone without the expressed consent of the command security manager, or an individual so designated by the command security manager or commander. An appropriate security clearance and need–to–know is required. No discussions will be made over non–secure circuits.

(3) If approached by a representative of the media who wishes to discuss information, personnel will neither confirm nor deny the accuracy of or the classification of the information, and will report the approach immediately to the appropriate command security and public affairs authorities.

d. Any incident in which the deliberate compromise of classified information or involvement of foreign intelligence agencies is suspected, will be reported to the command security manager and the supporting counterintelligence organization.

10–3. The preliminary inquiry

When an incident of possible loss or compromise of classified information is reported, the command will immediately initiate a preliminary inquiry into the incident. If the information was in the custody of another activity at the time of the possible compromise, that activity will be notified and will assume responsibility for the preliminary inquiry. This preliminary inquiry will be conducted according to these guidelines:

a. The person appointed to conduct the preliminary inquiry will have the appropriate security clearance, the ability and available resources to conduct an effective preliminary inquiry, and will not be likely to have been involved, directly or indirectly, in the incident. Except in unusual circumstances, the command security manager will not be appointed to conduct the preliminary inquiry. It is typically the responsibility of the security manager, unless command policy states otherwise, to make sure that an official is appointed to conduct the preliminary inquiry and to ensure that the preliminary inquiry is completed in accordance with this regulation and command policy and procedure. Advice and assistance may be requested from the supporting counterintelligence organization.

b. In cases of apparent loss of classified material, the person conducting the preliminary inquiry will ensure that a thorough search for the material has been conducted. Document the steps taken to locate the material.

c. The preliminary inquiry will focus on answering the following questions:

(1) When, where, and how did the incident occur? Exactly what happened?

(2) What specific classified information and/or material (to include foreign government information) was involved? What was the level of classification of the information?

(3) What persons, situations, or conditions caused or contributed to the incident?

d. Every preliminary inquiry into possible loss or compromise of classified information or material will include a judgment about whether any compromise did occur and what, if any, potential damage to national security has occurred. One of the following alternatives will be chosen:

(1) Compromise of classified information did not occur.

(2) Compromise of classified information may have occurred.

(3) Compromise of classified information did occur, but there is no reasonable possibility of damage to the national security. Note, the determinations about damage here, and in the following paragraph, are not "damage assessments" as discussed in paragraph 10–5. The determination to be made here is whether the circumstances of the incident are such, that the possibility of damage to the national security can be discounted.

(4) Compromise of classified information did occur and damage to the national security may result.

e. In cases of apparent unauthorized disclosure of classified information to the public media, the preliminary inquiry will include the following additional questions in order to determine if a leak investigation is warranted:

(1) What is the date and identity of the article disclosing classified information?

(2) What specific statements in the article are considered classified and whether the data was properly classified?

(3) If the data came from a specific document, what is the source document's origin, and the identity of the individual responsible for the security of the classified information disclosed?

(4) What is the extent of dissemination of the data?

(5) Has the information been previously officially released?

(6) Was prepublication clearance sought from proper authorities?

(7) Have portions of, or background data on, the material, been published officially or in the open press from which an educated speculation on the consolidated data is derived?

(8) Can the data be declassified or otherwise made available for prosecution and, if so, what is the identity of the person competent to testify concerning its classification?

(9) Had declassification been decided upon before the data was published?

(10) What is the effect the disclosure of the classified data would have on the national security?

(11) Is the disclosed classified data accurate?

f. If at any time, during the preliminary inquiry, it appears that deliberate compromise of classified information may have occurred, the situation will be immediately reported to the chain of command and supporting counterintelligence unit. Apparent violations of other criminal law will be reported to the supporting criminal investigative activity. Coordination with the command's legal counsel is recommended whenever it seems likely that administrative or other sanctions may be taken against someone because of the incident.

10–4. Reporting results of the preliminary inquiry

a. If the conclusion of the preliminary inquiry is as stated in paragraph 10–3d(2) or (4), (compromise could have occurred, or compromise did occur and damage to the national security can result) the official initiating the preliminary inquiry will immediately notify the originator of the information or material involved. If the originator was not the original classification authority, the OCA will also be immediately notified (see paragraph 10–5a, below). If the originator cannot be determined, the command's MACOM will be contacted for guidance. The MACOM will contact DAMI–CH, for those cases in which the MACOM cannot direct the command to the appropriate activity. Notification of the originator and original classification authority will not be delayed pending completion of any additional inquiry or resolution of other related issues.

b. If the conclusion of the preliminary inquiry is as stated in paragraph 10–3d(2) or (4), the command will report the matter through command channels to its MACOM, or to the Administrative Assistant to the Secretary of the Army (AASA) for offices and activities under HQDA. The MACOM or the AASA will review the report for completeness and adequacy of investigation and for the appropriateness of the corrective action/sanctions taken. Such reports will be filed and retained for a period no less than two years and are subject to HQDA or other appropriate agency oversight. MACOMs and the AASA will establish policy and procedures concerning whether or not there will be a forwarding of the reports of preliminary inquiry when the conclusion is other than stated in paragraph 10–3d(2) or (4). Reports of preliminary inquiry will be included in the Command management control review and oversight. If analysis shows that defects in the procedures and requirements of this regulation, or another Army regulation or DOD directive, contributed to the incident, MACOM, and the AASA officials will so advise DAMI–CH. DAMI–CH officials will evaluate the incident and report the conclusions, where deemed warranted, to DOD officials, if the problem concerns a DOD requirement. Report defects in the procedures and requirements regarding Army or other DOD SAPs directives, regulations, instructions, or other regulatory guidance through command channels to DAMI–CH (SAP) and DACS–DMP. If the problem concerns a DOD SAPs Directive, Instruction, or other regulatory guidance, HQDA will report to the Director, Special Programs, ODUSD(P).

c. If the conclusion of the preliminary inquiry is as stated in paragraph 10–3d(2) or (4), and foreign government information is involved, the incident will be reported through command channels and DAMI–CH to the Director of International Security Programs, ODUSD(P), who will notify the foreign government.

d. If the preliminary inquiry concludes that violations of the provisions of this regulation or criminal statutes did occur, see Chapter I, section VI, for other reporting requirements that may apply.

e. Commands will forward, through command channels to DAMI–CH, a copy or summary of the preliminary inquiry or investigation conducted, as a result of the unauthorized disclosure of classified information to the public media. An example of a preliminary report format can be found at figure 10–1, of this Chapter. DAMI–CH will forward such preliminary inquiry reports to the Director, Counterintelligence and Security Programs, OASD(C3I). SAPs leak inquiries or investigations will be provided directly to DAMI–CH (SAP) and DACS–DMP, for forwarding to the Director, Special Programs, ODUSD(P)SP (see appendix I of this regulation and AR 380–381 for more details).

10–5. Reevaluation and damage assessment

a. When notified of possible or actual compromise, the holder of the information or material will ensure that the original classification authority, responsible for each item of the information, is notified of the incident. The OCA will verify and reevaluate the classification of the information and will conduct a damage assessment.

b. When classified information under the control of more than one command or agency is involved, the affected activities are responsible for coordinating their efforts in damage assessment and reevaluation. When participation by foreign governments or international organizations in damage assessment and reevaluation is required, contacts will be made through established intergovernmental liaison channels.

c. The first step in the reevaluation and damage assessment process is for the OCA to verify the actual, current classification of the information involved. The OCA determines whether the information currently is classified and the level and duration of classification that applies.

d. The second step is to reevaluate the classification of the information to see whether the classification should be continued or changed. This review will consider the following possibilities:

(1) The information has lost all or some of its sensitivity since it was classified, and will be downgraded or declassified. In rare cases, it might also be discovered that the information has gained in sensitivity and must be upgraded.

(2) The information has been so compromised by this incident that attempting to protect it further is unrealistic, or inadvisable, and it is be declassified.

(3) The information must continue to be classified at the same level.

e. The third step is to determine whether there are countermeasures that can be taken to minimize or eliminate the damage to the national security that could result from the compromise. These countermeasures might include changing plans or system design features, revising operating procedures, providing increased protection to related information, through classification or upgrading, etc. The OCA performing this function is responsible for initiating or recommending the appropriate countermeasures.

f. The final step is performing the damage assessment. The OCA will determine, given the nature of the information and the countermeasures, if any, that will be employed, what the probable impact of the compromise will be on our national security. In contrast to the first three steps in this process, which must be completed quickly, this step is sometimes a long–term, multi–disciplinary analysis of the adverse effects of the compromise on systems, plans, operations, and/or intelligence.

10–6. Debriefings in cases of unauthorized access

In cases where a person has had unauthorized access to classified information, it is advisable to discuss the situation with the individual to enhance the probability that they will properly protect it. Whether such a discussion, commonly called a "debriefing," is held, is to be decided by the commander, security manager, or other designated official. This decision must be based on the circumstances of the incident, what is known about the person or persons involved, and the nature of the classified information. The following general guidelines apply:

a. If the unauthorized access was by a person with the appropriate security clearance but no need–to–know, debriefing is usually unnecessary. Debriefing is required if the individual is not aware the information is classified and that it needs protection. Inform the person that the information is classified and it requires protection. In these cases, the signing of a debriefing statement (see subparagraph e, below) is usually not necessary.

b. If the unauthorized access was by U.S. government personnel, civilian or military, without the appropriate security clearance, debriefing will be accomplished. Personnel will be advised of their responsibility to prevent further dissemination of the information and of the administrative sanctions and criminal penalties which might follow if they fail to do so. The debriefing official will make sure the individual understands what classified information is and why its protection is important.

c. If the person who had unauthorized access is an employee of a cleared contractor participating in the national industrial security program, the same guidelines apply as for U.S. Government personnel. Coordination with the employing firm's facility security officer/manager is recommended unless such coordination would place the information at increased risk.

d. If the person involved is neither U.S. government personnel, nor an employee of a cleared contractor, the decision will be made by the commander. The key question to be decided is whether the debriefing will have any likely positive effect on the person's ability and/or willingness to protect the information. As a general rule, it is often more effective in the long run to explain that a mistake occurred and that the person had unauthorized access to certain sensitive U.S. government information. Also, that such access should not have happened and that the U.S. Army needs the individual to understand that the information must be protected and never further discussed or otherwise revealed to other unauthorized personnel.

e. It is useful to have the person being debriefed sign a statement acknowledging the debriefing and their understanding of its contents. This may have a significant psychological effect in emphasizing the seriousness of the situation. If the person refuses to sign a debriefing statement, when asked, this fact, and their stated reasons for refusing, will be made a matter of record in the preliminary inquiry. The nearest counterintelligence unit will immediately be notified so that a trained CI investigator can explain the reason for the debriefing and advise the individual that a refusal to sign could indicate an unwillingness to protect classified information and could place their clearance, if held at the time, in jeopardy.

f. In any case where the person to be debriefed may be the subject of criminal prosecution or disciplinary action, command officials are advised to consult with legal counsel before attempting to debrief the individual.

10–7. Management and oversight

a. Department of the Army commands, and especially MACOMs, will establish necessary reporting and oversight mechanisms, to ensure that inquiries are conducted when required, that they are done in a timely and effective manner, and that appropriate management action is taken to correct identified problem areas. Inquiries and management analyses of security incidents will consider possible systemic shortcomings which could have caused or contributed to the incident. The effectiveness of command security procedures, security education, supervisory oversight of security practices, command management emphasis on security, etc., will be considered when determining causes and contributing factors. The focus of management's response to security incidents will be to eliminate, or minimize, the possibility of further incidents occurring. Appropriate disciplinary action or legal prosecution, discussed in Chapter 1, section VII, of this regulation, is sometimes one means of doing this, but the broader focus on prevention must not be lost. Disciplinary action will not be the sole command reaction to a security incident, unless there has been a consideration of what other factors may have contributed to the situation.

b. Commands, and especially MACOMs and MSCs, will establish a system of controls and procedures to make sure that reports of security inquiries and damage assessments are conducted, when required, and that their results are available as needed. Such reports will be available for review during inspections and oversight reviews. MACOMs, and the AASA for HQDA activities, can establish reporting requirements for such inquiries and assessments. Reports of the results of security inquiries will be reported to DAMI–CH, only for those situations stated in paragraph 10–4.

10–8. Additional investigation

Additional investigation, beyond what is required by this Chapter, such as an AR 15–6 investigation, may be needed to permit application of appropriate sanctions for violation of regulations, criminal prosecution, or determination of effective remedies for discovered vulnerabilities. The preliminary inquiry required by this Chapter, serves as a part of these investigations, but notification of originators will not be delayed pending the completion of these investigations.

10–9. Unauthorized absences, suicides, or incapacitation

When an individual, who has had access to classified information, is absent without authorization, commits or attempts to commit suicide, or is temporarily or permanently incapacitated, the command will inquire into the situation to see if there are indications of activities, behavior, or associations, that could indicate classified information might be at risk. If so, the supporting counterintelligence organization will be notified. The scope and depth of this preliminary inquiry will depend on the length of the absence, factors leading to the actual or attempted suicide, or reasons and causes for the incapacitation, and the sensitivity of the classified information involved. See AR 190–40 for further details.

10–10. Negligence

DOD military and civilian personnel are subject to administrative sanctions if they negligently disclose, to unauthorized persons, information properly classified under EO 12958 or any prior or subsequent order. Administrative action against U.S. military personnel, under the Uniform Code of Military Justice (UCMJ), can be pursued, but is not required. Administrative action against civilian personnel can be pursued under U.S. Army civilian personnel regulations, but is not required. No action is to be taken until a full inquiry has been completed to determine the seriousness of the incident.

Section II
Extracts of Espionage Laws and Federal Statutes

10–11. United States Code, Title 18, Section 641 – Public Money, Property Or Records

Whoever embezzles, steals, purloins, or knowingly converts to his use or the use of another, or without authority, sells, conveys or disposes of any record, voucher, money, or thing of value of the United States or of any department or agency thereof, or any property made or being made under contract for the United States or any department or agency thereof; or Whoever receives, conceals, or retains the same with intent to convert it to his use or gain, knowing it to have been embezzled, stolen, purloined or converted – Shall be fined under this title or imprisoned not more than ten years, or both; but if the value of such property does not exceed the sum of $1,000, he shall be fined under this title or imprisoned not more than one year, or both. The word "value" means face, par, or market value, or cost price, either wholesale or retail, whichever is greater.

10–12. United States Code, Title 18, Section 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 vehicle, aircraft, work or defense, facilities,

fueling station, fort, battery, station, dockyard, engineering facility, railroad, arsenal, camp, factory, mine, telegraph, telephone, wireless, or signal station, vessel, navy yard, naval station, submarine base, torpedo station, or other place connected with the national defense owned or constructed, 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 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 this 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, when information the possessor has reason to believe could be used to the injury of the United States or 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 to the office 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, note, or information 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, will be fined not more than $10,000 or imprisoned not more than ten(10) 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 will be subject to the punishment provided for the offense which is the object of such conspiracy. June 25, 1948, c. 645, section 1, 62 Stat. 736, amended Sept. 23, 1950, c. 1024, section 18, 64 Stat.

10–13. United States Code Title 18, Section 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, will be punished by death or by imprisonment for any term of years or for life.

b. Whoever, in time of war, with intent that same will 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, will 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 will be subject to the punishment provided for the offense which is the object of such conspiracy. As amended Sept. 3, 1954, c. 1261, Title II, section 201, 68 Stat. 1219.

10–14. United States Code, Title 18, Section 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 will 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 or naval command concerned, or higher authority, and promptly submitting the product obtained to such command officer or higher authority for censorship or such other action as he may deem necessary.

b. Whoever violates this section will be fined not more than $1,000 or imprisoned not more than one year, or both. (June 25, 1948, ch. 645, 62 Stat. 737.)

10–15. United States Code, Title 18, Section 796 – Use Of Aircraft For Photographs Of Defense Installations

Whoever uses or permits the use of an aircraft or any contrivance used, or designed for navigation or flight in the air, for the purpose of making a photograph, sketch, picture, drawing, map, or graphical representation of vital military or naval installations or equipment, in violation of section 795 of this title, will be fined not more than $1,000 or imprisoned not more than one year, or both. (June 25, 1948, ch. 645,62 Stat. 738.)

10–16. United States Code, Title 18, Section 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, will be fined not more than $1,000 or imprisoned not more than one year, or both. (June 25, 1948, ch. 645,62 Stat. 738.)

10–17. United States Code, Title 18, Section 798 – Disclosure Of Classified Information

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 or 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 from the communications of any foreign government, knowing the same to have been obtained by such processes – will be fined not more than $10, 000 or imprisoned not more than ten (10) years, or both. (Added Oct 31, 1951, ch. 655, section 24(a), 65 Stat. 719.)

10–18. United States Code, Title 50, Section 797 – Violate Regulations And Aiding And Abetting

a. Whoever willfully will violate any such regulation or order as, pursuant to lawful authority, will be or has been promulgated or approved by the Secretary of Defense, or by any military commander designated by the Secretary of Defense, or by the Director of the National Advisory Committee for Aeronautics, for the protection or security of military or naval aircraft, airports, airport facilities, vessels, harbors, ports, piers, water–front facilities, bases, forts, posts, laboratories, stations, vehicles, equipment, explosives, or other property or places subject to the jurisdiction, administration, or in the custody of the Department of Defense, any Department or agency of which said Department consists, or any officer or employee of said Department or agency, or of the National Advisory Committee for Aeronautics, or any officer or employee thereof, relating to fire hazards, fire protection, lighting, machinery, guard service, disrepair, disuse or other re–satisfactory conditions thereon, or the ingress thereto or egress or removal of persons therefrom, or otherwise providing for safeguarding the same against destruction, loss, or injury by accident or

by enemy action, sabotage, or other subversive actions, will be guilty of a misdemeanor and upon conviction thereof will be liable to a fine of not to exceed $5,000 or to imprisonment for not more than one year, or both.

b. Every such regulation or order will be posted in conspicuous and appropriate places. (Sept 23, 1950, ch. 1024, Title I, section 21, 64 Stat. 1005.)

10–19. United States Code, Title 18, Section 952 – Diplomatic Codes And Correspondence

Whoever, by virtue of his employment by the United States, obtains from another or has or has had custody of or access to, any official diplomatic code or any matter prepared in any such code, or which purports to have been prepared in any such code, and without authorization or competent authority, willfully publishes or furnishes to another any such code or matter, or any matter which was obtained while in the process of transmission between any foreign government and its diplomatic mission in the United States, shall be fined under this title or imprisoned not more than ten years, or both.

10–20. United States Code, Title 18, Section 1001 – False And Fraudulent Statements

Whoever, in any matter within the jurisdiction of any department or agency of the United States, knowingly and willfully falsifies, conceals, or covers up by any trick, scheme or device, a material fact or makes any false fictitious or fraudulent statements or representations or makes or uses any false writing or document knowing the same to contain any false, fictitious or fraudulent statement or entry, will be fined not more than $10,000 or imprisoned not more than five (5) years, or both.

10–21. United States Code, Title 18, Section 1924 – Unauthorized Removal And Retention Of Classified Documents Or Material

a. Whoever, being an officer, employee, contractor, or consultant of the United States, and, by virtue of his office, employment, position, or contract, becomes possessed of documents or materials containing classified information of the United States, knowingly removes such documents or materials without authority and with the intent to retain such documents or materials at an unauthorized location shall be fined not more than $1,000, or imprisoned for not more than one year, or both.

b. For purposes of this section, the provision of documents and materials to the Congress shall not constitute an offense under subsection a.

c. In this section, the term "classified information of the United States" means information originated, owned, or possessed by the United States Government concerning the national defense or foreign relations of the United States that has been determined pursuant to law or Executive Order to require protection against unauthorized disclosure in the interest of national security.

10–22. United States Code, Title 50, Sections 783 (B) And (D)

a. Section 783 (b). It will be unlawful for any officer or employee of the United States or any department or agency thereof, or of any corporation the stock of which is owned in whole or in major part by the United States or any department or agency thereof, to communicate in any manner or by any means, to any other person whom such officer or employee knows or has reason to believe to be an agent or representative of any foreign government or an officer or member of any Communist organization as defined in paragraph (5) of section 782 of this title, any information of a kind which will have been classified by the President (or by the head of any such department, agency, or corporation with the approval of the President) as affecting the security of the United States, knowing or having reason to know that such information has been so classified, unless such officer or employee will have been specifically authorized by the President or by the head of the department, agency or corporation by which this officer or employee is employed, to make such disclosure of such information.

b. Section 783 (d). Any person who violates any provision of this section will, upon conviction thereof, be punished by a fine of not more than $10,000, or imprisonment for not more than ten (10) years, or by both such fine and such imprisonment, and will moreover, be thereafter ineligible to hold any office, or place of honor, profit, or trust created by the Constitution or laws of the United States.

10–23. UNIFORM CODE OF MILITARY JUSTICE Article 106a ESPIONAGE

a. Any person subject to this Chapter who, 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 entity described in paragraph (2), either directly or indirectly, any thing described in paragraph (3) will be punished as a court–martial may direct, except that if the accused is found guilty of an offense that directly concerns (A) nuclear weaponry, military spacecraft or satellites, early warning systems, or other means of defense or retaliation against large scale attack, (B) war plans, (C) communications intelligence or cryptographic information, or (D) any other major weapons system or major element of defense strategy, the accused will be punished by death or such other punishment as a court–martial may direct.

b. An entity referred to in paragraph (1) is—

(1) A foreign government;

(2) A faction or party or military or naval force within a foreign country, whether recognized or unrecognized by the United States; or

(3) A representative, officer, agent, employee, subject or citizen of such a government, faction, party, or force.

(4) A thing referred to in paragraph (1) is a document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, note, instrument, appliance, or information relating to the national defense.

c. No person may be sentenced by court–martial to suffer death for an offense under this section (article) unless—

(1) The members of the court–martial unanimously find at least one of the aggravating factors set out in subsection c; and

(2) The members unanimously determine that any extenuating or mitigating circumstances are substantially outweighed by any aggravating circumstances, including the aggravating factors set out under subsection (c).

(3) Findings under this subsection may be based on (A) evidence introduced on the issue of guilt or innocence; (B) evidence introduced during the sentencing proceeding; or (C) all such evidence.

(4) The accused will be given broad latitude to present matters in extenuation and mitigation.

d. A sentence of death may be adjudged by a court–martial for an offense under this section (article) only if the members unanimously find, beyond a reasonable doubt, one of more of the following aggravating factors:

(1) The accused has been convicted of another offense involving espionage or treason for which either a sentence of death or imprisonment for life was authorized by statute.

(2) In the commission of the offense, the accused knowingly created a grave risk of substantial damage to the national security.

(3) In the commission of the offense, the accused knowingly created a grave risk of death to another person.

(4) Any other factor that may be prescribed by the President by regulations under section 836 of this title (Article 36).

Sample Preliminary Inquiry Report

(*Appropriate office symbol)* (380-5s)

MEMORANDUM THRU (*Commander at the next level up. May require more than one.)*

MEMORANDUM FOR (*See paragraph 10-4 for appropriate addressee.)*

SUBJECT: Preliminary Inquiry - Possible Compromise of Classified Information

1. In compliance with AR 380-5, the following is my Report of Preliminary Inquiry.

2. Facts and Circumstances. (*The investigating officer will be completely objective and consider all facts and circumstances to answer the following questions. When the facts are lengthy or complicated, a separate paragraph containing a narrative summary of events, in chronological order, may also be necessary.*)

a. Who? (*Complete identity of everyone involved, including responsible officials, and how they are involved.*)

b. What? (*Exact description of the information/material involved, what happened to it, and, if lost, what steps were taken to locate the missing information.*)

c. When? (*Date and time the incident occurred (if known) and the date and time the situation was discovered and reported.*)

d. Where? (*Complete identification of unit, section, activity, building and room number, and/or geographic location.*)

e. How? (*Circumstances of the incident, chronologically, relating how the information/material was lost or compromised. Summarize the evidence supporting your conclusion and attach supporting enclosure(s) when appropriate.*)

f. Why? (*What are the applicable policies, regulations, etc., for controlling the information/material involved? Were they followed? Was anyone negligent or derelict in their duties? Was the unit/activity SOP adequate to ensure compliance with applicable regulations/directives of higher headquarters and/or for ensuring the proper protection of the information/material concerned under the circumstances? Was the unit/activity's security education program sufficient enough to cover all information security aspects required by AR 380-5?*)

Figure 10-1. Sample Preliminary Inquiry Report

3. Findings. When all of the above questions have been answered, the Investigating Officer will review the facts to reach findings on the following matters (*In cases of a media leak, use the eleven questions in paragraph 10-3e*):

a. Did a loss of classified information/material occur?

b. Did a compromise occur, or under the circumstances, what is the probability of compromise? (*Or state that a compromise did not occur, or that there is minimal risk of damage to the national security.*)

c. If a loss or compromise occurred, has a damage assessment been done? (*Outline the damage assessment procedures taken.*)

d. Is there any indication of significant security weaknesses in the unit/activity? If so, state them. (*Were there any deficiencies in procedures for safeguarding classified information? Were there any violations of established procedures? If so, were they significant or contributory to the loss or compromise? How so?*)

e. Is disciplinary action appropriate? Have administrative procedures as required by Chapter 1, section VI, of this regulation, been initiated? If so, what were they?

4. Recommendations. (*The investigating officer will make specific recommendations based upon their findings. The recommendation(s) will include any relevant corrective action(s) or administrative sanctions consistent with the findings, but, as a minimum, will address the following:*)

a. (*A compromise of classified information did not occur.*)

b. (*If the findings are that a loss occurred and the probability of damage to the national security cannot be discounted, or it is determined that further investigation is likely to be productive, a recommendation that an investigation under AR 15-6, a counterintelligence investigation, or a criminal investigation, be conducted, may be included.*)

c. (*If there was a significant security weakness, the recommendation will include specific changes that should be made to correct the deficiency. In addition, further investigation, under AR 15-6, may be appropriate if the weakness resulted from conscious noncompliance with applicable regulations and directives.*)

d. (*If administrative sanction(s) are warranted, the recommendation(s) should identify the specific violation committed, by whom it was committed, and by whom the sanction(s) should be administered. If further investigation under AR 15-6 is not recommended for one of the reasons listed above, there need not be a recommendation for further investigation under AR 15-6 solely to impose administrative sanctions. The investigative officer should consult with the Staff Judge Advocate to determine whether*

Figure 10-1. Sample Preliminary Inquiry Report—Continued

to recommend additional investigation or whether normal channels under the Uniform Code of Military Justice will suffice.)

e. (*If further investigation under AR 15-6 is recommended, the recommendation will identify any person(s) who should be designated as the respondent and make a recommendation as to whether formal or informal investigation should be conducted, pursuant to AR 15-6, paragraph 1-2b.*)

5. Comments. (*Use this area for any additional comments not covered by the preceding paragraphs. If there are none, do not include this paragraph.*)

6. Point of Contact. (*Give full identification of the investigating officer to include, full name, rank, SSAN, full unit designation/location, and phone number(s).*)

(*Signature and Signature Block*
Of investigating officer)

Figure 10-1. Sample Preliminary Inquiry Report—Continued

Appendix A
References

Section I
Required Publications

DOD Directive 5200.1–R
Information Security Program Regulation (Cited in para 1–1)

Executive Order 12958
Classified National Security Information (Cited in para 1–1)

Executive Order 12972
Amendment to Executive Order No. 12958 (Cited in para 3–5)

Executive Order 13142
Amendment to Executive Order No. 12958 (Cited in para 4–10)

Section II
Related Publications

A related publication is merely a source of additional information. The user does not have to read it to understand this regulation.

AR 15–6
Procedures for Investigating Officers and Boards of Officers

AR 25–55
Freedom of Information Act Program

AR 25–400–2
The Modern Army Recordkeeping System (MARKS)

AR 190–13
The Army Physical Security Program

AR 190–16
Physical Security

AR 190–40
Serious Incident Report

AR 195–2
Criminal Investigation Activities

AR 380–10
Technology Transfer, Disclosure of Information and Contacts with Foreign Representatives

AR 380–15
Safeguarding Classified NATO Information

AR 380–19
Information Systems Security

AR 380–28
Department of the Army Special Security System

AR 380–40
Policy for Safeguarding and Controlling Communications Security (COMSEC) Material

AR 380–49
Department of the Army Industrial Security Program

AR 380–53
Information Systems Security Monitoring

AR 380–67
Personnel Security Program

AR 380–381
Special Access Programs

AR 381–12
Subversion and Espionage Directed Against the U.S. Army (SAEDA)

AR 381–20
The Army Counterintelligence Program

AR 525–13
Antiterrorism Force Protection: Security of Personnel, Information, and Critical Resources

DCID 1/19
Security Policy for Sensitive Compartmented Information (SCI)

DCID 1/21
Physical Security Standards for SCIFs

DCID 1/7
Security Controls on the Dissemination of Intelligence Information

DCID 5/6
Intelligence Disclosure Policy, and the National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations (abbreviated title: National Disclosure Policy 1 or NDP 1)

DOD Directive 5000.1
Defense Acquisition

DOD Directive 5030.47
National Supply System

DOD Directive 5142.1
Assistant Secretary of Defense (Legislative Affairs)

DOD 5200.1–H
DOD Handbook for Writing Security Classification Guidance

DOD O 5200.1–1
DOD Index of Security Classification Guides

DOD 5200.2–R
Department of Defense Personnel Security Program (DODPSP)

DOD Directive 5200.28
Security Requirements for Automated Data Processing (ADP) Systems

DOD Directive 5210.2
Defense Courier Service

DOD Directive 5210.2
Access to and Dissemination of Restricted Data

DOD Directive 5210.83
Department of Defense Controlled Unclassified Nuclear Information (DOD UCNI)

DOD 5220.22–M
National Industrial Security Program (NISP) Operating Manual

DOD 5220.22–R
Industrial Security Regulation

DOD Directive 5230.11
Disclosure of Classified Military Information to Foreign Governments and International Organizations

DOD Directive 5230.20
Visits, Assignments, and Exchanges of Foreign Nationals

DOD Directive 5230.24
Distribution Statements on Technical Documents

DOD Directive 5400.4
Provision of Information to Congress

DOD 5400.11–R
Department of Defense Privacy Program

DOD Directive 5405.2
Release of Official Information in Litigation and Testimony by DOD Personnel As Witnesses

DOD Directive 7650.1
General Accounting Office (GAO) and Comptroller General Access to Records

DOD Handbook 5200.1–PH
Department of Defense Handbook for Writing Security Classification Guidance

DOD Instruction 5240.4
Reporting of Counterintelligence and Criminal Violations

DOD Instruction 5505.2
Criminal Investigations of Fraud Offenses

DOD Manual 5105.21–M–1
Sensitive Compartmented Information Administrative Security Manual

Federal Standard FED–STD–809
Neutralization and Repair of GSA Approved Containers

FM 19–30
Physical Security

JCS Policy Memorandum 39
Release Procedures for JCS Papers

Joint Army–Navy–Air Force Publication (JANAP) 299
US Joint Code Word Index

Military Handbook 1013/1A
Design Guidance for Physical Security of Facilities

Office of Management and Budget, Information Security Oversight Office, Directive No. 1, Classified National Security Information (32 CFR Part 2001)

Title 18, United States Code
U.S. Central Registry

Section III
Prescribed Forms

Except where indicated below, the following forms are available on the Army Electronic Library (AEL) CD-ROM (EM 0001) and the USAPA web site (www.usapa.army.mil).

DA Form 455
Mail and Document Register. (Prescribed in para 6–21b.)

DA Form 969
Top Secret Document Record. (Prescribed in para 6–21f.)

DA Form 1575
Request for/or Notification of Regrading Action (Prescribed in para 2–22a.)

DA Form 1965
Delivery and Pick Up Service. (Prescribed in para 8–8.) Form is available in paper through normal forms supply channels.

DD Form 2501
Courier Authorization Card. (Prescribed in para 8–13b.) This form is available in paper through normal forms supply channels.

DA Form 2962
Security Termination Statement. (Prescribed in 6–5b.)

DA Form 3964
Classified Document Accountability Record. (Prescribed in para 6–29a.)

DOE Form 5631.20
Request for Visit or Access Approval. (Prescribed in para 6-7b and 6-17b.) This form is available at www.explorer.doe.gov:1776/htmls/DOEFORMS.html.

SF 311
Agency Information Security Program Data. (Prescribed in para 1–7h.)

SF 312
Classified Information Nondisclosure Agreement (NDA). (Prescribed in para 6–2.)

SF 700
Security Container Information. (Prescribed in para 7–8c.) This form is available in paper through the Federal Supply Service, Ft. Worth, TX Phone: 817-978-2051.

SF 701
Activity Security Checklist. (Prescribed in para 6–11.) This form is available in paper through the Federal Supply Service, Ft. Worth, TX Phone: 817-978-2051.

SF 702
Security Container Check Sheet. (Prescribed in para 6–10b.) This form is available in paper through the Federal Supply Service, Ft. Worth, TX Phone: 817-978-2051. The electronic form is available at http://web1.osd.mil/icdhome/sfeforms.htm

SF 703
Top Secret Cover Sheet. (Prescribed in para 6–10a.) (This form is available in paper through normal forms supply channels.)

SF 704
Secret Cover Sheet. (Prescribed in para 6–10a.) (This form is available in paper through normal forms supply channels.)

SF 705
Confidential Cover Sheet. (Prescribed in para 6–10a.) (This form is available in paper through normal forms supply channels.)

SF 706
Orange Top Secret Label. (Prescribed in para 4–34.) (This form is available in paper through normal forms supply channels.)

SF 707
Red Secret Label. (Prescribed in para 4–34.) (This form is available in paper through normal forms supply channels.)

SF 708
Blue Confidential Label. (Prescribed in para 4–34.) (This form is available in paper through normal forms supply channels.)

SF 710
Green Unclassified Label. (Prescribed in para 4–34.) (This form is available in paper through normal forms supply channels.)

SF 711
Data Descriptor Label. (Prescribed in para 4–34.) (This form is available in paper through normal forms supply channels.)

SF 712
Classified SCI Label. (Prescribed in para 4–34.) This form is available in paper through the Federal Supply Service, Ft. Worth, TX Phone: 817-978-2051.

Section IV
Referenced Forms

DA Form 11–2–R
Management Control Evaluation Certification Statement

DA Form 873
Certificate of Clearance and/or Security Determination

DD Form 2
Armed Forces of the United States Geneva Convention Identification Card

DD Form 173/1
Joint Message Form. (This form is available in paper through normal forms supply channels.

DD Form 1610
Request and Authorization for TDY Travel of DOD Personnel

DD Form 1847–1
Sensitive Compartmented Information Nondisclosure Statement. (This form is available in paper through normal forms supply channels.)

DD Form 2024
DOD Security Classification Guide Data Elements

DD Form 2056
Telephone Monitoring Notification Decal. (This form is available in paper through normal forms supply channels.)

SF 75
Request for Preliminary Employment Data. (This form is available in paper through normal supply channels.)

SF 135
Records Transmittal and Receipt

SF 135–A
Records Transmittal and Receipt Continuation

Appendix B
Presidential Executive Orders (EO) 12958, EO 12972 and EO 13142

This regulation implements the policy set forth in Executive Order (E.O.) 12958, Classified National Security Information, April 17, 1995, with amendments, and Department of Defense Directive 5200.1–R, Information Security Program, January 14, 1997. The following are reprints of Executive Order (EO) 12958 and its supplements, EO 12972 and EO 13142."

1.0. — Section 1.0
Executive Order 12958 of April 17, 1995
The President
Classified National Security Information

This Order prescribes a uniform system for classifying, safeguarding, and declassifying national security information. Our democratic principles require that the American people be informed of the activities of their Government. Also, our nation's progress depends on the free flow of information. Nevertheless, throughout our history, the national interest has required that certain information be maintained in confidence in Order to protect our citizens, our democratic institutions, and our participation within the community of nations. Protecting information critical to our Nation's security remains a priority. In recent years, however, dramatic changes have altered, although not eliminated, the national security threats that we confront. These changes provide a greater opportunity to emphasize our commitment to open Government.

NOW, THEREFORE, by the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby Ordered as follows:

Part 1 – Original Classification

1.1. — Section 1.1
Definitions

For purposes of this Order:

a. "National security" means the national defense or foreign relations of the United States.

b. "Information" means any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the United States Government. "Control" means the authority of the agency that originates information, or its successor in function, to regulate access to the information.

c. "Classified national security information" (hereafter "classified information") means information that has been determined pursuant to this Order or any predecessor Order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

d. "Foreign Government Information" means:

(1) Information provided to the United States Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence.

(2) Information produced by the United States pursuant to or as a 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.

(3) Information received and treated as "Foreign Government Information" under the terms of a predecessor Order.

e. "Classification" means the act or process by which information is determined to be classified information.

f. "Original classification" means an initial determination that information requires, in the interest of national security, protection against unauthorized disclosure.

g. "Original classification authority" means an individual authorized in writing, either by the President, or by agency heads or other officials designated by the President, to classify information in the first instance.

h. "Unauthorized disclosure" means a communication or physical transfer of classified information to an unauthorized recipient.

i. "Agency" means any " Executive agency," as defined in 5 USC 105, and any other entity within the executive branch that comes into the possession of classified information.

j. "Senior agency official" means the official designated by the agency head under section 5.6(c) of this Order to direct and administer the agency's program under which information is classified, safeguarded and declassified.

k. "Confidential source"means 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 that the information or relationship, or both, are to be held in confidence.

l. "Damage to the national security" means harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, to include the sensitivity, value, and utility of that information.

1.2. — Section 1.2
Classification Standards

a. Information may be originally classified under the terms of this Order only if all of the following conditions are met:

(1) An original classification authority is classifying the information.

(2) The information is owned by, produced by or for, or is under the control of the United States Government.

(3) The information falls within one or more of the categories of information listed in section 1.5 of this Order.

(4) The original classification authority determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security and the original classification authority is able to identify or describe the damage.

b. If there is significant doubt about the need to classify information, it will not be classified. This provision does not:

(1) Amplify or modify the substantive criteria or procedures for classification.

(2) Create any substantive or procedural rights subject to judicial review.

c. Classified information will not be declassified automatically as a result of any unauthorized disclosure of identical or similar information.

1.3. — Section 1.3
Classification Levels

a. Information may be classified at one of the following three levels:

(1) "TOP SECRET" will be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.

(2) "SECRET" will be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.

(3) "CONFIDENTIAL" will be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

b. Except as otherwise provided by statute, no other terms will be used to identify United States classified information.

c. If there is significant doubt about the appropriate level of classification, it will be classified at the lower level.

1.4. — Section 1.4
Classification Authority

a. The authority to classify information originally may be exercised only by:

(1) The President.

(2) Agency heads and officials designated by the President in the Federal Register.

(3) United States Government officials delegated this authority pursuant to paragraph (c), below.

b. Officials authorized to classify information at a specified level are also authorized to classify information at a lower level.

c. Delegation of original classification authority.

(1) Delegation of original classification authority will be limited to the minimum required to administer this Order. Agency heads are responsible for ensuring that designated subordinate officials have a demonstrable and continuing need to exercise this authority.

(2) "TOP SECRET" original classification authority may be delegated only by the President or by an agency head or official designated pursuant to paragraph (a)(2), above.

(3) "SECRET" or "CONFIDENTIAL" original classification authority may be delegated only by the President; an

agency head or official designated pursuant to paragraph a.2, above; or the senior agency official, provided that official has been delegated "TOP SECRET" original classification authority by the agency head.

(4) Each delegation of original classification authority will be in writing and the authority will not be re–delegated except as provided in this Order. Each delegation will identify the official by name or position title.

d. Original classification authorities must receive training in original classification as provided in this Order and its implementing directives.

e. Exceptional Cases. When an employee, contractor, licensee, certificate holder, or grantee of an agency that does not have original classification authority originates information believed by that person to require classification, the information will be protected in a manner consistent with this Order and its implementing directives. The information will be transmitted promptly as provided under this Order or its implementing directives to the agency that has appropriate subject matter interest and classification authority with respect to this information. That agency will decide within 30 days whether to classify this information. If it is not clear which agency has classification responsibility for this information, it will be sent to the Director of the Information Security Oversight Office (ISOO). The Director will determine the agency having primary subject matter interest and forward the information, with appropriate recommendations, to that agency for a classification determination.

1.5. — Section 1.5
Classification Categories

Information may not be considered for classification unless it concerns:

a. Military plans, weapons systems, or operations.

b. Foreign government information.

c. Intelligence activities (including special activities), intelligence sources or methods, or cryptology.

d. Foreign relations or foreign activities of the United States, including confidential sources.

e. Scientific, technological, or economic matters relating to the national security.

f. United States Government programs for safeguarding nuclear materials or facilities; or

g. Vulnerabilities or capabilities of systems, installations, projects or plans relating to the national security.

1.6. — Section 1.6
Duration of Classification

a. At the time of original classification, the original classification authority will attempt to establish a specific date or event for declassification based upon the duration of the national security sensitivity of the information. The date or event will not exceed the time frame in paragraph b, below.

b. If the original classification authority cannot determine an earlier specific date or event for declassification, information will be marked for declassification 10 years from the date of the original decision, except as provided in paragraph d, below.

c. An original classification authority may extend the duration of classification or reclassify specific information for successive periods not to exceed 10 years at a time if such action is consistent with the standards and procedures established under this Order. This provision does not apply to information contained in records that are more than 25 years old and have been determined to have permanent historical value under Title 44, United States Code.

d. At the time of original classification, the original classification authority may exempt from declassification within 10 years specific information, the unauthorized disclosure of which could reasonably be expected to cause damage to the national security, for a period greater than that provided in paragraph b, above, and the release of which could reasonably be expected to:

(1) Reveal an intelligence source, method, or activity, or a cryptologic system or activity.

(2) Reveal information that would assist in the development or use of weapons of mass destruction.

(3) Reveal information that would impair the development or use of technology within a United States weapon system.

(4) Reveal United States military plans, or national security emergency preparedness plans.

(5) Reveal foreign government information.

(6) Damage relations between the United States and a foreign government, reveal a confidential source, or seriously undermine diplomatic activities that are reasonably expected to be ongoing for a period greater than that provided in paragraph b, above.

(7) Impair the ability of responsible United States Government officials to protect the President, the Vice President, and other individuals for whom protection services, in the interest of national security, are authorized.

(8) Violate a statute, treaty, or international agreement.

e. Information marked for an indefinite duration of classification under predecessor Orders, for example, "Originating Agency's Determination Required" (OADR), or information classified under predecessor Orders that contains no declassification instructions will be declassified in accordance with part 3 of this Order.

1.7. — Section 1.7
Identification and Markings

a. At the time of original classification, the following will appear on the face of each classified document, or will be applied to other classified media in an appropriate manner:

(1) One of the three classification levels defined in Section 1.3 of this Order.

(2) The identity, by name or personal identifier and position, of the original classification authority.

(3) The agency and office of origin, if not otherwise evident.

(4) Declassification instructions, which will indicate one of the following:

(a) The date or event for declassification, as prescribed in Section 1.6.a or Section 1.6.c.

(b) The date that is ten years from the date of original classification, as prescribed in Section 1.6.b.

(c) The exemption category from automatic declassification, as prescribed in Section 1.6.d.

(5) A concise reason for classification which, at a minimum, cites the applicable classification categories in Section 1.5 of this Order.

b. Specific information contained in paragraph a, above, may be excluded if it would reveal additional classified information.

c. Each classified document will, by marking or other means, indicate which portions are classified, with the applicable classification level, which portions are exempt from declassification under section 1.6.d of this Order, and which portions are unclassified. In accordance with standards prescribed in directives issued under this Order, the Director of the Information Security Oversight Office may grant waivers of this requirement for specified classes of documents or information. The Director will revoke any waiver upon a finding of abuse.

d. Markings implementing the provisions of this Order, including abbreviations and requirements to safeguard classified working papers, will conform to the standards prescribed in implementing directives issued pursuant to this Order.

e. Foreign government information will retain its original classification markings or will be assigned a U.S. classification that provides a degree of protection at least equivalent to that required by the entity that furnished the information.

f. Information assigned a level of classification under this or predecessor Orders will be considered as classified at that level of classification despite the omission of other required markings. Whenever such information is used in the derivative classification process or is reviewed for possible declassification, holders of such information will coordinate with an appropriate classification authority for the application of omitted markings.

g. The classification authority will, whenever practicable, use a classified addendum whenever classified information constitutes a small portion of an otherwise unclassified document.

1.8. — Section 1.8
Classification Prohibitions and Limitations

a. In no case will information be classified in Order to:

(1) Conceal violations of law, inefficiency, or administrative error.

(2) Prevent embarrassment to a person, organization, or agency.

(3) Restrain competition.

(4) Prevent or delay the release of information that does not require protection in the interest of national security.

b. Basic scientific research information not clearly related to the national security may not be classified.

c. Information may not be reclassified after it has been declassified and released to the public under proper authority.

d. Information that has not previously been disclosed to the public under proper authority may be classified or reclassified after an agency has received a request for it under the Freedom of Information Act (5 USC 552) or the Privacy Act of 1974 (5 USC 552a), or the mandatory review provisions of section 3.6 of this Order only if such classification meets the requirements of this Order and is accomplished on a document–by–document basis with the personal participation or under the direction of the agency head, the deputy agency head, or the senior agency official designated under section 5.6 of this Order. This provision does not apply to classified information contained in records that are more than 25 years old and have been determined to have permanent historical value under title 44, United States Code.

e. Compilations of items of information which are individually unclassified may be classified if the compiled information reveals an additional association or relationship that:

(1) Meets the standards for classification under this Order.

(2) Is not otherwise revealed in the individual items of information. As used in this Order, “compilation” means an aggregation of pre–existing unclassified items of information.

1.9. — Section 1.9
Classification Challenges

a. Authorized holders of information who, in good faith, believe that its classification status is improper are encouraged and expected to challenge the classification status of the information in accordance with agency procedures established under paragraph b, below.

b. In accordance with implementing directives issued pursuant to this Order, an agency head or senior agency official will establish procedures under which authorized holders of information are encouraged and expected to challenge the classification of information that they believe is improperly classified or unclassified. These procedures will assure that:

(1) Individuals are not subject to retribution for bringing such actions.

(2) An opportunity is provided for review by an impartial official or panel.

(3) Individuals are advised of their right to appeal agency decisions to the Interagency Security Classification Appeals Panel established by Section 5.4 of this Order.

Part 2 – Derivative Classification

2.1. — Section 2.1
Definitions

For purposes of this Order:

a. "Derivative classification" means the incorporating, paraphrasing, restating or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. Derivative classification includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification.

b. "Classification guidance"means any instruction or source that prescribes the classification of specific information.

c. "Classification guide" means a documentary form of classification guidance issued by an original classification authority that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element.

d. "Source document" means an existing document that contains classified information that is incorporated, paraphrased, restated, or generated in new form into a new document.

e. "Multiple sources" means two or more source documents, classification guides or a combination of both.

2.2. — Section 2.2
Use of Derivative Classification

a. 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, need not possess original classification authority.

b. Persons who apply derivative classification markings will—

(1) Observe and respect original classification decisions.

(2) Carry forward to any newly created documents the pertinent classification markings. For information derivatively classified based on multiple sources, the derivative classifier will carry forward:

(a) The date or event for declassification that corresponds to the longest period of classification among the sources.

(b) Listing of these sources on or attached to the official file or record copy.

2.3. — Section 2.3
Classification Guides

a. Agencies with original classification authority will prepare classification guides to facilitate the proper and uniform derivative classification of information. These guides will conform to standards contained in directives issued under this Order.

b. Each guide will 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.

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

c. Agencies will establish procedures to assure that classification guides are reviewed and updated as provided in directives issued under this Order.

Part 3 – Declassification and Downgrading

3.1. — Section 3.1
Definitions

For purposes of this Order:

a. "Declassification" means the authorized change in the status of information from classified information to unclassified information.

b. "Automatic declassification" means the declassification of information based solely upon:

(1) The occurrence of a specific date or event as determined by the original classification authority.

(2) The expiration of a maximum time frame for duration of classification established under this Order.

c. "Declassification authority" means:

(1) The official who authorized the original classification, if that official is still serving in the same position.

(2) The originator's current successor in function.

(3) A supervisory official.

(4) Officials delegated declassification authority in writing by the agency head or the senior agency official.

d. "Mandatory declassification review" means the review for declassification of classified information in response to a request for declassification that meets the requirements under Section 3.6 of this Order.

e. "Systematic declassification review" means the review for declassification of classified information contained in records that have been determined by the Archivist of the United States ("Archivist") to have permanent historical value in accordance with Chapter 33 of Title 44, United States Code.

f. "Declassification guide" means written instructions issued by a declassification authority that describes the elements of information regarding a specific subject that may be declassified and the elements that must remain classified.

g. "Downgrading" means a determination by a declassification authority that information classified and safeguarded at a specified level will be classified and safeguarded at a lower level.

h. "File series" means documentary material, regardless of its physical form or characteristics, that is arranged in accordance with a filing system or maintained as a unit because it pertains to the same function or activity.

3.2. — Section 3.2
Authority for Declassification

a. Information will be declassified as soon as it no longer meets the standards for classification under this Order.

b. It is presumed that information that continues to meet the classification requirements under this Order requires continued protection. In some exceptional cases, however, the need to protect such information may be outweighed by the public interest in disclosure of the information, and in these cases the information should be declassified. When such questions arise, they will be referred to the agency head or the senior agency official. That official will determine, as an exercise of discretion, whether the public interest in disclosure outweighs the damage to national security that might reasonably be expected from disclosure. This provision does not:

(1) Amplify or modify the substantive criteria or procedures for classification.

(2) Create any substantive or procedural rights subject to judicial review.

c. If the Director of the Information Security Oversight Office determines that information is classified in violation of this Order, the Director may require the information to be declassified by the agency that originated the classification. Any such decision by the Director may be appealed to the President through the Assistant to the President for National Security Affairs. The information will remain classified pending a prompt decision on the appeal.

d. The provisions of this section will also apply to agencies that, under the terms of this Order, do not have original classification authority, but had such authority under predecessor Orders.

3.3. — Section 3.3
Transferred Information

a. In the case of classified information transferred in conjunction with a transfer of functions, and not merely for storage purposes, the receiving agency will be deemed to be the originating agency for purposes of this Order.

b. In the case of classified information that is not officially transferred as described in paragraph a, above, but that originated in an agency that has ceased to exist and for which there is no successor agency, each agency in possession of such information will be deemed to be the originating agency for purposes of this Order. Such information may be declassified or downgraded by the agency in possession after consultation with any other agency that has an interest in the subject matter of the information.

c. Classified information accessioned into the National Archives and Records Administration ("National Archives")

as of the effective date of this Order will be declassified or downgraded by the Archivist in accordance with this Order, the directives issued pursuant to this Order, agency declassification guides, and any existing procedural agreement between the Archivist and the relevant agency head.

d. The originating agency will take all reasonable steps to declassify classified information contained in records determined to have permanent historical value before they are accessioned into the National Archives. However, the Archivist may require that records containing classified information be accessioned into the National Archives when necessary to comply with the provisions of the Federal Records Act. This provision does not apply to information being transferred to the Archivist pursuant to Section 2203 of Title 44, United States Code, or information for which the National Archives and Records Administration serves as the custodian of the records of an agency or organization that goes out of existence.

e. To the extent practicable, agencies will adopt a system of records management that will facilitate the public release of documents at the time such documents are declassified pursuant to the provisions for automatic declassification in sections 1.6 and 3.4 of this Order.

3.4. — Section 3.4
Automatic Declassification

a. Subject to paragraph b, below, within five years from the date of this Order, all classified information contained in records that: (1) are more than 25 years old; and (2) have been determined to have permanent historical value under Title 44, United States Code, will be automatically declassified whether or not the records have been reviewed. Subsequently, all classified information in such records will be automatically declassified no longer than 25 years from the date of its original classification, except as provided in paragraph b, below.

b. An agency head may exempt from automatic declassification under paragraph a, above, specific information, the release of which should be expected to:

(1) Reveal the identity of a confidential human source, or reveal information about the application of an intelligence source or method, or reveal the identity of a human intelligence source when the unauthorized disclosure of that source would clearly and demonstrably damage the national security interests of the United States.

(2) Reveal information that would assist in the development or use of weapons of mass destruction.

(3) Reveal information that would impair U.S. cryptologic systems or activities.

(4) Reveal information that would impair the application of state of the art technology within a U.S. weapon system.

(5) Reveal actual U.S. military war plans that remain in effect.

(6) Reveal information that would seriously and demonstrably impair relations between the United States and a foreign government, or seriously and demonstrably undermine ongoing diplomatic activities of the United States.

(7) Reveal information that would clearly and demonstrably impair the current ability of United States Government officials to protect the President, Vice President, and other officials for whom protection services, in the interest of national security, are authorized.

(8) Reveal information that would seriously and demonstrably impair current national security emergency preparedness plans.

(9) Violate a statute, treaty, or international agreement.

c. No later than the effective date of this Order, an agency head will notify the President through the Assistant to the President for National Security Affairs of any specific file series of records for which a review or assessment has determined that the information within those file series almost invariably falls within one or more of the exemption categories listed in paragraph b, above, and which the agency proposes to exempt from automatic declassification. The notification will include:

(1) A description of the file series.

(2) An explanation of why the information within the file series is almost invariably exempt from automatic declassification and why the information must remain classified for a longer period of time.

(3) Except for the identity of a confidential human source or a human intelligence source, as provided in paragraph b, above, a specific date or event for declassification of the information. The President may direct the agency head not to exempt the file series or to declassify the information within that series at an earlier date than recommended.

d. At least 180 days before information is automatically declassified under this section, an agency head or senior agency official will notify the Director of the Information Security Oversight Office, serving as executive Secretary of the Interagency Security Classification Appeals Panel, of any specific information beyond that included in a notification to the President under paragraph c, above, that the agency proposes to exempt from automatic declassification. The notification will include:

(1) A description of the information.

(2) an explanation of why the information is exempt from automatic declassification and must remain classified for a longer period of time.

(3) Except for the identity of a confidential human source or a human intelligence source, as provided in paragraph b, above, a specific date or event for declassification of the information. The Panel may direct the agency not to exempt the information or to declassify it at an earlier date than recommended. The agency head may appeal such a

decision to the President through the Assistant to the President for National Security Affairs. The information will remain classified while such an appeal is pending.

e. No later than the effective date of this Order, the agency head or senior agency official will provide the Director of the Information Security Oversight Office with a plan for compliance with the requirements of this section, including the establishment of interim target dates. Each such plan will include the requirement that the agency declassify at least 15 percent of the records affected by this section no later than 1 year from the effective date of this Order, and similar commitments for subsequent years until the effective date for automatic declassification.

f. Information exempted from automatic declassification under this section will remain subject to the mandatory and systematic declassification review provisions of this Order.

g. The Secretary of State will determine when the United States should commence negotiations with the appropriate officials of a foreign government or international organization of governments to modify any treaty international agreement that requires the classification of information contained in records affected by this section for a period longer than 25 years from the date of its creation, unless the treaty or international agreement pertains to information that may otherwise remain classified beyond 25 years under this section.

3.5. — Section 3.5
Systematic Declassification Review

a. Each agency that has originated classified information under this Order or its predecessors will establish and conduct a program for systematic declassification review. This program will apply to historically valuable records exempted from automatic declassification under Section 3.4 of this Order. Agencies will prioritize the systematic review of records based upon:

(1) Recommendations of the Information Security Policy Advisory Council, established in Section 5.5 of this Order, on specific subject areas for systematic review concentration.

(2) The degree of researcher interest and the likelihood of declassification upon review.

b. The Archivist will conduct a systematic declassification review program for classified information 1), accessioned into the National Archives as of the effective date of this Order 2), information transferred to the Archivist pursuant to Section 2203 of Title 44, United States Code, and 3), information for which the National Archives and Records Administration serves as the custodian of the records of an agency or organization that has gone out of existence. This program will apply to pertinent records no later than 25 years from the date of their creation. The Archivist will establish priorities for the systematic review of these records based upon the recommendations of the Information Security Policy Advisory Council, or the degree of researcher interest and the likelihood of declassification upon review. These records will be reviewed in accordance with the standards of this Order, its implementing directives, and declassification guides provided to the Archivist by each agency that originated the records. The Director of the Information Security Oversight Office will assure that agencies provide the Archivist with adequate and current declassification guides.

c. After consultation with affected agencies, the Secretary of Defense may establish special procedures for systematic review for declassification of classified cryptologic information, and the Director of Central Intelligence may establish special procedures for systematic review for declassification of classified information pertaining to intelligence activities (including special activities), or intelligence sources or methods.

3.6. — Section 3.6
Mandatory Declassification Review

a. Except as provided in paragraph b, below, all information classified under this Order or predecessor Orders will be subject to a review for declassification by the originating agency if:

(1) The request for a review describes the document or material containing the information with sufficient specificity to enable the agency to locate it with a reasonable amount of effort.

(2) The information is not exempted from search and review under the Central Intelligence Agency Information Act.

(3) The information has not been reviewed for declassification within the past two years. If the agency has reviewed the information within the past two years, or the information is the subject of pending litigation, the agency will inform the requester of this fact and of the requester's appeal rights.

b. Information originated by:

(1) The incumbent President.

(2) The incumbent President's White House Staff.

(3) Committees, commissions, or boards appointed by the incumbent President.

(4) Other entities within the Executive Office of the President that solely advise and assist the incumbent President is exempted from the provisions of paragraph a, above. However, the Archivist will have the authority to review, downgrade, and declassify information of former presidents under the control of the Archivist pursuant to Sections 2107, 2111, 2111 note, or 2203 of Title 44, United States Code. Review procedures developed by the Archivist will provide for consultation with agencies having primary subject matter interest and will be consistent with the provisions of applicable laws or lawful agreements that pertain to the respective presidential papers or records. Agencies with

primary subject matter interest will be notified promptly of the Archivist's decision. Any final decision by the Archivist may be appealed by the requester or an agency to the Interagency Security Classification Appeals Panel. The information will remain classified pending a prompt decision on the appeal.

c. Agencies conducting a mandatory review for declassification will declassify information that no longer meets the standards for classification under this Order. They will release this information unless withholding is otherwise authorized and warranted under applicable law.

d. In accordance with directives issued pursuant to this Order, agency heads will develop procedures to process requests for the mandatory review of classified information. These procedures will apply to information classified under this or predecessor Orders. They also will provide a means for administratively appealing a denial of a mandatory review request, and for notifying the requester of the right to appeal a final agency decision to the Interagency Security Classification Appeals Panel.

e. After consultation with affected agencies, the Secretary of Defense will develop special procedures for the review of cryptologic information, the Director of Central Intelligence will develop special procedures for the review of information pertaining to intelligence activities (including special activities), or intelligence sources or methods, and the Archivist will develop special procedures for the review of information accessioned into the National Archives.

3.7. — Section 3.7
Processing Requests and Reviews

In response to a request for information under the Freedom of Information Act, the Privacy Act of 1974, or the mandatory review provisions of this Order, or pursuant to the automatic declassification or systematic review provisions of this Order:

a. An agency may refuse to confirm or deny the existence or non–existence of requested information whenever the fact of its existence or non–existence is itself classified under this Order.

b. When an agency receives any request for documents in its custody that contain information that was originally classified by another agency, or comes across such documents in the process of the automatic declassification or systematic review provisions of this Order, it will refer copies of any request and the pertinent documents to the originating agency for processing, and may, after consultation with the originating agency, inform any requester of the referral unless such association is itself classified under this Order. In cases in which the originating agency determines in writing that a response under paragraph (a), above, is required, the referring agency will respond to the requester in accordance with that paragraph.

3.8. — Section 3.8
Declassification Database

a. The Archivist in conjunction with the Director of the Information Security Oversight Office and those agencies that originate classified information, will establish a Government–wide database of information that has been declassified. The Archivist will also explore other possible uses of technology to facilitate the declassification process.

b. Agency heads will fully cooperate with the Archivist in these efforts.

c. Except as otherwise authorized and warranted by law, all declassified information contained within the database established under paragraph (a), above, will be available to the public.

Part 4 – Safeguarding

4.1. — Section 4.1
Definitions

For purposes of this Order:

a. "Safeguarding" means measures and controls that are prescribed to protect classified information.

b. "Access" means the ability or opportunity to gain knowledge of classified information.

c. "Need–to–know" means a determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in Order to perform or assist in a lawful and authorized governmental function.

d. "Automated information system" means an assembly of computer hardware, software, or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information.

e. "Integrity" means the state that exists when information is unchanged from its source and has not been accidentally or intentionally modified, altered, or destroyed.

f. "Network" means a system of two or more computers that can exchange data or information.

g. "Telecommunications" means the preparation, transmission, or communication of information by electronic means.

h. "Special access program" means a program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level.

4.2. — Section 4.2
General Restrictions on Access

a. A person may have access to classified information provided that:

(1) A favorable determination of eligibility for access has been made by an agency head or the agency head's designee.

(2) The person has signed an approved nondisclosure agreement.

(3) The person has a need–to–know the information.

b. Classified information will remain under the control of the originating agency or its successor in function. An agency will not disclose information originally classified by another agency without its authorization. An official or employee leaving agency service may not remove classified information from the agency's control.

c. Classified information may not be removed from official premises without proper authorization.

d. Persons authorized to disseminate classified information outside the executive branch will assure the protection of the information in a manner equivalent to that provided within the executive branch.

e. Consistent with law, directives and regulation, an agency head or senior agency official will establish uniform procedures to ensure that automated information systems, including networks and telecommunications systems, that collect, create, communicate, compute, disseminate, process, or store classified information have controls that:

(1) Prevent access by unauthorized persons.

(2) Ensure the integrity of the information.

f. Consistent with law, directives and regulation, each agency head or senior agency official will establish controls to ensure that classified information is used, processed, stored, reproduced, transmitted, and destroyed under conditions that provide adequate protection and prevent access by unauthorized persons.

g. Consistent with directives issued pursuant to this Order, an agency will safeguard foreign government information under standards that provide a degree of protection at least equivalent to that required by the government or international organization of governments that furnished the information. When adequate to achieve equivalency, these standards may be less restrictive than the safeguarding standards that ordinarily apply to United States CONFIDENTIAL information, including allowing access to individuals with a need to know who have not otherwise been cleared for access to classified information or executed an approved nondisclosure agreement.

h. Except as provided by statute or directives issued pursuant to this Order, classified information originating in one agency may not be disseminated outside any other agency to which it has been made available without the consent of the originating agency. An agency head or senior agency official may waive this requirement for specific information originated within that agency. For purposes of this section, the Department of Defense will be considered one agency.

4.3. — Section 4.3
Distribution Controls

a. Each agency will establish controls over the distribution of classified information to assure that it is distributed only to organizations or individuals eligible for access who also have a need to know the information.

b. Each agency will update, at least annually, the automatic, routine, or recurring distribution of classified information that they distribute. Recipients will cooperate fully with distributors who are updating distribution lists and will notify distributors whenever a relevant change in status occurs.

4.4. — Section 4.4
Special Access Programs

a. Establishment of special access programs. Unless otherwise authorized by the President, only the Secretaries of State, Defense and Energy, and the Director of Central Intelligence, or the principal deputy of each, may create a special access program. For special access programs pertaining to intelligence activities (including special activities, but not including military operational, strategic and tactical programs), or intelligence sources or methods, this function will be exercised by the Director of Central Intelligence. These officials will keep the number of these programs at an absolute minimum, and will establish them only upon a specific finding that:

(1) The vulnerability of, or threat to, specific information is exceptional.

(2) The normal criteria for determining eligibility for access applicable to information classified at the same level are not deemed sufficient to protect the information from unauthorized disclosure.

(3) The program is required by statute.

b. Requirements and limitations.

(1) Special access programs will be limited to programs in which the number of persons who will have access ordinarily will be reasonably small and commensurate with the objective of providing enhanced protection for the information involved.

(2) Each agency head will establish and maintain a system of accounting for special access programs consistent with directives issued pursuant to this Order.

(3) Special access programs will be subject to the oversight program established under section 5.6(c) of this Order.

In addition, the Director of the Information Security Oversight Office will be afforded access to these programs, in accordance with the security requirements of each program, in Order to perform the functions assigned to the Information Security Oversight Office under this Order. An agency head may limit access to a special access program to the Director and no more than one other employee of the Information Security Oversight Office; or, for special access programs that are extraordinarily sensitive and vulnerable, to the Director only.

(4) The agency head or principal deputy will review annually each special access program to determine whether it continues to meet the requirements of this Order.

(5) Upon request, an agency will brief the Assistant to the President for National Security Affairs, or his or her designee, on any or all of the agency's special access programs.

c. Within 180 days after the effective date of this Order, each agency head or principal deputy will review all existing special access programs under the agency's jurisdiction. These officials will terminate any special access programs that do not clearly meet the provisions of this Order. Each existing special access program that an agency head or principal deputy validates will be treated as if it were established on the effective date of this Order.

d. Nothing in this Order will supersede any requirement made by or under 10 USC 119.

4.5. — Section 4.5
Access by Historical Researchers and Former Presidential Appointees

a. The requirement in Section 4.2.a.3 of this Order that access to classified information may be granted only to individuals who have a need–to–know the information may be waived for persons who:

(1) Are engaged in historical research projects.

(2) Previously have occupied policy–making positions to which they were appointed by the President.

b. Waivers under this section may be granted only if the agency head or senior agency official of the originating agency:

(1) Determines in writing that access is consistent with the interest of national security.

(2) Takes appropriate steps to protect classified information from unauthorized disclosure or compromise, and ensures that the information is safeguarded in a manner consistent with this Order.

(3) Limits the access granted to former presidential appointees to items that the person originated, reviewed, signed, or received while serving as a presidential appointee.

Part 5 – Implementation and Review

5.1. — Section 5.1
Definitions

For purposes of this Order:

a. "Self–inspection" means the internal review and evaluation of individual agency activities and the agency as a whole with respect to the implementation of the program established under this Order and its implementing directives.

b. "Violation" means:

(1) Any knowing, willful or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information.

(2) Any knowing, willful or negligent action to classify or continue the classification of information contrary to the requirements of this Order or its implementing directives.

(3) Any knowing, willful or negligent action to create or continue a special access program contrary to the requirements of this Order.

c. "Infraction" means any knowing, willful or negligent action contrary to the requirements of this Order or its implementing directives that does not comprise a "violation," as defined above.

5.2. — Section 5.2
Program Direction

a. The Director of the Office of Management and Budget, in consultation with the Assistant to the President for National Security Affairs and the co–chairs of the Security Policy Board, will issue such directives as are necessary to implement this Order. These directives will be binding upon the agencies. Directives issued by the Director of the Office of Management and Budget will establish standards for:

(1) Classification and marking principles.

(2) Agency security education and training programs.

(3) Agency self–inspection programs.

(4) Classification and declassification guides.

b. The Director of the Office of Management and Budget will delegate the implementation and monitorship functions of this program to the Director of the Information Security Oversight Office.

c. The Security Policy Board, established by a Presidential Decision Directive, will make a recommendation to the President through the Assistant to the President for National Security Affairs with respect to the issuance of a Presidential directive on safeguarding classified information. The Presidential directive will pertain to the handling, storage, distribution, transmittal and destruction of and accounting for classified information.

5.3. — Section 5.3
Information Security Oversight Office

a. There is established within the Office of Management and Budget an Information Security Oversight Office. The Director of the Office of Management and Budget will appoint the Director of the Information Security Oversight Office, subject to the approval of the President.

b. Under the direction of the Director of the Office of Management and Budget acting in consultation with the Assistant to the President for National Security Affairs, the Director of the Information Security Oversight Office will—

(1) Develop directives for the implementation of this Order.

(2) Oversee agency actions to ensure compliance with this Order and its implementing directives.

(3) Review and approve agency implementing regulations and agency guides for systematic declassification review prior to their issuance by the agency.

(4) Have the authority to conduct on–site reviews of each agency's program established under this Order, and to require of each agency those reports, information, and other cooperation that may be necessary to fulfill its responsibilities. If granting access to specific categories of classified information would pose an exceptional national security risk, the affected agency head or the senior agency official will submit a written justification recommending the denial of access to the Director of the Office of Management and Budget within 60 days of the request for access. Access will be denied pending a prompt decision by the Director of the Office of Management and Budget, who will consult on this decision with the Assistant to the President for National Security Affairs.

(5) Review requests for original classification authority from agencies or officials not granted original classification authority and, if deemed appropriate, recommend presidential approval through the Director of the Office of Management and Budget.

(6) Consider and take action on complaints and suggestions from persons within or outside the government with respect to the administration of the program established under this Order.

(7) Have the authority to prescribe, after consultation with affected agencies, standardization of forms or procedures that will promote the implementation of the program established under this Order.

(8) Report at least annually to the President on the implementation of this Order.

(9) Convene and chair interagency meetings to discuss matters pertaining to the program established by this Order.

5.4. — Section 5.4
Interagency Security Classification Appeals Panel

a. Establishment and Administration.

(1) There is established an Interagency Security Classification Appeals Panel ("Panel"). The Secretaries of State and Defense, the Attorney General, the Director of Central Intelligence, the Archivist of the United States, and the Assistant to the President for National Security Affairs will each appoint a senior level representative to serve as a member of the Panel. The President will select the Chair of the Panel from among the Panel members.

(2) A vacancy on the Panel will be filled as quickly as possible as provided in paragraph 1, above.

(3) The Director of the Information Security Oversight Office will serve as the Executive Secretary. The staff of the Information Security Oversight Office will provide program and administrative support for the Panel.

(4) The members and staff of the Panel will be required to meet eligibility for access standards in Order to fulfill the Panel's functions.

(5) The Panel will meet at the call of the Chair. The Chair will schedule meetings as may be necessary for the Panel to fulfill its functions in a timely manner.

(6) The Information Security Oversight Office will include in its reports to the President a summary of the Panel's activities.

b. Functions. The Panel will—

(1) Decide on appeals by persons who have filed classification challenges under Section 1.9 of this Order.

(2) Approve, deny or amend agency exemptions from automatic declassification as provided in Section 3.4 of this Order.

(3) Decide on appeals by persons or entities who have filed requests for mandatory declassification review under Section 3.6 of this Order.

c. Rules and Procedures. The Panel will issue bylaws, which will be published in the Federal Register no later than

120 days from the effective date of this Order. The bylaws will establish the rules and procedures that the Panel will follow in accepting, considering, and issuing decisions on appeals. The rules and procedures of the Panel will provide that the Panel will consider appeals only on actions in which: (1) the appellant has exhausted his or her administrative remedies within the responsible agency; (2) there is no current action pending on the issue within the federal courts; and (3) the information has not been the subject of review by the federal courts or the Panel within the past two years.

d. Agency heads will cooperate fully with the Panel so that it can fulfill its functions in a timely and fully informed manner. An agency head may appeal a decision of the Panel to the President through the Assistant to the President for National Security Affairs. The Panel will report to the President through the Assistant to the President for National Security Affairs any instance in which it believes that an agency head is not cooperating fully with the Panel.

e. The Appeals Panel is established for the sole purpose of advising and assisting the President in the discharge of his constitutional and discretionary authority to protect the national security of the United States. Panel decisions are committed to the discretion of the Panel, unless reversed by the President.

5.5. — Section 5.5
Information Security Policy Advisory Council

a. Establishment. There is established an Information Security Policy Advisory Council ("Council"). The Council will be composed of seven members appointed by the President for staggered terms not to exceed four years, from among persons who have demonstrated interest and expertise in an area related to the subject matter of this Order and are not otherwise employees of the Federal Government. The President will appoint the Council chair from among the members. The Council will comply with the Federal Advisory Committee Act, as amended, 5 USC App. 2.

b. Functions. The Council will—

(1) Advise the President, the Assistant to the President for National Security Affairs, the Director of the Office of Management and Budget, or such other executive branch officials as it deems appropriate, on policies established under this Order or its implementing directives, including recommended changes to those policies.

(2) Provide recommendations to agency heads for specific subject areas for systematic declassification review.

(3) Serve as a forum to discuss policy issues in dispute.

c. Meetings. The Council will meet at least twice each calendar year, and as determined by the Assistant to the President for National Security Affairs or the Director of the Office of Management and Budget.

d. Administration.

(1) Each Council member may be compensated at a rate of pay not to exceed the daily equivalent of the annual rate of basic pay in effect for grade GS–18 of the general schedule under Section 5376 of Title 5, United States Code, for each day during which that member is engaged in the actual performance of the duties of the Council.

(2) While away from their homes or regular place of business in the actual performance of the duties of the Council, members may be allowed travel expenses, including per diem in lieu of subsistence, as authorized by law for persons serving intermittently in the Government service (5 USC 5703.b).

(3) To the extent permitted by law and subject to the availability of funds, the Information Security Oversight Office will provide the Council with administrative services, facilities, staff, and other support services necessary for the performance of its functions.

(4) Notwithstanding any other Executive Order, the functions of the President under the Federal Advisory Committee Act, as amended, that are applicable to the Council, except that of reporting to the Congress, will be performed by the Director of the Information Security Oversight Office in accordance with the guidelines and procedures established by the General Services Administration.

5.6. — Section 5.6
General Responsibilities

Heads of agencies that originate or handle classified information will—

a. Demonstrate personal commitment and commit senior management to the successful implementation of the program established under this Order.

b. Commit necessary resources to the effective implementation of the program established under this Order.

c. Designate a senior agency official to direct and administer the program, whose responsibilities will include:

(1) Overseeing the agency's program established under this Order, provided, an agency head may designate a separate official to oversee special access programs authorized under this Order. This official will provide a full accounting of the agency's special access programs at least annually.

(2) Promulgating implementing regulations, which will be published in the Federal Register to the extent that they affect members of the public.

(3) Establishing and maintaining security education and training programs.

(4) Establishing and maintaining an ongoing self–inspection program, which will include the periodic review and assessment of the agency's classified product.

(5) Establishing procedures to prevent unnecessary access to classified information, including procedures that i), require that a need for access to classified information is established before initiating administrative clearance

procedures, and ii), ensure that the number of persons granted access to classified information is limited to the minimum consistent with operational and security requirements and needs.

(6) Developing special contingency plans for the safeguarding of classified information used in or near hostile or potentially hostile areas.

(7) Assuring that the performance contract or other system used to rate civilian or military personnel performance includes the management of classified information as a critical element or item to be evaluated in the rating of: (i) original classification authorities; (ii) security managers or security specialists; and (iii) all other personnel whose duties significantly involve the creation or handling of classified information.

(8) Accounting for the costs associated with the implementation of this Order, which will be reported to the Director of the Information Security Oversight Office for publication.

(9) Assigning in a prompt manner agency personnel to respond to any request, appeal, challenge, complaint or suggestion arising out of this Order that pertains to classified information that originated in a component of the agency that no longer exists and for which there is no clear successor in function.

5.7. — Section 5.7
Sanctions

a. If the Director of the Information Security Oversight Office finds that a violation of this Order or its implementing directives may have occurred, the Director will make a report to the head of the agency or to the senior agency official so that corrective steps, if appropriate, may be taken.

b. Officers and employees of the United States Government, and its contractors, licensees, certificate holders, and grantees will be subject to appropriate sanctions if they knowingly, willfully, or negligently:

(1) Disclose to unauthorized persons information properly classified under this Order or predecessor Orders.

(2) Classify or continue the classification of information in violation of this Order or any implementing directive.

(3) Create or continue a special access program contrary to the requirements of this Order.

(4) Contravene any other provision of this Order or its implementing directives.

c. Sanctions may include reprimand, suspension without pay, removal, termination of classification authority, loss or denial of access to classified information, or other sanctions in accordance with applicable law and agency regulation.

d. The agency head, senior agency official, or other supervisory official will, at a minimum, promptly remove the classification authority of any individual who demonstrates reckless disregard or a pattern of error in applying the classification standards of this Order.

e. The agency head or senior agency official will—

(1) Take appropriate and prompt corrective action when a violation or infraction under paragraph b, above, occurs.

(2) Notify the Director of the Information Security Oversight Office when a violation under paragraph b.1, 2 or 3, above, occurs.

Part 6 – General Provisions

6.1. — Section 6.1
General Provisions

a. Nothing in this Order will supersede any requirement made by or under the Atomic Energy Act of 1954, as amended, or the National Security Act of 1947, as amended. “Restricted Data” and “Formerly Restricted Data” will be handled, protected, classified, downgraded, and declassified in conformity with the provisions of the Atomic Energy Act of 1954, as amended, and regulations issued under that Act.

b. The Attorney General, upon request by the head of an agency or the Director of the Information Security Oversight Office, will render an interpretation of this Order with respect to any question arising in the course of its administration.

c. Nothing in this Order limits the protection afforded any information by other provisions of law, including the exemptions to the Freedom of Information Act, the Privacy Act, and the National Security Act of 1947, as amended. This Order is not intended, and should not be construed, to create any right or benefit, substantive or procedural, enforceable at law by a party against the United States, its agencies, its officers, or its employees. The foregoing is in addition to the specific provisos set forth in Sections 1.2.b, 3.2.b and 5.4.e of this Order.

d. Executive Order No. 12356 of April 6, 1982, is revoked as of the effective date of this Order.

6.2. — Section 6.2
Effective Date

This Order will become effective 180 days from the date of its issuance.

William J. Clinton

THE WHITE HOUSE

April 17, 1995

Executive Order 12972 of September 18, 1995

The President

Amendment to Executive Order No. 12958

By the authority vested in me as President by the Constitution and the laws of the United States of America, and in Order to amend Executive Order No. 12958, it is hereby Ordered that the definition of "agency" in Section 1.1.i of such Order is hereby amended to read as follows: (i)"Agency" means any "Executive agency" as defined in 5 USC 105, any "Military department" as defined in 5 USC 102, and "any other entity within the executive branch that comes into the possession of classified information."

William J. Clinton

THE WHITE HOUSE

September 18, 1995

Executive Order 13142 of November 19, 1999

The President

Amendment to Executive Order 12958

By the authority vested in me as President by the Constitution and the laws of the United States of America, and in order to extend and establish specific dates for the time within which all classified information contained in records more than 25 years old that have been determined to have historical value under title 44, United States Code, should be automatically declassified, and to establish the Information Security Oversight Office within the National Archives and Records Administration, it is hereby ordered that Executive Order 12958 is amended as follows:

Sec. 1. In the first sentence of section 3.4(a) of Executive Order 12958, the words "within five years from the date of this order" are deleted and the words "within six and one half years from the date of this order" are inserted in lieu thereof.

Sec. 2. The following new language is inserted at the end of section 3.4(a): "For records otherwise subject to this paragraph for which a review or assessment conducted by the agency and confirmed by the Information Security Oversight Office has determined that they: (1) contain information that was created by or is under the control of more than one agency, or (2) are within file series containing information that almost invariably pertains to intelligence sources or methods, all classified information in such records shall be automatically declassified, whether or not the records have been reviewed, within 8 years from the date of this order, except as provided in paragraph (b), below. For records that contain information that becomes subject to automatic declassification after the dates otherwise established in this paragraph, all classified information in such records shall be automatically declassified, whether or not the records have been reviewed on December 31 of the year that is 25 years from the origin of the information, except as provided in paragraph (b), below."

Sec. 3. Subsections (a) and (b) of section 5.2 are amended to read as follows:

"(a) The Director of the Information Security Oversight Office, under the direction of the Archivist of the United States and in consultation with the Assistant to the President for National Security Affairs and the co–chairs of the Security Policy Board, shall issue such directives as are necessary to implement this order. These directives shall be binding upon the agencies. Directives issued by the Director of the Information Security Oversight Office shall establish standards for:

(1) classification and marking principles;
(2) agency security education and training programs;
(3) agency self–inspection programs; and
(4) classification and declassification guides.

(b) The Archivist of the United States shall delegate the implementation and monitorship functions of this program to the Director of the Information Security Oversight Office."

Sec. 4. Subsection (a) and the introductory clause and item (4) of subsection (b) of section 5.3 are amended as follows:

(a) Subsection (a) shall read "(a) There is established within the National Archives and Records Administration an Information Security Oversight Office. The Archivist of the United States shall appoint the Director of the Information Security Oversight Office, subject to the approval of the President."

(b) The introductory clause of subsection (b) shall read "Under the direction of the Archivist of the United States, acting in consultation with the Assistant to the President for National Security Affairs, the Director of the Information Security Oversight Office shall:

(c) Item (4) of subsection (b) shall read "(4) have the authority to conduct on–site reviews of each agency's program established under this order, and to require of each agency those reports, information, and other cooperation that may be necessary to fulfill its responsibilities. If granting access to specific categories of classified information would pose an exceptional national security risk, the affected agency head or the senior agency official shall submit a written justification recommending the denial of access to the President through the Assistant to the President for National Security Affairs within 60 days of the request for access. Access shall be denied pending the response,".

WILLIAM J. CLINTON

THE WHITE HOUSE,

November 19, 1999.

Appendix C
Special Procedures for Use in Systematic and Mandatory Review of Cryptologic Information

C–1. General guidelines

a. Cryptologic information uncovered in systematic or mandatory review for declassification of 25–year–old government records is not to be declassified by other than the National Security Agency. The information could concern or reveal the processes, techniques, operations, and scope of Signals Intelligence (SIGINT), which consists of Communications Intelligence (COMINT), Electronic Intelligence (ELINT), and Foreign Instrumentation Signals Intelligence (FISINT), or it could concern the components of Information Systems Security (INFOSEC), which consists of Communications Security (COMSEC) and Computer Security (COMPUSEC), including the communications portion of cover and deception plans. Much cryptologic information is also considered "Foreign Government Information" as defined in paragraph 1.l.d of Executive Order 12958.

b. Recognition of cryptologic information cannot always be an easy task. There are several broad classes of cryptologic information, as follows:

(1) Those that relate to INFOSEC. In documentary form, they provide COMSEC/COMPUSEC guidance or information. Many COMSEC/COMPUSEC documents and materials are accountable under the Communications Security Material Control System. Examples are items bearing Telecommunications Security (TSEC) nomenclature and crypto keying material for use in enciphering communications, other COMSEC/COMPUSEC documentation such as the National Telecommunications and Information Systems Security Committee (NTISSC) or its predecessor organization, COMSEC/COMPUSEC Resources Program documents, COMSEC Equipment Engineering Bulletins, COMSEC Equipment System Descriptions, and COMSEC Technical Bulletins.

(2) Those that relate to SIGINT. These appear as reports in various formats that bear security classifications, frequently followed by five letter code–words, ULTRA (from World War II) for example, and often carry warning caveats such as "This document contains code–word material" and "Utmost secrecy is necessary…" or "Handle Via COMINT Channels Only" "HVCCO" or "CCO." Formats can appear as messages having addresses, "from" and "to" sections, and as summaries with SIGINT content with or without other kinds of intelligence and comment.

(3) Research. Research, development, test, life cycle support, planning, and evaluation reports and information that relates to either COMSEC, COMPUSEC, or SIGINT.

C–2. Identification

a. Some commonly used words that help to identify cryptologic documents and materials are: "cipher," "code," "code–word," "Communications Intelligence," "special intelligence," "Communications Security," "Computer Security," "cryptoanalysis," "crypto," "cryptography," "cryptosystem," "decipher," "decode," "decrypt," "direction finding," "Electronic Intelligence," "Electronic Security" (ELSEC), "encipher," "encode," "encrypt," "Foreign Instrumentation Signals Intelligence," "telemetry," "Information Systems Security," "intercept," "key book," "one–time–pad," "bookbreaking," "Signals Intelligence," "Signals Security" (SIGSEC), "TEMPEST," and "Traffic Analysis" (TA).

b. Special procedures apply to the review and declassification of classified cryptologic information. The following will be observed in the review of such information.

(1) INFOSEC (COMSEC/COMPUSEC) Documents and materials.

(2) If records or materials in this category are found in agency or department component files that are not under INFOSEC control, refer them to the senior COMSEC/COMPUSEC authority of the agency or department concerned or return them, by appropriate channels, to the address in paragraph C–2b(5).

(3) If the COMSEC/COMPUSEC information has been incorporated into other documents by the receiving agency, that information must be referred to the National Security Agency/Chief, Central Security Service (NSA/CSS), for review before declassification occurs.

(4) SIGINT (COMINT, ELINT, and FISINT) Information.

(a) If the SIGINT information is contained in a document or record originated by a U.S. Government cryptologic organization and is in the files of a non–cryptologic agency or department, such material will not be declassified. The material can be destroyed unless the holding agency's approved records disposition schedule requires its retention. If the material must be retained, it must be referred to the NSA/CSS for systematic review for declassification when it becomes 25 years old.

(b) If the SIGINT information has been incorporated by the receiving agency into documents it produces, referral of the SIGINT information to the NSA/CSS for review is necessary prior to any declassification action.

(5) COMSEC/COMPUSEC or SIGINT information which requires declassification by the NSA/CSA should be sent to: Director, National Security Agency, Chief, Central Security Service, ATTN: Information Policy Staff (N5P6), Fort George G. Meade, MD 20755–6000.

Appendix D
Security Controls on Dissemination and Marking of Warning Notices on Intelligence Information

D–1. General

Intelligence information will be controlled and marked in accordance with Director of Central Intelligence Directive (DCID) 1/7, "Security Controls on the Dissemination of Intelligence Information", included as figure D–1 of this appendix, and future revisions. Control markings as well as all other policy stipulated in DCID 1/7 apply solely to intelligence information and not to other classified information. Except as specifically stipulated in this appendix, intelligence information will be safeguarded in the same manner as other types of classified information of the same classification level.

a. Department of the Army security education and awareness programs will include the provisions of DCID 1/7.

b. The challenge procedures regarding classification of information contained in this regulation will be followed in implementing the challenge procedures concerning intelligence information as stipulated in section 14.2 of DCID 1/7.

c. The procedures regarding the investigation and reporting of the compromise of classified information, contained in this regulation, will be followed for classified intelligence. If the compromise involves the intelligence of another (non–DA) agency, a report will be made to the Director of Central Intelligence, through command channels (DAMI–CH), and the agency that originated the intelligence.

d. These classification and control markings, and their authorized abbreviations, are compiled in the Authorized Classification and Control Markings Register, maintained by the Controlled Access Program Coordination Office (CAPCO). The Authorized Classification and Control Markings Register is available, on Intelink–TS at: http://www.cms.ic.gov/capco/ and on Intelink–S at: http://www.cms.cia.sgov.gov/capco/. Examples of proper marking of intelligence community documents can be found at figures D–2 and D–3.

D–2. Responsibilities

a. The HQDA Deputy Chief of Staff for Intelligence (DCSINT) is the principal DA proponent for intelligence policy matters, to include the security controls on dissemination of intelligence information. The DCSINT is the DA Senior Official of the Intelligence Community (SOIC).

b. The DCSINT has, effective by this regulation, delegated to the senior intelligence official at each MACOM, and to the Administrative Assistant to the Secretary of the Army for HQDA staff offices and activities, authority to execute all the provisions of DCID 1/7 that refer to the "designee" of the SOIC. Those designees may further delegate this authority, in writing, to the senior intelligence official at major subordinate commands. This authority includes the release of intelligence information to contractors and consultants, subject to the conditions of this regulation. This includes those situations requiring access in response to a formal solicitation, such as a request for proposal, invitation to bid, or similar solicitation request.

c. The DCSINT has, effective by this regulation, delegated to the Director, Defense Security Service (DSS), the authority to release intelligence information to appropriately cleared U.S. contractors supporting an Army mission, and

having a demonstrated need to know, subject to the controls of DCID 1/7, to include those in section 6. The Director, DSS can further delegate this authority to subordinate DSS officials.

d. Army personnel, to include those who are not original classification authorities, who generate classified intelligence products or incorporate intelligence information in primarily non–intelligence products, are authorized and will apply, effective by DCID 1/7, control markings specified in DCID 1/7, section 9.

D–3. General Guidance

a. Under this classification marking system, for documents containing intelligence information, the following rules apply to the classification line, used at the top and bottom of each page of a document, and portion marking:

(1) The full classification line must be conspicuously placed at both the top and bottom of each page of a classified document, or an unclassified document which either has other control markings or is being transmitted electronically. Note: It is optional to mark UNCLASSIFIED on the top and bottom of documents which are not classified and bear no other control markings, such as FOUO or PROPIN.

(2) The classification line and portion markings always use uppercase letters.

(3) The specified U.S. or non–U.S. classification portion of the classification line at the top and bottom of page must be spelled out in full and in English, and may not be abbreviated. Any other information included on the classification line may be spelled out or abbreviated unless otherwise directed by component policy. Note: All classified and unclassified information which bears any control markings, must bear either a U.S. or non–U.S. classification marking, but not both, at the top and bottom of each page.

(4) If the classification is TOP SECRET, SECRET, or CONFIDENTIAL, there must be a declassification date or exemption entry (for example, TOP SECRET//17 December 2001 or SECRET//X1). The full class/declass block, required by EO 12958, must still appear on the first page of a classified document.

(5) The pertinent caveats from each category in the Authorized Classification and Control Markings Register form a field in the classification line or portion marking. Fields are always separated by a double right slash (for example, (U// FOUO).

(6) Only fields with entries applicable to the document are represented in the classification line. No slashes, hyphens, or spaces, are used to hold the place of fields with no entries applicable to the document.

(7) Only one entry may appear in the U.S. classification, non–U.S. classification, and declassification date fields.

(8) All information may only bear one classification marking, either U.S. or non–U.S..

(9) Multiple entries may be chosen from the SCI Control System, Dissemination Control, and Non–Intelligence Community Marking categories, if the entries are applicable to the document. If multiple entries are used within the field, they are listed in the order in which they appear in the Authorized Classification and Control Markings Register.

(a) For multiple SCI Control System entries, use a single right slash as the separator between the individual SCI Control System entries.

(b) Use a comma with no space interjected as the separator between multiple Dissemination Control or multiple Non–Intelligence Community Marking entries.

(10) Portion markings are to be included at the beginning of the respective portion and enclosed in parentheses. Standard marking separators (slashes, hyphens, commas, etc.) are to be used where necessary.

(11) The order for markings must follow the order in which the markings appear in the Authorized Classification and Control Markings Register.

b. Some of the dissemination control and non–intelligence community markings are restricted to use by certain agencies. Non–U.S. classification markings are restricted to the respective countries or international organizations. In addition, some of the markings in the register are prohibited from use with other markings. Further information is provided in the "Relationship to Other Markings" column of the Authorized Classification and Control Markings Register.

Director of Central Intelligence Directive (DCID) 1/7, Security Controls on the Dissemination of Intelligence Information

DIRECTOR OF CENTRAL INTELLIGENCE DIRECTIVE 1/7[1]

Security Controls on the Dissemination of Intelligence Information

(Effective 30 June 1998)

Introduction

Pursuant to the provisions of the National Security Act of 1947, as amended, Executive Order 12333, Executive Order 12958 and implementing directives thereto, policies, controls, and procedures for the dissemination and use of intelligence information and related materials are herewith established in this Director of Central Intelligence Directive (Directive or DCID). Nothing in this policy is intended to amend, modify, or derogate the authorities of the DCI contained in Statute or Executive Order.

Figure D-1. Director of Central Intelligence Directive (DCID) 1/7, Security Controls on the Dissemination of Intelligence Information

1.0. Policy

1.1.
It is the policy of the DCI that intelligence be produced in a way that balances the need for maximum utility of the information to the intended recipient with protection of intelligence sources and methods. The controls and procedures established by this directive should be applied uniformly in the dissemination and use of intelligence originated by all Intelligence Community components in accordance with the following principles:

1.1.1.
Originators of classified intelligence information should write for the consumer. This policy is intended to provide for the optimum dissemination of timely, tailored intelligence to consumers in a form that allows use of the information to support all need to know customers.

1.1.2.
The originator of intelligence is responsible for determining the appropriate level of protection prescribed by classification and dissemination policy. Originators shall take a risk management approach when preparing information for dissemination.

2.0. Purpose

2.1.
This directive establishes policies, controls, and procedures for the dissemination and use of intelligence information to ensure that, while facilitating its interchange for intelligence purposes, it will be adequately protected. This directive implements and amplifies applicable portions of the directives of the Information Security Oversight Office issued pursuant to Executive Order (EO) 12958 and directives of the Security Policy Board issued pursuant to EO 12958 and PDD–29.

2.2.
Additionally, this directive sets forth policies and procedures governing the release of intelligence to contractors and consultants, foreign governments, international organizations or coalition partners consisting of sovereign states, and to foreign nationals and immigrant aliens, including those employed by the US Government.

2.3.
Executive Order 12958 provides for the establishment of Special Access Programs, including Sensitive Compartmented Information. DCID 3/29 provides procedures for the establishment and review of Special Access Programs pertaining to intelligence activities and restricted collateral information. Intelligence Community components may establish and maintain dissemination controls on such information as approved under the policies and procedures contained in DCID 3/29, this DCID, and implementing guidance.

3.0. Definitions

3.1.
“Caveated” information is information subject to one of the authorized control markings under section 9.

3.2.
Intelligence Community (and agencies within the Intelligence Community) refers to the United States Government agencies and organizations and activities identified in section 3 of the National Security Act of 1947, as amended, 50 USC 401a(4), and section 3.4(f) (1 through 6) of Executive Order 12333.

3.3.
Intelligence information and related materials (hereinafter referred to as “Intelligence”) include the following information, whether written or in any other medium, classified pursuant to EO 12958 or any predecessor or successor Executive Order:

3.3.1.
Foreign intelligence and counterintelligence defined in the National Security Act of 1947, as amended, and in Executive Order 12333;

3.3.2.
Information describing US foreign intelligence and counterintelligence activities, sources, methods, equipment, or methodology used for the acquisition, processing, or exploitation of such intelligence; foreign military hardware obtained through intelligence activities for exploitation and the results of the exploitation; and any other data resulting from US intelligence collection efforts; and,

3.3.3.
Information on Intelligence Community protective security programs (e.g., personnel, physical, technical, and information security).

3.4.
"Need–to–know" is the determination by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function. Such persons shall possess an appropriate security clearance and access approval granted pursuant to Executive Order 12968, Access to Classified Information.

3.5.
Senior Official of the Intelligence Community (SOIC) is the head of an agency, office, bureau, or other intelligence element as identified in section 3 of the National Security Act of 1947, as amended, 50 USC 401a(4), and section 3.4(f) (1 through 6) of Executive Order 12333.

3.6.
A "tear line" is the place on an intelligence report (usually denoted by a series of dashes) at which the sanitized version of a more highly classified and/or controlled report begins. The sanitized information below the tear line should contain the substance of the information above the tear line, but without identifying the sensitive sources and methods. This will permit wider dissemination, in accordance with the "need to know" principle and foreign disclosure guidelines, of the information below the tear line.

4.0. General Applicability

4.1.
In support of the policy statement in section 1.0, classifiers of intelligence information shall take a risk management approach when preparing information for dissemination. In the interest of the widest possible dissemination of information to consumers with a "need to know", classifiers shall carefully consider the needs of all appropriate intelligence consumers regarding sources and methods information or sensitive analytic comments and use control markings only when necessary and in accordance with this directive, using tear lines and other formats to meet consumer needs for intelligence.

4.2.
In carrying out this policy, intelligence producers shall prepare their reports and products at the lowest classification level commensurate with expected damage that could be caused by unauthorized disclosure. When necessary, the material should be prepared in other formats (e.g. tear line form) to permit broader dissemination or release of information.

4.3.
All material shall be portion marked to allow ready identification of information that cannot be broadly disseminated or released, except for material for which a waiver has been obtained under EO 12958.

4.4.
The substance of this directive shall be promulgated by each Intelligence Community component, and appropriate procedures permitting prompt interagency consultation established.

5.0. Use By and Dissemination Among Executive Branch Departments/Agencies of the US Government

5.1.
Executive Order 12958 provides that classified information originating in one US department or agency shall not be disseminated beyond any recipient agency without the consent of the originating agency. However, to facilitate use and dissemination of intelligence within and among Intelligence Community components and to provide for the timely flow of intelligence to consumers, the following controlled relief to the "third agency rule" is hereby established:

5.1.1.
Each Intelligence Community component consents to the use of its classified intelligence in classified intelligence products of other Intelligence Community components, including its contractors under section 6, and to the dissemination of those products within executive branch departments/agencies of the US Government, except as specifically restricted by controls defined in this directive or other DCI guidance.

5.1.2.
As provided in 5.1.1, classified intelligence that bears no restrictive control markings may be given secondary US dissemination in classified channels to any U.S. Executive Branch department/agency not on original distribution if: (a) the intelligence has first been sanitized by the removal of all references and inferences to intelligence sources and methods and the identity of the producing agency; or (b) if the product is not so sanitized, the consent of the originator has been obtained. If there is any doubt concerning a reference or inference to intelligence sources and methods, relevant intelligence documents should not be given secondary dissemination until the recipient has consulted with the originator.

5.1.3.
Any component disseminating intelligence beyond the Intelligence Community assumes responsibility for ensuring that recipient organizations agree to observe the need–to–know principle and the restrictions prescribed by this directive, and to maintain adequate safeguards.

6.0. Policy and Procedures Governing the Release of Intelligence to Contractors and Consultants

6.1.
SOICs, or their designees, may release intelligence to appropriately cleared or access–approved US contractors and consultants (hereinafter "contractor") having a demonstrated "need–to–know" without referral to the originating agency prior to release provided that:

6.1.1.
At the initiation of the contract, the SOIC or his/her designee specifies and certifies in writing that disclosure of the specified information does not create an unfair competitive advantage for the contractor or a conflict of interest with the contractor's obligation to protect the information. If, during the course of the contract, the contractor's requirements for information changes to require new or significantly different information, the SOIC or his/her designee shall make a new specification and certification. In cases where the designated official cannot or does not resolve the issue of unfair competitive advantage or conflict of interest, consent of the originator is required;

6.1.2.
Release is made only to contractors certified by the SOIC (or designee) of the sponsoring organization as performing classified services in support of a national security mission;

6.1.3.
The contractor has an approved safeguarding capability if retention of the intelligence is required;

6.1.4.
Contractors are not authorized to disclose further or release intelligence to any of their components or employees or to another contractor (including subcontractors) without the prior written notification and approval of the SOIC or his/her designee unless such disclosure or release is authorized in writing at the initiation of the contract as an operational requirement;

6.1.5.
Intelligence released to contractors, all reproductions thereof, and all other material generated based on, or incorporating data therefrom (including authorized reproductions), remain the property of the US Government. Final disposition of intelligence information shall be governed by the sponsoring agency;

6.1.6.
National Intelligence Estimates (NIEs), Special National Intelligence Estimates (SNIEs), and Interagency Intelligence Memoranda may be released to appropriately cleared contractors possessing an appropriate level facility clearance and need–to–know, except as regulated by provisions concerning proprietary information as defined in sections 6.1.7 and 9.3, below;

6.1.7.
Except as provided in section 6.3 below, intelligence that bears the control marking "CAUTION–PROPRIETARY

INFORMATION INVOLVED" (abbreviated "PROPIN" or "PR") may not be released to contractors, unless prior permission has been obtained from the originator and those providing the intelligence to the originator. Intelligence that bears the control marking, "DISSEMINATION AND EXTRACTION OF INFORMATION CONTROLLED BY ORIGINATOR" (abbreviated "ORCON") may only be released to contractors within Government facilities. These control markings are further described under sections 9.2 and 9.3, below; and

6.1.8.
Authorized release to foreign nationals or foreign contractors is undertaken through established channels in accordance with sections 7 and 8, and DCID 5/6, Intelligence Disclosure Policy, and the National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations (abbreviated title: National Disclosure Policy 1 or NDP 1) to the extent consistent with DCIDs and other DCI guidance.

6.2. Policies and Procedures for Contractors Inside Government Owned or Controlled Facilities

6.2.1.
Contractors who perform duties inside a Government owned or controlled facility will follow the procedures and policies of that sponsoring Intelligence Community member in accordance with section 6.1 of this directive.

6.3. Policies and Procedures for Contractors Outside Government Owned or Controlled Facilities

6.3.1.
Contractors who perform duties outside of Government owned or controlled facilities will adhere to the following additional policies and procedures:

6.3.1.1.
The SOIC of the sponsoring agency, or his/her designee, is responsible for ensuring that releases to contractors of intelligence marked ORCON and/or PROPIN are made only with the consent of the originating agency pursuant to this directive and through established channels; (See sections 9.2 and 9.3);

6.3.1.2.
The sponsoring agency shall maintain a record of material released;

6.3.1.3.
Contractors shall establish procedures to control all intelligence received, produced, and held by them in accordance with the provisions of the National Industrial Security Program Operating Manual. This will not impose internal receipt and document accountability requirements for internal traceability and audit purposes;

6.3.1.4.
All reproductions and extractions of intelligence shall be classified, marked, and controlled in the same manner as the original(s);

6.3.1.5.
Sensitive Compartmented Information released to contractors shall be controlled pursuant to the provisions of DCID 1/19, Security Policy for Sensitive Compartmented Information (SCI); and,

6.3.1.6.
Sponsoring agencies shall delete any reference to the Central Intelligence Agency (CIA), the phrase "Directorate of Operations" and any of its components, the place acquired, the field number, the source description, and field dissemination from all CIA Directorate of Operations reports passed to contractors, unless prior approval to do otherwise is obtained from CIA.

7.0. Release to Foreign Governments, International Organizations, and Coalition Partners

7.1.
It is the policy of the DCI that intelligence may be shared with foreign governments, and international organizations or coalition partners consisting of sovereign states to the extent such sharing promotes the interests of the United States, is consistent with US law, does not pose unreasonable risk to US foreign policy or national defense, and is limited to a specific purpose and normally of limited duration. The release of intelligence to such entities is subject to this directive, DCID 5/6, Intelligence Disclosure Policy, and NDP 1 to the extent consistent with DCIDs and other DCI guidance.

7.1.1.
Intelligence Community elements shall restrict the information subject to control markings to the minimum necessary.

If it is not possible to prepare the entire report at the collateral, uncaveated level, IC elements shall organize their intelligence reports and products to identify clearly information not authorized for release to foreign entities.

7.2.
Intelligence information that bears no specific control marking may be released to foreign governments, international organizations, or coalition partners provided that:

7.2.1.
A positive foreign disclosure decision is made by a Designated Intelligence Disclosure Official in accordance with procedures in DCID 5/6;

7.2.2.
No reference is made to the originating agency or to the source of the documents on which the released product is based; and,

7.2.3.
The source or manner of acquisition of the intelligence (including analytic judgments or techniques), and/or the location where the intelligence was collected (if relevant to protect sources and methods) is not revealed and cannot be deduced in any manner.

7.3.
RESTRICTED DATA and FORMERLY RESTRICTED DATA may only be released to foreign governments pursuant to an agreement for cooperation as required by sections 123 and 144 of Public Law 585, Atomic Energy Act of 1954, as amended.

8.0. Dissemination to Non–Governmental Foreign Nationals or Foreign Contractors

8.1.
It is the policy of the DCI that no classified intelligence will be shared with foreign nationals, foreign contractors, or international organizations not consisting of sovereign states, except in accordance with the provisions of this section.

8.2.
Intelligence, even though it bears no restrictive control markings, will not be released in any form to foreign nationals or immigrant aliens (including those employed by, used by, or integrated into the US Government) without the permission of the originator. In such cases where permission of the originator has been granted, the release must be in accordance with DCID 5/6, and the NDP 1 to the extent consistent with DCIDs and other DCI guidance.

8.3.
Release of intelligence to a foreign contractor or company under contract to the US Government must be through the foreign government of the country which the contractor is representing, unless otherwise directed in government–to–government agreements or there is an appropriate US channel for release of the information. Provisions concerning release to foreign governments is contained in section 7.0, above.

9.0. Authorized Control Markings

9.1.
DCI policy is that the authorized control markings for intelligence information in this section shall be individually assigned as prescribed by an Original Classification Authority (OCA) or by officials designated by a SOIC and used in conjunction with security classifications and other markings specified by Executive Order 12958 and its implementing directive(s). Unless originator consent is obtained, these markings shall be carried forward to any new format or medium in which the same information is incorporated.

9.1.1.
To the maximum extent possible, information assigned an authorized control marking shall not be combined with uncaveated information in such a way as to render the uncaveated information subject to the control marking. To fulfill the requirements of paragraph 9.6.1 below, SOICs shall establish procedures in implementing directives to expedite further dissemination of essential intelligence. Whenever possible, caveated intelligence information reports should include the identity and contact instructions of the organization authorized to approve further dissemination on a case–by–case basis.

9.2. "DISSEMINATION AND EXTRACTION OF INFORMATION CONTROLLED BY ORIGINATOR" (ORCON)

9.2.1.
This marking (ORCON or abbreviated OC) may be used only on classified intelligence that clearly identifies or would reasonably permit ready identification of intelligence sources or methods that are particularly susceptible to countermeasures that would nullify or measurably reduce their effectiveness. It is used to enable the originator to maintain continuing knowledge and supervision of distribution of the intelligence beyond its original dissemination. This control marking may not be used when access to the intelligence information will reasonably be protected by use of its classification markings, i.e., CONFIDENTIAL, SECRET or TOP SECRET, or by use of any other control markings specified herein or in other DCIDs. Requests for further dissemination of intelligence bearing this marking shall be reviewed in a timely manner.

9.2.2.
Information bearing this marking may be disseminated within the headquarters and specified subordinate elements of recipient organizations, including their contractors within Government facilities. This information may also be incorporated in whole or in part into other briefings or products, provided the briefing or intelligence product is presented or distributed only to original recipients of the information. Dissemination beyond headquarters and specified subordinate elements or to agencies other than the original recipients requires advance permission from the originator.

9.2.3.
Information bearing this marking must not be used in taking investigative or legal action without the advance permission of the originator.

9.2.4.
As ORCON is the most restrictive marking herein, agencies that originate intelligence will follow the procedures established in the classified DCID 1/7 Supplement, "Guidelines for Use of ORCON Caveat."

9.3.
"CAUTION–PROPRIETARY INFORMATION INVOLVED" (PROPIN). This marking is used, with or without a security classification, to identify information provided by a commercial firm or private source under an express or implied understanding that the information will be protected as a proprietary trade secret or proprietary data believed to have actual or potential value. This marking may be used on government proprietary information only when the government proprietary information can provide a contractor(s) an unfair advantage, such as US Government budget or financial information. Information bearing this marking shall not be disseminated outside the Federal Government in any form without the express permission of the originator of the intelligence and provider of the proprietary information. This marking precludes dissemination to contractors irrespective of their status to, or within, the US Government without the authorization of the originator of the intelligence and provider of the information. This marking shall be abbreviated "PROPIN" or "PR."

9.4.
"NOT RELEASABLE TO FOREIGN NATIONALS" – NOFORN (NF). This marking is used to identify intelligence which an originator has determined falls under the criteria of DCID 5/6, "Intelligence Which May Not Be Disclosed or Released," and may not be provided in any form to foreign governments, international organizations, coalition partners, foreign nationals, or immigrant aliens without originator approval.

9.5.
"AUTHORIZED FOR RELEASE TO..(name of country(ies)/international organization)" (REL TO). This control marking is used when a limited exception to the marking requirements in section 9.4 may be authorized to release the information beyond US recipients. This marking is authorized only when the originator has an intelligence sharing arrangement or relationship with a foreign government approved in accordance with DCI policies and procedures that permits the release of the specific intelligence information to that foreign government, but to no other in any form without originator consent.

9.6. Further Dissemination of Intelligence with Authorized Control Marking(s)

9.6.1.
This directive does not restrict an authorized recipient of intelligence at any level from directly contacting the originator of the intelligence to ask for relief from a specific control marking(s) in order to further disseminate intelligence material to additional users for which the authorized original recipient believes there is a valid need–to–know. Authorized recipients are encouraged to seek such further dissemination through normal liaison

channels for release to US Government agencies or contractors and through foreign disclosure channels for foreign release, on a case–by–case basis, in order to expedite further dissemination of essential intelligence.

9.6.2.
Authorized recipients may obtain information regarding points of contact at agencies that originate intelligence from their local dissemination authorities or from instructions issued periodically by these intelligence producers. Intelligence products often also carry a point of contact name/office and telephone number responsible for the product. If no other information is available, authorized recipients are encouraged to contact the producing agency of the document to identify the official or office authorized to provide relief from authorized control marking(s).

9.6.3.
If there are any questions about whom to contact for guidance, recipients are also encouraged to contact the Director of Central Intelligence (DCI) representative at the Commander–in–Chief (CINC) Headquarters, overseas mission, trade delegation, or treaty negotiating team under which they operate.

9.7.
A SOIC may authorize the use of additional security control markings for Sensitive Compartmented Information (SCI), Special Access Program (SAP) information, restricted collateral information, or other classified intelligence information, consistent with policies and procedures contained in DCID 3/29 and this directive. A uniform list of security control markings authorized for dissemination of classified information by components of the Intelligence Community, and the authorized abbreviated forms of such markings, shall be compiled in the central register maintained pursuant to DCID 3/29. The forms of the markings and abbreviations listed in this register shall be the only forms of those markings used for dissemination of classified information by components of the Intelligence Community, unless an exception is specifically authorized by a SOIC.

10.0. Dissemination and Disclosure Under Emergency Conditions

10.1.
Certain emergency situations4 that involve an imminent threat to life or mission warrant dissemination of intelligence to organizations and individuals not routinely included in such dissemination. When the National Command Authority (NCA) directs that an emergency situation exists, SOICs will ensure that intelligence support provided to the ongoing operations conforms with this directive, DCID 5/6, and NDP 1 to the maximum extent practical and consistent with the mission.

10.1.1.
Dissemination of intelligence under this provision is authorized only if: (a) an authority designated by the military commander or civilian official determines that adherence to this DCID reasonably is expected to preclude timely dissemination to protect life or mission; (b) disseminations are for limited duration and narrowly limited to persons or entities that need the information within 72 hours to satisfy an imminent emergency need; and (c) there is insufficient time to obtain approval through normal intelligence disclosure channels.

10.1.2.
The disclosing authority will report the dissemination through normal disclosure channels within 24 hours of the dissemination, or at the earliest opportunity thereafter as the emergency permits. For purposes of this provision, planning for contingency activities or operations not expected to occur within 72 hours does not constitute “imminent” need that warrants exercise of the emergency waiver to bypass the requirements of this DCID.

10.1.3.
Military commanders and/or responsible civilian officials will ensure that written guidelines for emergency dissemination contain provisions for safeguarding disseminated intelligence and notifying producers of disclosures of information necessary to meet mission requirements.

10.1.4.
The NCA, and/or major commands or responsible civilian officials will immediately advise intelligence producers when the emergency situation ends.

11.0. Procedures Governing Use of Authorized Control Markings

11.1.
Any recipient desiring to disseminate intelligence in a manner contrary to the control markings established by this directive must obtain the advance permission of the agency that originated the intelligence. Such permission applies only to the specific purpose agreed to by the originator and does not automatically apply to all recipients. Producers of

intelligence will ensure that prompt consideration is given to recipients' requests with particular attention to reviewing and editing, if necessary, sanitized or paraphrased versions to derive a text suitable for release subject to lesser or no control marking(s).

11.2.
The control markings authorized above shall be shown on the title page, front cover, and other applicable pages of documents; incorporated in the text of electrical communications; shown on graphics; and associated (in full or abbreviated form) with data stored or processed in automated information systems. The control markings also shall be indicated by parenthetical use of the marking abbreviations at the beginning or end of the appropriate portions in accordance with EO 12958.

12.0. Obsolete Restrictions and Control Markings

12.1.
The following control markings are obsolete and will not be used in accordance with the following guidelines:

12.1.1.
WNINTEL and NOCONTRACT. The control markings, Warning Notice – Intelligence Sources or Methods Involved (WNINTEL), and NOT RELEASABLE TO CONTRACTORS/CONSULTANTS (abbreviated NOCONTRACT or NC) were rendered obsolete effective 12 April 1995. No permission of the originator is required to release, in accordance with this directive, material marked WNINTEL. Holders of documents prior to 12 April 1995 bearing the NOCONTRACT marking should apply the policies and procedures contained in section 6.1 for possible release of such documents.

12.1.2.
Remarking of material bearing the WNINTEL, or NOCONTRACT, control marking is not required; however, holders of material bearing these markings may line through or otherwise remove the marking(s) from documents or other material.

12.1.3.
Other obsolete markings include: WARNING NOTICE–INTELLIGENCE SOURCES OR METHODS INVOLVED, WARNING NOTICE–SENSITIVE SOURCES AND METHODS INVOLVED, WARNING NOTICE–INTELLIGENCE SOURCES AND METHODS INVOLVED, WARNING NOTICE–SENSITIVE INTELLIGENCE SOURCES AND METHODS INVOLVED, CONTROLLED DISSEM, NSC PARTICIPATING AGENCIES ONLY, INTEL COMPONENTS ONLY, LIMITED, CONTINUED CONTROL, NO DISSEM ABROAD, BACKGROUND USE ONLY, USIB ONLY, NFIB ONLY.

12.2.
Questions with respect to current applications of all control markings authorized by earlier directives on the dissemination and control of intelligence and used on documents issued prior to the effective date of this directive should be referred to the agency or department originating the intelligence so marked.

13.0. Reporting Unauthorized Disclosures

13.1.
Violations of the foregoing restrictions and control markings that result in unauthorized disclosure by one agency of the intelligence of another shall be reported to the Director of Central Intelligence through appropriate Intelligence Community channels.

14.0. Responsibilities of SOICs

14.1.
SOICs shall be responsible for the implementation of internal controls and shall conduct training to ensure that the dissemination and release policies contained in this directive and the limitations on the use of control markings are followed. SOICs shall assure that agency personnel are accountable for the proper marking of classified information under this directive and section 5.6 of EO 12958.

14.2.
SOICs shall establish challenge procedures by which US consumers may register complaints about the misuse of control markings or the lack of use of tear line reporting or portion marking. Information concerning such challenges shall be provided to the Security Policy Board staff upon request or for the annual review.

15.0. Annual Report on the Use of Control Markings

15.1.

The Security Policy Board staff shall report to the DCI and Deputy Secretary of Defense on Intelligence Community compliance with this directive, including recommendations for further policies in this area. The report will include an in–depth evaluation of the use of control markings in intelligence reporting/production, including consumer evaluations and producer perspectives on implementation of the directive. The report shall also include information and statistics on challenges formally lodged pursuant to agency procedures under section 1.9 of Executive Order 12958 within and among intelligence agencies on the use of control markings, including their adjudication and the number of times the authority in section 10 was used and the documents provided. In order to inform the Security Policy Board staff of substantive detail in these areas for purposes of this review, Intelligence Community elements shall respond to requests for information from the Security Policy Board staff. Intelligence Community elements may build this program into their Self–Inspection programs under EO 12958. The Security Policy Board staff shall also obtain pertinent information on this subject from intelligence consumers as required.

15.2.

The report required by this section shall be conducted annually, unless otherwise directed by the DCI. The Staff Director, Security Policy Board shall establish the schedule for the report.

16.0. Interpretation

16.1.

Questions concerning the implementation of this policy and these procedures shall be referred to the Community Management Staff.

_____/S/_____ 30 June 1998
Director of Central Intelligence Date

ENDNOTES:

[1]This directive supersedes DCID 1/7, dated 12 April 1995

[2]Recipients will apprise originating agencies as to which components comprise the headquarters element and identify subordinate elements that may be included as direct recipients of intelligence information.

[3]This provision is a requirement of the Trade Secrets Act, as amended (18 USC 1905). The consent of the originator is required to permit release of material marked CAUTION–PROPRIETARY INFORMATION INVOLVED, PROPIN, or PR to other than federal government employees.

[4]For the purposes of implementing this portion of the DCID, “emergency situation” is defined as one of the following:

a) Declared Joint Chiefs of Staff (JCS) alert condition of defense emergency, air defense emergency or Defense Readiness Condition (DEFCON) 3;
b) Hostile action(s) being initiated against the United States or combined US/coalition/friendly forces;
c) US persons or facilities being immediately threatened by hostile forces;
d) US or combined US/coalition/friendly forces planning for or being deployed to protect or rescue US persons, or US/coalition/friendly forces;
e) US civilian operations in response to US or international disasters/catastrophes of sufficient severity to warrant Presidential declared disaster assistance/relief.

Sample of Marking an Originally Classified Intelligence Community Document

CLASSIFICATION MARKINGS FOR TRAINING PURPOSES ONLY
SECRET//X1

Subject: Sample of Marking an Originally Classified Intelligence Community Document (U)

1. (S) This page is UNCLASSIFIED and is marked SECRET for training purposes only. IMPORTANT: You must be an Original Classification Authority to originally classify a document. In most cases, documents are classified based on a Security Classification Guide or guidance (that was approved by an OCA) or upon information taken out of a source document (or both). This sample memo only pertains to those relatively few cases in which an OCA is generating a document that the OCA is originally classifying.

2. (C) The OCA must be identified (see paragraph 4-8a), the reason that the information is classified must be stated (see paragraph 4-9), and the OCA must indicate a date, event, or exemption category for declassification (see paragraph 4-9a). If there is more than one reason or exemption, then all must be listed. In this example, the OCA has selected reason 1.5(c) (intelligence activities, intelligence sources or methods, or cryptology). Instead of a date or event for declassification within 10 years, the OCA has authorized exemption category X1 (information that would reveal an activity, intelligence source, or methods), or a cryptologic system or activity that must be protected beyond 10 years).

I.M. Trying
Director, Security Awareness

Classified by: LTG A. SECRET, Chief of Intelligence Programs, Army Security Is Important Command
Reason: 1.5(c)

Declassify on: X1

Date of source: 26 March 1999

SECRET//X1
CLASSIFICATION MARKINGS FOR TRAINING PURPOSES ONLY

Figure D-2. Sample of Marking an Originally Classified Intelligence Community Document

Sample of Marking Foreign Government Intelligence Information

CLASSIFICATION MARKINGS FOR TRAINING PURPOSES ONLY

//FGI SECRET//X5

SUBJECT: Sample of Marking Foreign Government Intelligence (FGI) Information (U)

1. (U) The U.S. Government affords protection to information provided by foreign governments. Care must be taken to identify the source of the information.

2. (//FGI C) Mark the portions that contain the foreign government information to indicate the country of origin and the classification level. Substitute the words "Foreign Government Information" or "FGI" where the identity of the specific government must be concealed. The identity of the concealed foreign source in this example must be maintained with the record copy and adequately protected.

3. (//FGI S) This paragraph contains information marked "SECRET" by the government of a foreign country. The "Derived From" citation should cite the title and date of the document provided. Declassification date, event, or exemption category is carried forward, if known.

Derived From: Foreign Government Source Document, *(fill-in date)*

Declassify On: X5, FGI

//FGI SECRET//X5

CLASSIFICATION MARKINGS FOR TRAINING PURPOSES ONLY

Figure D-3. Sample of Marking Foreign Government Intelligence Information

Appendix E
Security Procedures for Documents Created for and on Automated Information Systems and Internet Web–based Display

Section I
Documents Produced by AIS Equipment and Electronic Mail

E–1. Introduction

a. As the level of technological advances increases more and more, it is beginning to be commonplace for units to create and communicate via automated information systems. Reports, training, inventories, and other day–to–day operations are created, transmitted and displayed with computers. Many units and agencies now create and maintain Internet websites, not only on the open unclassified systems, but also on all levels of classified Local Area Networks (LANs) and Wide Area Networks (WANs). Until now, there have been no definitive instructions regarding the handling of these types of materials and systems. Particularly, this is true when it comes to classification marking. The creation of these "digital documents" is probably the only time that the rules governing who can be the originating authority do not apply. Hopefully by explaining the procedures for handling these materials it will eliminate the possibility of accidental security violations.

b. The World Wide Web (WWW) provides the Department of the Army with a powerful tool to convey information quickly and efficiently on a broad range of topics relating to its activities, objectives, policies, programs, and personnel. The global reach of the web makes this information easily accessible to the men and women of the Armed Forces, their families, the American public, and the international audience. Recently, however, it has become apparent that some information on publicly accessible websites provides too much detail on DOD capabilities, infrastructure, personnel, and operational procedures, past, present, and future. While it may be true that the majority of this information is wholly, and truly, unclassified, when combined with information from other sources and/or sites, they can become sensitive and even classified. They also may increase the vulnerability of DOD systems and potentially be used to threaten or harass DOD personnel and/or their families. All DA commanders who establish publicly accessible websites are responsible for ensuring that the information published on their sites do not compromise national security or place DA personnel at risk. The commander's responsibility extends beyond general public affairs considerations regarding the release of information into the realm of operational security and force protection. Commanders must apply comprehensive risk management procedures to ensure that the considerable mission benefits gained by using the web are carefully balanced against the potential security and privacy risks created by having aggregated DOD information more readily accessible to a worldwide audience than ever before.

E–2. Printed Documents Produced by AIS Equipment

There are no special provisions for documents produced by Automated Information Systems (AIS) which function as word processing systems. Documents produced on an AIS will be marked like any other documents. For other AIS–generated documents, special exceptions may apply where the application of the marking requirements are not feasible. These exceptions are:

a. Classification markings on interior pages of fan–folded printouts. These markings will be applied and can be done so on the AIS equipment, however they may not meet the standard requirement of being conspicuous.

b. Special warning notices, identification of classification sources, and declassification (and downgrading, where applicable) instructions will either be marked on the cover of the document (or on the first page if there is no cover) or will be placed on a separate notice attached to the front of the document.

c. Pages or other portions of AIS printouts removed for separate use or maintenance will be marked in the standard manner as individual documents.

E–3. Classified electronic mail

With advent of electronic mail (E–mail or e–mail), communication between units and personnel has increased exponentially. However, with this increase in e–mail, there is also a decrease in security awareness when it comes to proper classification markings on these messages. Department of the Army personnel take for granted that since they are communicating over a classified LAN they do not have to use proper markings. This is incorrect. Proper page and portion markings will be used on all correspondence just as if it were a typed or hand–written paper. If the entire message, on a classified LAN, is UNCLASSIFIED, it can be marked on its face, top and bottom: "UNCLASSIFIED", and a statement added: "All portions of this message are UNCLASSIFIED." No further markings are required. All other classified messages will be marked according to chapter 4 of this regulation.

E–4. E–mail sensitivity

The availability and use of commercial e–mail programs within the Department of the Army has added another potential for security violations. These programs offer what is called "sensitivity" categories for messages. The most commonly available categories are: (1) NORMAL; (2) PERSONAL; (3) PRIVATE; and (4) CONFIDENTIAL. The use of this last category could open the user to potential security violations since classified information will not be sent over an unclassified system. The term "CONFIDENTIAL" is reserved strictly for classification purposes only. Therefore, this sensitivity category will not be used on any e–mail, sent or received on or by a government owned and/or operated machine and/or system.

Section II
Internet Websites

E–5. General Overview

One of the most popular, and convenient, forms of spreading information about a unit or agency is to post it on the Internet. The cost of "surfing" has diminished to the point where an overwhelming majority of people have Internet access, not only at work, but also at home. It is as common as the family television set. It is estimated that by the next millenium, the majority of unit data exchange will be via Internet websites. It is for this reason that measures need to be instituted now before it is too late. For purposes of this appendix, the term "page" is used to represent every webpage or file related to, and linked from, any files that contain Department of Defense information on a unit or activity's Internet site, regardless if it is on an unclassified or a classified LAN. This includes embedded items, such as graphics, multimedia, etc.

E–6. Unclassified websites

Much as classified and unclassified documents are easily marked and recognized, so must be unclassified webpages. For each unclassified Internet homepage/website, a banner stating that the website contains only unclassified, non–sensitive, and non–Privacy Act information is required as the first page visitors will come to. A banner similar to the one at figure E–1 will be used and no further markings are required.

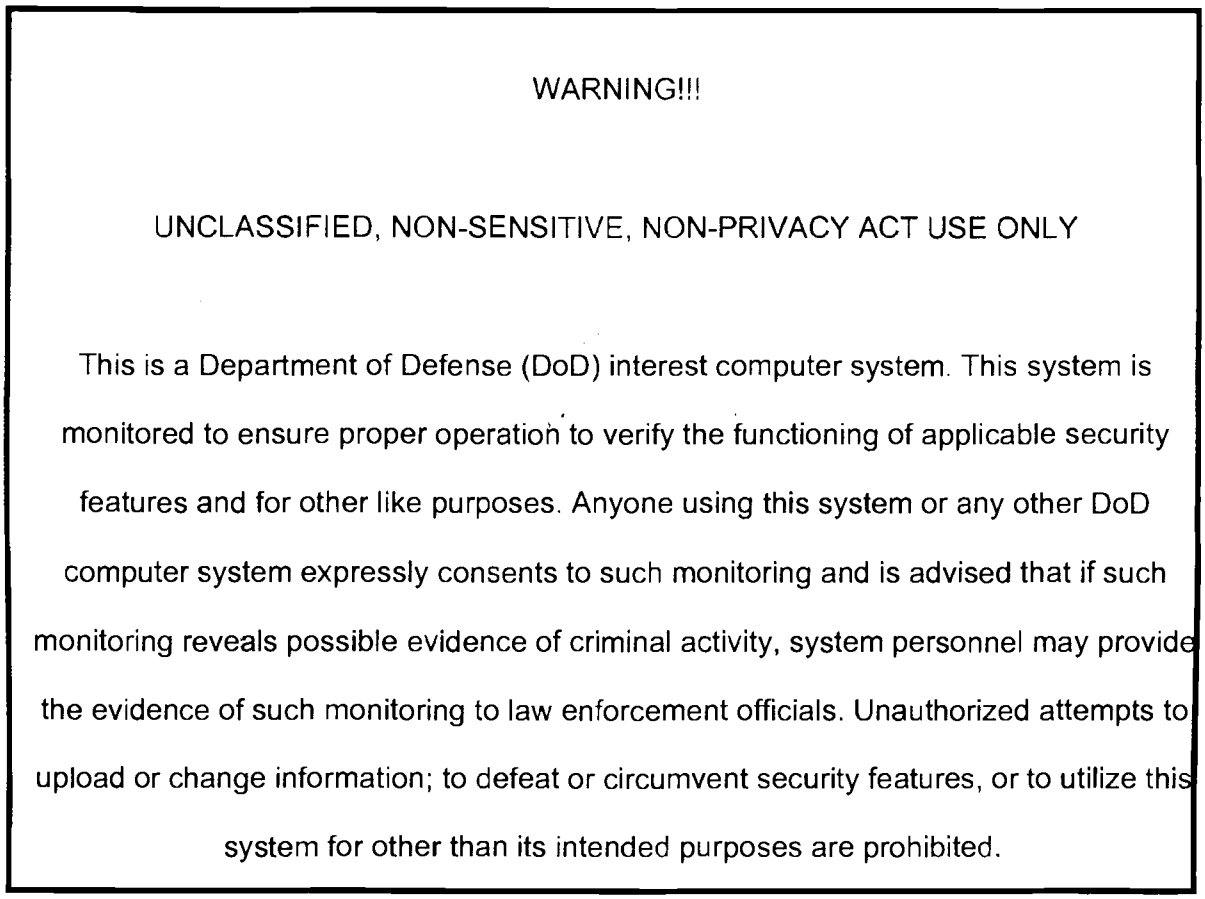


Figure E-1. Unclassified Warning Banner

E–7. Classified websites

Homepages/websites, on a classified network, are the same thing as pages in a classified document, especially after they have been printed out. It is vitally important that proper marking and handling procedures are implemented to reduce the risk of a security violation. For each classified homepage/website, a banner similar to the one at figure E–2 is required on the first page visitors come to.

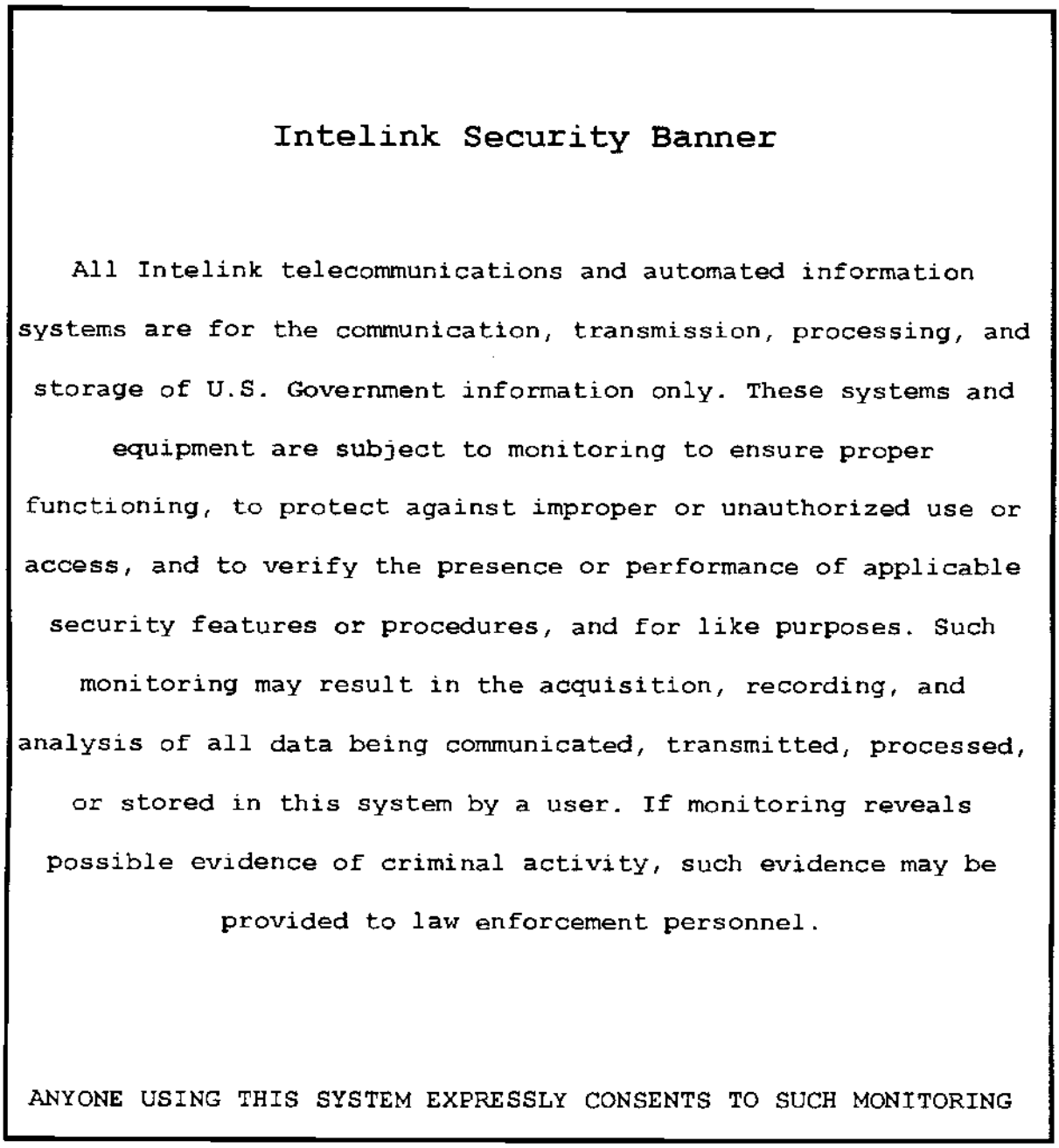


Figure E-2. Intelink Security Banner

E–8. Marking Classified Websites

Homepages/websites, on a classified network, will be handled in much the same manner, when it comes to marking and handling, as you would for a printed classified document.

a. Every page will bear the following markings:

(1) The overall (highest) classification of the information.

(2) The command, office of origin, date, and if not evident by the name of the command, the fact that the page was generated by the Army.

(3) Identification of the specific classified information in the page and its level of classification (page and portion markings).

(4) Identification of the source(s) of the classified information ("Classified By" or "Derived From" line).

(5) Declassification instructions ("Declassify On" line), and downgrading instructions, if any downgrading applies.

(6) Warning notices, if any, and other markings, if any, that apply to the page.

b. Each section, part, paragraph, and similar portion of each classified webpage will be marked to show the highest level of classification of information it contains, or that it is wholly UNCLASSIFIED. "Portion marking" is the term used to meet this requirement. The term "paragraph marking" is generally used interchangeably with "portion marking". Whether referred to as portion or paragraph marking, the term includes the marking of all portions of a webpage, not just paragraphs. When deciding whether a subportion (such as a subparagraph) will be marked separately as a "similar subportion", the deciding factor is whether or not the marking is necessary to eliminate doubt about the classification of its contents. Unless the original classification authority or originator of the source document indicates otherwise, each classified portion of a webpage will be presumed to carry the declassification instructions (date, event, or exemption category) of the overall document.

(1) Each portion of text will be marked with the appropriate abbreviation ("TS" for TOP SECRET, "S" for SECRET, "C" for CONFIDENTIAL, "U" for UNCLASSIFIED, "SBU" for Sensitive But Unclassified), placed in parentheses immediately before the beginning of the portion. If the portion is numbered or lettered, the abbreviation will be placed in parentheses between the letter or number and the start of the text. Some agencies permit portion marking at the end of the portion, rather than at the beginning. The Army does not. When extracts from non–Army source documents are made and incorporated into Army webpages, the portion marking will be placed at the beginning of the portion.

(2) Portions containing Restricted Data and Formerly Restricted Data will have abbreviated markings ("RD" or "FRD") included with the classification marking, for example, "(S–RD) or (S–FRD)". Critical Nuclear Weapons Design Information (CNWDI) will be marked with an "N" in separate parentheses following the portion marking, for example, "(S–RD)(N)".

(3) The abbreviation "FOUO" will be used in place of "U" when a portion is UNCLASSIFIED but contains For Official Use Only (FOUO) information. DODD 5200.1–R, appendix C, contains the definition and policy application of FOUO markings.

(4) Portions of Army webpages containing foreign government or NATO information will include identification of the foreign classification in the marking in parentheses. For example, "(UK–S)" for information classified "SECRET" by the United Kingdom; and "(NATO–C)" for NATO information classified as "CONFIDENTIAL".

(5) The subject and title of classified webpages will be marked to show the classification of the information in the subject or title. The same abbreviations ("TS", "S", "C", "U", or "FOUO") will be used but the abbreviations will be placed in parentheses at the end of the subject or title.

(6) Charts, graphs, photographs, illustrations, figures, tables, drawings, and similar items will be marked with the unabbreviated classification such as "UNCLASSIFIED", based on the level of classified information revealed. The marking will be placed within the chart, graph, etc., or next to it, such as on the frame holding the document. Captions and titles of charts, graphs, etc., will be marked as required for text portions (such as paragraphs) and will be placed at the beginning of the caption or title.

(7) See appendix D, of this regulation, for an explanation of portion marking certain intelligence control markings (for instance, ORCON and PROPIN). Portion marking of those intelligence control markings will follow the same policy as stated in this section of the regulation.

E–9. Publicly Accessible Websites

Figure E–3, of this appendix, contains a memorandum, from the Director of Information Systems for Command Control, Communications, and Computers (DISC4), that provides guidance for the establishment and operation of publicly accessible, non–restricted, U.S. Army World Wide Web websites (Army websites). Publicly accessible, non–restricted Army websites will only provide information that has been properly cleared for release. The organization's leadership is responsible for the release of all information on the organization's website.

Guidance for Management of Publicly Accessible U.S. Army Websites

30 November 1998

SUBJECT: Guidance for Management of Publicly Accessible U.S. Army Websites

1. Purpose

a. This memorandum provides guidance for the establishment and operation of publicly accessible, non-restricted, U.S. Army World Wide Web (WWW) websites (Army websites). Publicly accessible, non-restricted Army websites will only provide information that has been properly cleared for release.

b. The World Wide Web is an efficient and effective means for the U.S. Army to share information. Army websites should focus on providing value-added information services and products to the organization's users, customers, the Army, and the public through the sharing of accurate, timely, and relevant information. To ensure that the Army fully leverages the capabilities of the WWW in a manner that is efficient, focused on saving resources, and moving toward a digital environment, the following guidance is provided.

2. Proponent and Exception Authority

a. The proponent for this memorandum is the Director of Information Systems for Command Control, Communications, and Computers (DISC4).

b. The DISC4 has the authority to approve exceptions to this memorandum that are consistent with controlling law and regulation. The DISC4 may delegate the authority to approve exceptions to this policy, in writing, to a division chief under his supervision within the proponent agency that holds the grade of Colonel or GM/GS-15.

Figure E-3. Guidance for Management of Publicly Accessible U.S. Army Websites

3. References

a. This policy supersedes Director of Information Systems for Command, Control, Communications, and Computers, 301404Z October 1996, Guidance for the Management of Army Websites.

b. 5 USC Chapter 35, "Paperwork Reduction Act", as amended.

c. Public Law 100-235, Computer Security Act of 1986.

d. For guidance on use of government-owned computing equipment and resources (e.g., non-duty related email use and web browsing in the workplace), see DoD 5500.7-R, Joint Ethics Regulation (JER) (30 August 1993) and Change 2 (25 March 1996).

e. For all DoD newspapers, including electronic publications, DoD Instruction 5120.4, DoD Newspapers and Civilian Enterprise Publications (May 29, 1996) applies.

f. For image manipulation standards, DoD Directive 5040.5, Alteration of Official DoD Imagery (August 29, 1995) applies.

g. AR 25-1, The Army Information Resource Management Program (25 March 1997).

h. AR 25-55, Army Freedom of Information Act Program (1 November 1997).

i. For access-controlled websites, AR 380-19, Information System Security (27 August 1998) applies.

j. AR 340-21, Army Privacy Act Program (5 July 1985).

k. AR 360-5, Public Information (31 May 1989).

l. AR 380-5, Department of the Army Information Security Program (25 February 1988).

m. AR 530-1, Operational Security (3 March 1995).

n. HTML 3.2 Reference Specification, World Wide Web Consortium (W3C) Recommendation (11 January 1997).

o. HTML 4.0 Specification, World Wide Web Consortium (W3C) Recommendation (24 April 1998).

Figure E-3. Guidance for Management of Publicly Accessible U.S. Army Websites—Continued

4. Definitions and Explanation of Abbreviations

a. WWW - World Wide Web

b. HTML - Hypertext Markup Language

c. W3C - World Wide Web Consortium

d. CGI - Common Gateway Interface

e. GILS - Government Information Locator Service

f. FOUO - For Official Use Only

g. FOIA - Freedom of Information Act

h. MACOM - Major Command

i. GO/SES - General Officer/Senior Executive

j. DoD - Department of Defense

k. Webpage - an individual HTML-compliant electronic file accessible through a TCP/IP network

l. TCP/IP network - a data communication network that uses Transport Control Protocol/Internet Protocol (TCP/IP); the public internet and the DoD Non-Classified IP Router Network (NIPRNET) are examples of TCP/IP networks

m. Website - a collection of HTML-compliant electronic files designed to provide information, services, or goods to users through a TCP/IP network

n. Homepage - the single, top-level, webpage designed to be the first file accessed by a user visiting a website; also known as an "index" or "default" page

5. Responsibilities

a. The leader of each organization that operates an official U.S. Army website (leadership), regardless of location or echelon (e.g., unit, office, installation, major command), will--

(1) exercise ultimate control over the content of the organization's website,

(2) define the purpose of the website in terms of how it supports the mission of the organization,

(3) define the core functions, products, and information that will be made available through the organization's website,

(4) ensure compliance with all applicable policies, including AR 530-1, Operational Security (3 March 1995), and

Figure E-3. Guidance for Management of Publicly Accessible U.S. Army Websites—Continued

(5) periodically reevaluate each website under their control to ensure performance of the responsibilities in paragraphs 5.a.(1) through 5.a.(4).

b. The organization's leadership may delegate the execution of this responsibility to one or more website managers and other appropriate officials. Where appropriate, the organization's leadership may delegate these responsibilities to a team of subject matter experts, the exact composition of which is left to the discretion of the leadership. This team may be composed of subject matter experts from one or more of the following communities: Public Affairs, Communications/Computers, Intelligence, Legal, and others.

6. Policy

a. Specifications and Standards.

(1) Official U.S. Army websites should be implemented in such a way as to support the widest range of potential users and computing platforms. Use of non-standard or proprietary website elements will not benefit the widest range of potential users.

(2) For hypertext markup language (HTML) documents, official U.S. Army websites must use any of the HTML specifications listed by the World Wide Web Consortium (W3C). As an alternative, official U.S. Army websites may employ any HTML specification that is a W3C Proposed Recommendation, or any non-HTML specification that is a W3C Recommendation. W3C Technical Reports (including Recommendations and Proposed Recommendations) are found online at "http://www.w3.org/TR/".

(3) Official U.S. Army websites may employ non-standard (e.g., browser-specific) HTML tags and browser extensions (plug-in). However, official U.S. Army websites may not require or encourage users to use any particular browser product or "plug-in" technologies. Official U.S. Army websites may not be designed to support any particular browser product.

Figure E-3. Guidance for Management of Publicly Accessible U.S. Army Websites—Continued

b. Requirements for Organizations Operating Websites.

(1) Every Army organization that maintains a website must register it with the U.S. Army Homepage through the online registration form found on the U.S. Army Homepage at "http://www.army.mil/register3.htm".

(2) Every Army organization that maintains a website must notify the U.S. Army Homepage Webmaster, via e-mail at webmaster@hqda.army.mil, when the Universal Resource Locator (URL) or any of the point of contact information required as part of the registration process changes.

(3) Every Army organization that maintains a website must register it with the Government Information Locator Service (GILS), see "http://www.dtic.mil/index/."

(4) Every Army organization that maintains a website must display a Privacy and Security Notice.

(5) U.S. Army organizations operating an official website will provide the following information or hyperlinks to the following information on their homepage:

(a) Organization missions and functions.

(b) Organizational structure, listing or hyperlinking to parent and subordinate command or organization websites. Organizational charts containing individuals' names and other personal information should not be made available to the public unless privacy and security concerns have been addressed; posting such information for members of deployable units and others in sensitive positions could make them potential targets of hostile organizations or individuals.

(c) Electronic mail address, phone number, or mail address of the point of contact responsible for the website content.

(d) A hyperlink to the U.S. Army Homepage using "http://www.army.mil".

Figure E-3. Guidance for Management of Publicly Accessible U.S. Army Websites—Continued

c. Requirements for Website Managers

A website manager is the organizations' leader, or an individual or group that has been delegated the following responsibilities by the organization's leadership. Website Managers (webmasters) will--

(1) Ensure that information published on their website is accurate, timely, represents the official Army position, and is properly cleared for public dissemination;

(2) Ensure appropriate security and access controls are in place, commensurate with the perceived threats, and to ensure that the following types of information is not made available to unauthorized individuals or organizations:

(a) Classified

(c) Information that cannot be disclosed under the Privacy Act

(d) For Official Use Only (FOUO)

(e) Freedom of Information Act (FOIA)-exempt information (including, but not limited to draft policies and regulations, and pre-decisional information)

(f) Copyrighted information for which releases from the copyright owner have not been obtained

(3) Provide the highest practicable level of assurance that information made available to or received from the public does not contain malicious software code (e.g., viruses, trojan horses), or if it does, to sufficiently notify the user before the download of such information begins;

(4) Respond to email, direct queries to the appropriate source of information, or otherwise fulfill or redirect requests for information;

(5) Ensure that the organization's website provides point of contact information for the webmaster.

d. Requirements for Webpages.

All U.S. Army webpages will display the date when that page was last updated, reviewed, or cleared for public release.

Figure E-3. Guidance for Management of Publicly Accessible U.S. Army Websites—Continued

e. Release of Information.

(1) The organization's leadership will institute a review process to ensure that information provided on their website(s) is current, timely, and cleared for public release. The organization's leadership is responsible for the release of all information on the organization's website.

(2) The following types of information will not be made available to the public through the WWW:

(a) Classified

(b) Unclassified but sensitive

(c) Information that cannot be disclosed under the Privacy Act

(d) For Official Use Only (FOUO)

(e) Freedom of Information Act (FOIA)-exempt information (e.g., draft policies and regulations, or pre-decisional information)

(f) Copyrighted information for which releases from the copyright owner have not been obtained

(3) Commanders of Army major commands (MACOM Commander), or equivalent, may authorize a waiver to the restrictions at paragraphs 6c(2) and 6e(2) for draft doctrinal and draft technical information only. The ability to waive this prohibition may not be delegated below the GO/SES-level in the MACOM Headquarters. To authorize a waiver in such cases, a MACOM Commander (or the delegated MACOM Headquarters authority) must:

(a) Sign a memorandum waiving the prohibition against releasing draft doctrinal or draft technical information to the public.

(b) Addresses the intelligence and national security, public affairs, legal, and contractual issues pertinent to the public release of the draft doctrinal or draft technical information to the public.

Figure E-3. Guidance for Management of Publicly Accessible U.S. Army Websites—Continued

f. Commercial Advertising and Sponsorship.

(1) Commercial advertising on official U.S. Army websites is prohibited. Corporate or product logos and trademarks (other than text or hyperlinked text) are considered commercial advertisements, and may not be served from official U.S. Army websites.

(2) No money, services, products, or in-kind payment (e.g., website hosting, site management, site design) will be accepted in exchange for a link to a non-Army web resources placed on an official U.S. Army website.

(3) No product endorsement will be served from an official U.S. Army website. Official U.S. Army websites will not provide preferential treatment to non-U.S. Government entities.

g. External Linked Content.

The ability to hyperlink to resources external to the Army is a fundamental feature of the World Wide Web, and can add value and functionality to Army websites.

(1) Hyperlinks to web resources other than official U.S. Army (non-Army) web resources are permitted if the organization's leadership certifies them to be in support the organization's mission.

(2) Official U.S. Army websites may use only text or hyperlinked text to direct users to non-Army software download sites.

(3) Army websites that provide links to non-Army web resources must display a disclaimer in accordance with DoD policy.

h. Collection of Information.

Army websites that collect standardized information from 10 or more members of the public must comply with:

(1) DoD Memorandum, *Establishing and Maintaining a Publicly Accessible Department of Defense Web Information Service*, 18 July 1997, found at "http://www.defenselink.mil/policy97.html."

(2) The Paperwork Reduction Act of 1995 (as amended).

Figure E-3. Guidance for Management of Publicly Accessible U.S. Army Websites—Continued

i. Personal Use.

(1) Personal use of government resources generally is improper.

(2) Hyperlinks on Army websites to homepages, websites, or other web resources of a personal and non-mission related nature are prohibited.

(3) Army Internet users are subject to DoD 5500.7-R, change 2, Joint Ethics Regulation (JER), 25 Mar 1996.

j. Restricted Access.

(1) In addition to not posting certain information to Army websites as noted above in paragraph 6.e., webmasters shall ensure that Army websites do not provide direct hyperlinks (or other methods to bypass access-controls, such as hyperlinking to webpages below password protection webpages) to the following types of information:

(a) Classified

(b) Unclassified but sensitive

(c) Information that cannot be disclosed under the Privacy Act

(d) For Official Use Only (FOUO)

(e) Freedom of Information Act (FOIA)-exempt information (including, but not limited to draft policies and regulations, and pre-decisional information)

(f) Copyrighted information for which releases from the copyright owner have not been obtained

(2) Publicly accessible Army websites may provide hyperlinks to access-controlled websites only through intervening access-control mechanisms or procedures that are sufficient to address the perceived level of threat and sensitivity of the information.

(3) Army websites must not use inflammatory or threatening language when describing access-controls and procedures, and must avoid the perception that the Army is hiding or withholding information that otherwise would be available to the public.

7. Point of Contact

Point of contact for this policy is the Army Homepage Webmaster. Their e-mail address is "webmaster@hqda.army.mil."

Figure E-3. Guidance for Management of Publicly Accessible U.S. Army Websites—Continued

Appendix F
Management Control

Section I
Management Control Evaluation Checklist

F–1. Purpose
The purpose of this checklist is to assist Command Security Managers and Management Control Administrators (MCAs) in evaluating the key management controls outlined below. It is not intended to cover all controls. It is to be answered in a YES/NO/NA format. A negative response (NO) is to be explained at the end of the question. The locations in bold are provided as reference points within AR 380–5.

F–2. Instructions
Answers must be based on the actual testing of key management controls (e.g., document analysis, direct observation, sampling, simulation, etc.). Answers that indicate deficiencies must be explained and corrective action indicated in supporting documentation. These key management controls must be formally evaluated at least once every five years. Certification that this evaluation has been conducted must be accomplished on DA Form 11–2–R (Management Control Evaluation Certification Statement). All Department of the Army units, with access to classified information, will develop and implement an inspection program for annual inspections. This checklist can serve as the base for the annual inspection and can include other questions as determined by the agency or command performing the inspection. Inspection programs are used to evaluate the effectiveness of these key management controls as well as other requirements of this regulation as they apply to the command being inspected.

F–3. Test questions

Chapter 1 General Provisions and Program Management

Paragraph 1–5

Responsibilities of Deputy Chief of Staff for Intelligence (DCSINT), Headquarters Department of the Army.

Does the DCSINT, DAMI–CH—

a. Promulgate (or cause to promulgate) policy, procedures, and programs necessary for the implementation of EO 12958 and resulting national and DOD directives?

b. Monitor, evaluate, and report on the administration of the Army Information Security Program?

c. Ensure the Major Army Commands (MACOM), and other agencies, establish and maintain an ongoing self–inspection program, to include periodic reviews and assessments of their classified products?

d. Respond to information security matters pertaining to classified information that originated in an Army activity that no longer exists and for which there is no successor in function?

e. Delegate SECRET and CONFIDENTIAL Original Classification Authority (OCA) to other Army officials?

f. Commit needed resources for effective policy development and oversight of the programs established by this regulation?

Paragraph 1–6

Responsibilities of the Commander.

Does the Commander—

a. Establish written local information security policies and procedures?

b. Initiate and supervise measures or instructions necessary to ensure continual control of classified information and materials?

c. Assure that persons requiring access to classified information are properly cleared?

d. Continually assess the individual trustworthiness of personnel who possess a security clearance?

e. Designate a Command Security Manager by written appointment? Is the Security Manager of sufficient rank or grade to effectively discharge assigned duties and responsibilities?

f. Make sure the Command Security Manager is afforded security training consistent to the duties assigned?

g. Make sure adequate funding and personnel are available to allow security management personnel to manage and administer applicable information security program requirements?

h. Review and inspect annually the effectiveness of the Information Security Program in subordinate commands?

i. Make sure prompt and appropriate responses are given, or forward for higher echelon decision, any problems, suggestions, requests, appeals, challenges, or complaints arising out of the implementation of this regulation?

Paragraph 1-7

Responsibilities of the Command Security Manager.

Does the Command Security Manager—

a. Advise and represent the Commander on matters related to the classification, downgrading, declassification, and safeguarding of national security information?

b. Establish and implement an effective security education program, as required by chapter 9 of this regulation?

c. Establish procedures for assuring that all persons handling classified material are properly cleared? Is the clearance status of each individual 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 properly prepared and maintained?

f. Conduct a periodic review of classifications assigned within the activity to ensure that classification decisions are proper?

g. Review all classified documents, in coordination with the agency or command records management officer, to ensure consistency with operational and statutory requirements?

h. Continually reduce, by declassification, destruction, or retirement, unneeded classified material?

i. Submit, in a timely manner, Standard Form 311 (Information Security Program Data Report) to DAMI–CH, annually, as required?

j. Supervise or conduct security inspections and spot checks and notify the Commander regarding compliance with this regulation and other applicable security directives?

k. Assist and advise the Commander on matters pertaining to the enforcement of regulations governing the dissemination, reproduction, transmission, safeguarding, and destruction of classified material?

l. Make recommendations on requests for visits by foreign nationals, and provide security and disclosure guidance if visit is approved?

m. Make sure of the completion of inquiries and reporting of security violations occur including compromises or other threats to the safeguarding of classified information?

n. Recommend to the decision official whether or not administrative sanction is warranted, and/or indicate corrective action that should be taken concerning security violations?

o. Make sure proposed public releases on classified programs are reviewed to preclude the release of classified information, or other sensitive unclassified information covered under the Freedom of Information Act?

p. Establish and maintain visit control procedures for visitors are authorized access to classified information?

q. Issue contingency plans for the emergency destruction of classified information and, where necessary, for the safeguarding of classified information used in or near hostile or potentially hostile areas?

r. Act as the single point of contact to coordinate and resolve classification or declassification problems?

s. Report data as required by this regulation?

Paragraph 1–8

Responsibilities of the Supervisor.

Does the Supervisor—

a. Make sure subordinate personnel who require access to classified information are properly cleared and are given access only to that information for which they have a need–to–know?

b. Make sure subordinate personnel are trained in, understand, and follow the requirements of this regulation and local command policy and procedures concerning the information security program?

c. Continually assess the eligibility for access to classified information of subordinate personnel and report to the Command Security Manager any information that may have a bearing on that eligibility?

d. Supervise personnel in the execution of procedures necessary to allow the continuous safeguarding and control of classified information?

e. Include the management of classified information as a critical element/item/objective in personnel performance evaluations, where deemed appropriate, in accordance with Army personnel policy and paragraph 1–5c of this regulation? (A supervisor should include the protection of classified information as a performance evaluation factor or objective for other personnel as the supervisor deems appropriate.)

f. Lead by example? Does he/she follow Command and Army policy and procedures to properly protect classified information and to appropriately classify and declassify information as stated in this regulation?

Chapter 2 Classification

Paragraph 2–1

Are personnel designated, in writing, by either the Secretary of the Army (SECARMY) or HQDA, as Original Classification Authorities (OCA)?

Paragraph 2–3:

Are requests for original classification authority submitted through command channels to DAMI–CH?

Paragraph 2–4:

Do officials who have been delegated as an Original Classification Authority receive training, as required by chapter 9 of this regulation, before exercising this authority?

Paragraph 2–5:

Do derivative classifiers make sure that the classification is properly applied based on the original source material marking and local security classification guides?

Paragraph 2–6:

Do personnel accomplishing derivative classification:

a. Observe and respect the classification determinations made by Original Classification Authorities?

b. Apply markings or other means of identification to the derivatively classified material, as required by this regulation, at the level and for the duration specified by the classification guide or source document?

c. Use only authorized sources such as classification guides, other forms of official classification guidance, and markings on source material from which the information is extracted, to determine the material's classification?

d. Use caution when paraphrasing or restating information extracted from a classified source to determine whether the classification could have been changed in the process?

e. Take appropriate and reasonable steps to resolve doubt or conflicts in classification?

f. Make a list of sources used when material is derivatively classified based on "Multiple Sources" (more than one security classification guide, classified source document, or any combination)? Is a copy of this list included in or attached to the file and/or record copy of the material?

g. Contact the classifier of the source document for resolution in cases in which the derivative classifier believes the classification applied to the information is not accurate?

Paragraph 2–7:

In making a decision to originally classify an item of information, do Original Classification Authorities:

a. Determine that the information has not already been classified?

b. Determine that the information is eligible for classification pursuant to paragraph 2–8 of this regulation?

c. Determine that classification of the information is a realistic course of action and that it can only be protected from unauthorized disclosure when classified?

d. Decide that unauthorized disclosure of the information could reasonably be expected to cause damage to the National Security that this disclosure is identifiable and can be described?

e. Select the appropriate level or category of classification to be applied to the information, based on a judgement as to the degree of damage unauthorized disclosure could cause?

f. Determine and include the appropriate declassification, and when applicable, downgrading instruction to be applied to the information?

g. Make sure that the classification decision is properly communicated so that the information will receive appropriate protection?

Paragraph 2–8:

U.S. classification can only be applied to information that is owned by, produced by or for, or is under the control of the United States Government. Does the Original Classification Authority determine that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security, and that the information falls within one or more of the categories specified in section 1.5 of Executive Order 12958?

Paragraph 2–9:

Does the Original Classification Authority determine that, if classification is applied or reapplied, there is a reasonable possibility that the information will be provided protection from unauthorized disclosure?

Paragraph 2–10:

Once a decision is made to classify, information will be classified at one of three levels. For each level, is the Original Classification Authority able to identify or describe the damage that unauthorized disclosure reasonably could be expected to cause to the national security?

Paragraph 2–11:

a. Is information declassified as soon as it no longer meets the standards for classification?

b. At the time of original classification, does the Original Classification Authority attempt to establish a specific date or event for declassification based upon the duration of the national security sensitivity of the information?

c. If unable to determine a date or event that is ten years or less, does the Original Classification Authority assign an exemption designation to the information if the information qualifies for exemption from automatic declassification in ten years?

Paragraph 2–16:

Is a security classification guide issued for each system, plan, program, or project in which classified information is involved?

Paragraph 2–17:

Do security classification guides, at a minimum, include the information outlined in paragraph 2–17a through f?

Paragraph 2–18:

a. Are security classification guides personally approved in writing by the Original Classification Authority who is authorized to classify information at the highest level designated by the guide, and who has program support or supervisory responsibility for the information or for the organization's Information Security Program?

b. Are security classification guides distributed to those commands, contractors, or other activities expected to be derivatively classifying information covered by the guide?

Paragraph 2–19:

a. Are security classification guides revised whenever necessary to promote effective derivative classification?

b. Are security classification guides reviewed by the originator for currency and accuracy at least once every five years, or if concerning a defense acquisition program, prior to each acquisition program milestone, whichever occurs first?

Paragraph 2–22a:

Does the Commander establish procedures through which authorized holders of classified information, within their Commands, can challenge a classification decision, and make sure that Command personnel are made aware of the established procedures?

Paragraph 2–22b:

Does each Original Classification Authority establish:

a. A system for processing, tracking, and recording formal challenges to classification?

b. Provide an acknowledgment or written response to the challenge within 60 calendar days following the receipt of the challenge?

c. Advise the challenger of the right to appeal the decision, if the challenge is denied and the Original Classification Authority determines that the information is properly classified?

Paragraph 2–22c:

Is information, that is the subject of a classification challenge, continue to be classified and appropriately safeguarded until a decision is made to declassify it?

Chapter 3 Declassification, Regrading, and Destruction

Paragraph 3–1:

a. Is information declassified when it no longer meets the standards and criteria for classification?

b. Do MACOMs establish programs to make sure that records are reviewed and either declassified or exempted prior to the date for automatic declassification?

Paragraph 3–3:

Is declassification of RD and FRD information only with the express specific approval of the Original Classification Authority for the information?

Paragraph 3–4:

Is information classified by other U.S. Executive Branch agencies or by foreign governments or international organizations (including foreign contractors) referred to the originating agency (or its successors in function) prior to declassification? (In the case of a foreign government, refer to its legitimate successor for a declassification decision.)

Paragraph 3–5:

a. Does the automatic declassification requirement exist for all records of permanent historical value as they become 25 years old?

b. Are Army files, determined to be of permanent historical value under Title 44, USC? (Unless that information has been reviewed and exempted, automatic declassification will occur whether or not the records have been reviewed.)

Paragraph 3–6:

In accordance with EO 12958, the Army has identified and proposed specific designated file series, with description and identification of information in those file series, to be exempt from the 25–year automatic declassification.

a. Are files containing information described in the list of exempt file series, located and marked to reflect the exemption from automatic declassification, the applicable exemption category, and the date or event for future declassification?

b. Is classified information, not contained in the exempted file series, exempted from declassification if they fall within one of the nine exemption categories that are listed in paragraph 3–6e?

c. Are requests for exemption for other than listed exemptions reported to DAMI–CH?

Paragraph 3–7:

Are documents that are exempted from automatic declassification after 25 years, marked with the designation “25X”, followed by the number of the exemption category (see categories listed in paragraph 3–6e), or by a brief reference to the pertinent exemption?

Paragraph 3–10:

Is information downgraded to a lower level of classification when the information no longer requires protection at the originally assigned level and can be properly protected at a lower level?

Paragraph 3–12:

Is classified information upgraded to a higher level of classification only by officials who have been delegated the appropriate level of Original Classification Authority? Do they also notify holders of the change in classification?

Paragraph 3–13:

Is classified material destroyed completely to preclude recognition or reconstruction of the classified information contained in or on the material? Is destruction accomplished in accordance with the guidelines outlined in this regulation?

Chapter 4 Marking

Paragraph 4–1:

Is classified material identified clearly by marking, designation, electronic labeling, or if physical marking of the medium is not possible, by some other means of notification?

Paragraph 4–3:

Does classified material bear the following markings:

a. The overall (highest) classification of the information?

b. The Command, office of origin, date, and if not evident by the name of the Command, the fact that the document was generated by the Department of the Army?

c. Identification of the specific classified information in the document and its level of classification (page and portion markings)?

d. Identification and date of the source(s) of classification ("Classified by" or "Derived from" line), and, for originally classified information, the concise reason(s) for classification?

e. Declassification instructions ("Declassify on" line), and downgrading instructions, if any downgrading applies?

f. Warning notices and other markings, if any, that apply to the document?

Paragraph 4–12:

a. Are required warning notices used, where applicable?

b. Is the required warning notice on all government owned or operated automated information systems?

Paragraph 4–15:

Are all unclassified Army records, including For Official Use Only (FOUO), regardless of media, and all classified Army records through SECRET, marked according to the MARKS system, to include disposition instructions?

Paragraph 4–16:

If a classified document has components likely to be removed and used or maintained separately, is each component marked as a separate document?

Paragraph 4–19:

Are translations of U.S. classified information into a foreign language marked with the appropriate U.S. classification markings and the foreign language equivalent?

Paragraph 4–21:

Are documents which contain no classified information, but are marked with classification markings for training purposes, marked to clearly show that they are actually UNCLASSIFIED?

Paragraph 4–22:

Are files, folders, and similar groups of documents containing classified information clearly marked as to the highest classification of information contained therein?

Paragraph 4–23:

Are documents produced on an AIS marked like other documents except where designated by paragraph 4–23?

Paragraph 4–24:

When classified information is contained in equipment, hardware, AIS media, or on film, tape, or other audiovisual media, or in another form not commonly thought of as a document, is the marking provisions of this regulation met in a way that is compatible with the type of material?

Paragraph 4–33:

Do System Managers make sure that AIS, including word processing systems, provide for classification designation of data stored in internal memory or maintained on fixed storage media?

Paragraph 4–45:

Are Joint Chiefs of Staff (JCS) papers, including extractions from such papers, safeguarded in accordance with this regulation?

Paragraph 4–56:

Are classified documents originated by NATO, if not already marked with the appropriate classification in English, so marked?

Chapter 5 Controlled Unclassified Information

Paragraph 5–2:

"For Official Use Only (FOUO)" is a designation that is applied to unclassified information, which is exempt from mandatory release to the public under the Freedom of Information Act (FOIA). The FOIA specifies nine categories of information which can be withheld from release if requested by a member of the public.

a. Does information to be exempt from mandatory release, fit into one of the qualifying categories and is there a legitimate government purpose served by withholding it?

b. Is information which has been determined to qualify for FOUO status indicated, by markings, when included in documents and similar material?

Paragraph 5–5:

a. During working hours, are reasonable steps taken to minimize risk of access by unauthorized personnel?

b. After working hours, is FOUO information stored in approved methods outlined in paragraph 5–5?

c. Are FOUO documents and material transmitted by approved means?

Paragraph 5–10:

Is SBU information protected as that required for FOUO information?

Paragraph 5–12:

Are UNCLASSIFIED documents containing DEA sensitive information marked as required by paragraph 5–12?

Paragraph 5–14:

a. Are UNCLASSIFIED documents containing DEA sensitive information transmitted outside CONUS by a means approved for transmission of SECRET material?

b. Is DEA sensitive material destroyed by a means approved for the destruction of CONFIDENTIAL material?

Paragraph 5–16:

Are UNCLASSIFIED documents and material containing DOD UCNI marked as required by paragraph 5–16?

Paragraph 5–22:

Is Information on DOD AIS systems, which is determined to be "sensitive," within the meaning of the Computer Security Act of 1987, provided protection as required by paragraph 5–22?

Paragraph 5–24:

Are distribution statements placed on technical documents no matter if they are classified or unclassified?

Chapter 6 Access, Control, Safeguarding & Visits

Paragraph 6–2:

a. Prior to granting access to classified information, do all unit personnel receive a briefing outlining their responsibility to protect classified information and have they signed the Classified Information Nondisclosure Agreement (NDA), Standard Form SF 312 or the SF 189?

b. Are SF 312 and SF 189 NDAs retained for 50 years from the date of signature?

Paragraph 6–3:

Prior to execution of the NDA, does the command have proof of clearance?

Paragraph 6–4:

a. If a person refuses to sign the form, is the individual advised of the applicable portions of the NDA?

b. If after the five days the individual still refuses to sign the NDA, is classified access, if it had been previously granted, formally suspended and the individual not permitted any access to classified information?

c. Is the Department of the Army's Central Clearance Facility notified concerning clearance revocation or denial action, and the matter reported as required by AR 380–67?

Paragraph 6–5:

a. Are all DA personnel who are retiring, resigning, being discharged, or will no longer have access to classified information, out–processed through the Command's Security Manager's office or other designated command office, and are they formally debriefed?

b. Do all personnel sign a debriefing statement during out–processing? (The debriefing statement will be either DA Form 2962 or the NDA Security Debriefing Acknowledgement section of the SF 312.)

c. For all DA military personnel retiring, resigning, or separating from military service, is the termination portion of the NDA executed and maintained on file by the Command Security Manager, or other designated command official, for two years?

d. Does the original NDA, for civilian employees, who retire or resign from government service, remain in the employee's OPF and will be retired as part of the OPF?

Paragraph 6–7:

Is access to RD (less CNWDI) and FRD by DA personnel at Army facilities, under the same conditions as for all other classified information, based on the appropriate security clearance and need–to–know for the information?

Paragraph 6–8:

Is access to classified information or material by Congress, its committees, subcommittees, members, and staff

representatives, in accordance with DOD Directive 5400.4?

Paragraph 6–9:

Do Commands maintain a system of control measures that ensures that access to classified information is limited only to authorized persons?

Paragraph 6–10:

a. Is classified material removed from storage kept under constant surveillance and control by authorized personnel?
b. Are classified document cover sheets, Standard Forms 703, 704, and 705 placed on classified documents or files not in security storage?

Paragraph 6–11:

Do Commands that access, process, or store classified information establish a system of security checks at the close of each working day to ensure that all classified material is properly secured? Is Standard Form 701 used to record these checks?

Paragraph 6–12:

Have Commands developed plans for the protection, removal, and destruction of classified material in case of fire, flood, earthquake, other natural disasters, civil disturbance, terrorist activities, or enemy action, to minimize the risk of its compromise?

Paragraph 6–13:

Is classified information only discussed, in telephone conversations, over secure communication equipment, such as a STU–III, and circuits approved for transmission of information at the level of classification being discussed?

Paragraph 6–15:

Are storage containers and information processing equipment, which had been used to store or process classified information, inspected by cleared personnel before removal from protected areas or before unauthorized persons are allowed unescorted access to them?

Paragraph 6–16:

Have Commands established procedures to control access to classified information by visitors?

Paragraph 6–18:

When a DA command wishes to be authorized to serve as the security sponsor for an association–related classified meeting, have they made the request, through command channels, to DAMI–CH, and is it received at least 120 days in advance of the meeting?

Paragraph 6–19:

Does the Command have security procedures that prescribe the appropriate safeguards to prevent unauthorized access to non–COMSEC–approved equipment, that are used to process classified information, and replace and destroy equipment parts, pursuant to the level of the classified material contained therein, when the information cannot be removed from them?

Paragraph 6–20:

a. Has the Command developed procedures to protect incoming mail, bulk shipments, and items delivered by messenger, until a determination is made whether classified information is contained in the mail?
b. Have screening points been established to limit access to classified information?

Paragraph 6–21:

a. Has the Command established procedures, tailored to the individual situation, in accordance with the principles of risk management, for the control and accountability of the TOP SECRET material they hold?

b. Have TOP SECRET Control Officers (TSCO) been designated within offices which handle or maintain TOP SECRET material?

c. Are TOP SECRET materials accounted for by a continuous chain of receipts, and are the receipts maintained for 5 years?

d. Is TOP SECRET material inventoried at least once annually? Does the inventory reconcile the TOP SECRET accountability register and records with 100 percent of the TOP SECRET material held? Is the inventory conducted by the TSCO, or alternate, and one properly cleared disinterested individual?

e. Before leaving the command, does the TSCO or alternate conduct a joint inventory with the new TSCO or alternate of all TOP SECRET material for which they have custodial responsibility?

Paragraph 6–22:

Has the Command established procedures to control all SECRET and CONFIDENTIAL information and material originated, received, distributed, or routed to subelements within the command, and all information disposed of by the command by transfer of custody or destruction?

Paragraph 6–24:

Are Working papers containing classified information handled IAW paragraph 6–24?

Paragraph 6–25:

a. Has the Command established and enforced procedures for the reproduction of classified material which limit reproduction to that which is mission essential and do they make sure that appropriate countermeasures are taken to negate or minimize any risk?

b. Are all copies of classified documents reproduced for any purpose, including those incorporated in working papers, subject to the same safeguards and controls prescribed for the document from which the reproduction is made?

c. Is stated prohibition against reproduction of information at any classification level prominently displayed?

d. Is specific equipment designated for the reproduction of classified information and prominently marked as such?

Paragraph 6–26:

Have Command established procedures which ensure that appropriate approval is granted before classified material is reproduced?

Paragraph 6–27:

a. Are classified documents and other material retained only if they are required for effective and efficient operation of the Command or if their retention is required by law or regulation?

b. Are documents which are no longer required for operational purposes disposed of in accordance with the provisions of the Federal Records Act (44 USC Chapters 21 and 33) as implemented by AR 25–400–2?

c. Do Commanders ensure that the management of the retention of classified material is included in oversight and evaluation of program effectiveness?

Paragraph 6–28:

Are classified documents and materials destroyed by burning or, when meeting the standards contained in Chapter 3, of this regulation, by melting, chemical decomposition, pulping, pulverizing, cross–cut shredding, or mutilation, sufficient to preclude recognition, or reconstruction of the classified information?

Paragraph 6–29:

a. Are records of destruction for TOP SECRET documents and material created at the time of destruction?

b. Are records of destruction for NATO and foreign government documents at the SECRET level created at the time of destruction?

c. Are records of destruction maintained for 5 years from the date of destruction?

Paragraph 6–35:

Do the heads of DA MACOMs, units, activities, and agencies establish and maintain a self–inspection program based on program needs and the degree of involvement with classified information?

Chapter 7 Storage and Physical Security Standards

Paragraph 7–4:

a. Is classified information, that is not under the personal control and observation of an authorized person, guarded or stored in a locked security container, vault, room, or area, pursuant to the level of classification and this regulation?

b. Do Commands establish administrative procedures for the control and accountability of keys and locks whenever key–operated, high–security padlocks are utilized?

Paragraph 7–8:

a. Is the requirement that there will be no external mark revealing the level of classified information, authorized to be stored in a given container or vault, followed?

b. Is the requirement that there will be no external mark revealing priorities for emergency evacuation and destruction marked or posted on the exterior of storage containers, vaults, or secure rooms, followed?

c. For identification and/or inventory purposes only, does each vault or container bear, externally, an assigned number or symbol?

d. Are Combinations changed:

(1) When placed in use?

(2) Whenever an individual knowing the combination no longer requires access?

(3) When the combination has been subject to possible compromise?

(4) At least once annually?

(5) When taken out of service, are built–in combination locks reset to the standard combination 50–25–50, and combination padlocks reset to the standard combination 10–20–30?

(6) Annually, per U.S. Central Registry, when NATO information is stored in the security container, vault, or secure room?

e. Is the combination of a container, vault or secure room used for the storage of classified information treated as information having a classification equal to the highest category of the classified information stored inside?

f. Is a record maintained for each vault or secure room door, or container used for storage of classified information, using Standard Form 700, "Security Container Information," or the equivalent?

g. Is access to the combination of a vault or container used for the storage of classified information granted only to those individuals who are authorized access to the classified information that is to be stored inside?

h. Are entrances to secure rooms or areas either under visual control at all times during duty hours, to preclude entry by unauthorized personnel, or is the entry equipped with electric, mechanical, or electro–mechanical access control devices to limit access during duty hours?

Paragraph 7–9:

Have there been unapproved modifications or repairs to security containers and vault doors? (Considered a violation of the container's or door's integrity and the GSA label will be removed.) If so, has the GSA label been removed?

Paragraph 7–10:

Have MACOMs established procedures concerning repair and maintenance of classified material security containers, vaults, and secure rooms, to include a schedule for periodic maintenance?

Paragraph 7–11:

Is security equipment inspected before turn–in or transfer to ensure that classified material is not left in the container?

Paragraph 7–21:

Do new purchases of combination locks, for GSA–approved security containers, vault doors and secure rooms, conform to Federal Specification FF–L–2740A?

Chapter 8 Transmission & Transportation

Paragraph 8–1:

Have Commands established local procedures to meet the minimum requirements to minimize risk of compromise while permitting use of the most effective transmission or transportation means?

Paragraph 8–2:

Is TOP SECRET information transmitted only as outlined in paragraph 8–2?

Paragraph 8–3:

Is SECRET information transmitted only as outlined in paragraph 8–3?

Paragraph 8–4:

Is CONFIDENTIAL information transmitted only as outlined in paragraph 8–4?

Paragraph 8–5:

Is NATO Restricted Information transmitted only as outlined in paragraph 8–5?

Paragraph 8–6:

Is classified information or material approved for release to a foreign government in accordance with AR 380–10? Will it be transferred only between authorized representatives of each government in compliance with the provisions of Chapter 8, of this regulation?

Paragraph 8–8:

Where applicable, have Commands established procedures for shipment of bulk classified material as freight, to include provisions for shipment in closed vehicles when required, appropriate notice to the consignee concerning the shipment, procedures at transshipment activities, and action to be taken in case of non–delivery or unexpected delay in delivery?

Paragraph 8–9:

When classified information is transmitted, is it enclosed in two opaque, sealed envelopes, wrappings, or containers, durable enough to properly protect the material from accidental exposure and to ease in detecting tampering, except where exempted by paragraph 8–9?

Paragraph 8–10:

a. Is the outer envelope or container for classified material addressed to an official government activity or to a DOD contractor with a facility clearance and appropriate storage capability?

b. Does the inner envelope or container show the address of the receiving activity, the address of the sender, the highest classification of the contents, including, where appropriate, any special markings, and any other special instructions?

c. Is the requirement that the outer envelope or single container not bear a classification marking or any other unusual marks that might invite special attention to the fact that the contents are classified strictly followed?

Paragraph 8–12:

Is handcarrying of classified material limited to situations of absolute necessity and carried out to make sure it does not pose an unacceptable risk to the information, IAW the provisions of paragraph 8–12, of this regulation?

Paragraph 8–13:

a. Do responsible officials provide a written statement to all individuals escorting or carrying classified material authorizing such transmission?

b. Do travelers who are authorized to carry classified material on international flights, or by surface conveyance if crossing international borders, have courier orders?

Paragraph 8–14:

a. When classified material is handcarried for delivery to a foreign government representative, or when classified information is discussed with or otherwise disclosed to foreign national personnel, are the requirements of AR 380–10 strictly followed?

b. The DOD requires that a request for travel outside the United States contain a written statement by the traveler that classified information will or will not, as applicable, be disclosed during the trip. If the foreign disclosure of classified information is involved, is there an additional written statement that disclosure authorization has been obtained in accordance with DOD Directive 5230.11?

Paragraph 8–15:

a. Is the individual designated as courier in possession of a DOD or contractor–issued identification card that includes 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.)

b. Does the courier have the original of the authorization letter since a reproduced copy is not acceptable? (The traveler will have sufficient authenticated copies to provide a copy to each airline involved.)

Chapter 9 Security Education

Paragraph 9–1:

Has the Commander established a Security Education Program?

Paragraph 9–3:

Have all personnel who could be expected to play a role in the Information Security Program been given an initial orientation?

Paragraph 9–4:

a. As a minimum, does the Information Security Program include the following points:

(1) The nature of U.S. and foreign government classified information, its importance to the national security, and the degree of damage associated with each level of classification?

(2) How to recognize U.S. and foreign government classified information that personnel may encounter, including markings, etc.?

(3) The individual's responsibility for protection of classified information, and the consequences of failing to do so?

(4) Procedures and criteria for authorizing access to classified information?

(5) Procedures for safeguarding and control of classified information in the individual's work environment?

(6) Proper reaction to discovery of information believed to be classified in the public media?

(7) The security management and support structure within the command, to include sources of help with security problems and questions and proper procedures for challenging classifications believed to be improper?

(8) Penalties associated with careless handling or compromise of classified information?

b. Before being granted access to classified information, have all employees signed a Standard Form 312?

Paragraph 9–6:

Are personnel who are not cleared for access to classified information included in the security education program if they will be working in situations where inadvertent access to classified information might occur or they will have access to unclassified information which might be of value to intelligence collectors?

Paragraph 9–7:

As a minimum, are DA employees who have access to, create, process, or handle classified information provided refresher training in their responsibilities at least once a year?

Paragraph 9–9:

Are DA personnel, who are in positions which require performance of specified roles in the Information Security Program, provided security education sufficient to permit quality performance of those duties? Is the training provided before, concurrent with, or not later than six months following assumption of those positions?

Paragraph 9–10:

Are officials who have been granted original classification authority educated in their responsibilities before they exercise the delegated authority?

Paragraph 9–11:

Are all DA personnel, whose responsibilities include derivative classification, trained in requirements and procedures appropriate to the information and material they will be classifying, to include the proper use of classification guides and source documents?

Paragraph 9–12:

Are Command Security Managers, security staff members, and others with significant responsibility for management of the Information Security Program, trained and educated to fulfill their roles?

Paragraph 9–14:

Does Command include in their security education programs, either in the general program or as part of special briefings to select personnel affected, provisions regarding special education and training for personnel who:

a. Use automated information systems to store, process, or transmit classified information?

b. Will be traveling to foreign countries where special concerns about possible exploitation exist or will be attending professional meetings or conferences where foreign attendance is likely?

c. Will be escorting, handcarrying, or serving as a courier for classified material?

d. Are authorized access to classified information requiring special control or safeguarding measures?

e. Are involved with international programs?

f. Regardless of clearance and/or access level held, do all DA personnel receive SAEDA training, at a minimum of every two years, pursuant to Interim Change IO1, AR 381–12?

Paragraph 9–16:

a. Do DA Commanders ensure that security education programs are appropriately evaluated during self–inspections and during oversight activities of subordinate commands or organizational units?

b. Do Commands maintain a record of the programs offered and of the personnel that participated? Are these records maintained for two years and available for review during oversight inspections and assistance visits?

Chapter 10 Unauthorized Disclosure & Other Security Incidents

Paragraph 10–2:

Are personnel aware of their responsibilities in the event of an actual or possible compromise or loss of classified information or material?

Paragraph 10–3:

a. When an incident of possible loss or compromise of classified information is reported, does the Command immediately initiate a preliminary inquiry into the incident?

b. Does the person appointed to conduct the preliminary inquiry have the appropriate security clearance, the ability and available resources to conduct an effective inquiry, and is not likely to have been involved, directly or indirectly, in the incident?

c. In cases of apparent loss of classified material, has the person conducting the preliminary inquiry ensured that a thorough search for the material has been conducted, and has documented the steps taken to locate the material?

d. Does the preliminary inquiry focus on answering all the basic interrogatives (who, what, where, why, how, when)?

e. As a result of the preliminary inquiry, has one of the following alternatives been chosen?

(1) Compromise of classified information did not occur.

(2) Compromise of classified information may have occurred.

(3) Compromise of classified information did occur, but there is no reasonable possibility of damage to the national security.

(4) Compromise of classified information did occur and damage to the national security may result.

f. If at any time, during the preliminary inquiry, it appears that deliberate compromise of classified information may have occurred, has the situation been immediately reported to the chain of command and supporting counterintelligence unit?

g. Have apparent violations of other criminal law been reported to the supporting criminal investigative activity?

Paragraph 10–5:

When notified of possible or actual compromise, has the holder of that information or material ensured that the original classification authority, responsible for each item of information, is notified of the incident?

Paragraph 10–6:

In cases where a person has had unauthorized access to classified information, has the person been debriefed to enhance the probability that he/she will properly protect it?

Paragraph 10–7:

a. Have Department of the Army Commands, and especially MACOMs, established necessary reporting and oversight mechanisms, to make sure that inquiries are conducted when required, that they are done in a timely and effective manner, and that appropriate management action is taken to correct identified problem areas?

b. Have Commands, and especially MACOMs, established a system of controls and procedures to make sure that reports of security inquiries and damage assessments are conducted, when required, and that their results are available as needed?

Paragraph 10–9:

When an individual who has had access to classified information is absent without authorization, commits or attempts to commit suicide, or is temporarily or permanently incapacitated, has the command inquired into the situation to see if there are indications of activities, behavior, or associations, that could indicate classified information might be at risk?

F–4. Comments

This appendix is designed to assist you in evaluating your management controls. Please submit any comments and/or suggestions to the following address: DEPARTMENT OF THE ARMY DAMI–CHS, 2511 Jefferson Davis Highway, Suite #9300, Arlington, VA 22202–3910

Section II
Recordkeeping Requirements

F–5. Updated requirements

The matrix below (table F–1) shows file titles and dispositions for records created and maintained under the purview of this regulation. The matrix will assist users to determine how long to keep the records in the current file areas (CFA) and when to transfer them to the Record Holding Area (RHA) or destroy them. The chart at table F–2 gives an expanded description of which files fall under what MARKS number.

Table F–1
File Titles and Dispositions for Records

MARKS Number	File Title	NARA Authority	Privacy Act Systems Notice	Organizational Level						
				A	B	C	D	E	F	G
380	General security correspondence files (no longer needed for current operations)	NN–167 NN–165–192	N/A	KE6	KE6	KE6	KE6	KE6	KE6	KE6
380–5a	Security briefings and debriefings (transfer or separation of person)	NC1–AU–78–116	A0380–67–DAMI	KE6	KE6	KE6	KE6	KE6	KE6	KE6
380–5b	Security inspections and surveys (next comparable inspection or survey)	NN–173–72		KE6	KE6	KE6	KE6	KE6	KE6	KE6
380–5d	Classified material access files (transfer, reassignment, or separation of the person, or when obsolete)	NN–166–204	OPM/GOVT–1	KE6	KE6	KE6	KE6	KE6	KE6	KE6
380–5g	Classified Information Nondisclosure Agreement (NDA)-– maintained separately from the individual's official personnel folder	GRS 18–25	A0380–67–DAMI	T75	T75	T75	T75	T75	T75	T75
380–5g	Classified Information Nondisclosure Agreement (NDA)-– maintained separately from the individual's official personnel folder	GRS 18–25	A0380–67–DAMI	T75	T75	T75	T75	T75	T75	T75
380–5j	TOP SECRET document records (related document is downgraded, transferred, or destroyed)	GRS 18–5b	A0001DAMI	KE6	KE6	KE6	KE6	KE6	KE6	KE6
380–5k	Security classification files – Offices in charge of issuance (after final declassification action)	NC1–AU–78–117	N/A	TE10	TE10	TE10	TE10	TE10	TE10	TE10
380–5k	Security classification files – Offices in charge of issuance (after final declassification action)	NC1–AU–78–117	N/A	KE6	KE6	KE6	KE6	KE6	KE6	KE6
380–5n	Office non–registered classified document destruction certificates	NC1–AU–79–27	N/A	KE6	KE6	KE6	KE6	KE6	KE6	KE6
380–5r	Security information exchanges	NC1–AU–78–117	N/A	T20	T20	T20	T20	T20	T20	T20
380–5s	Security compromise cases (completion of final corrective or disciplinary action)	NC1–AU–330–76–1	N/A	KE6	KE6	KE6	KE6	KE6	KE6	KE6
380–5s	Security compromise cases: records of violations of a sufficiently serious nature to be classified as felonies (completion of final corrective or disciplinary action)	NC1–AU–330–76–1	N/A	TEP	TEP	TEP	TEP	TEP	TEP	TEP
380–5u	Security equipment files (termination of the exception)	NN–166–204	N/A	TE10	TE10	TE10	TE10	TE10	TE10	TE10

Table F–1
File Titles and Dispositions for Records—Continued

MARKS Number	File Title	NARA Authority	Privacy Act Systems Notice	Organizational Level						
				A	B	C	D	E	F	G
380–5w	Security regrading cases – Offices in charge of regrading	NC1–AU–78–117	N/A	T15	T15	T15	T15	T15	T15	T15
380–5w	Security regrading cases – Other offices	NC1–AU–78–117	N/A	KE6	KE6	KE6	KE6	KE6	KE6	KE6
380–5x	Security information access cases – Offices having Army-wide responsibility	NC1–AU–78–117	A0380–67–DAMI	T20	T20	T20	T20	T20	T20	T20
380–5x	Security information access cases – Other offices	NC1–AU–78–117	A0380–67–DAMI	KE6	KE6	KE6	KE6	KE6	KE6	KE6
380–5y	Security information releases – Offices having Army–wide responsibility	NCI–AU–78–117	N/A	T20	T20	T20	T20	T20	T20	T20
380–5y	Security information releases – Other offices	NCI–AU–78–117	N/A	KE6	KE6	KE6	KE6	KE6	KE6	KE6
380–5z	Non–cryptographic registered document accounts (superseded by a new report if all information referred to is accounted for either by a report of destruction or inclusion in the new report)	II–NNA–1002	A0001DAMI	KE6	KE6	KE6	KE6	KE6	KE6	KE6
380–5aa	TOP SECRET material accountability (after all items on each page have been destroyed, downgraded, dispatched, or when entries are transferred to a new page)	GRS 18–5a	N/A	KE6	KE6	KE6	KE6	KE6	KE6	KE6
380–5bb	Industrial information security	NC1–AU–83–28	N/A	TP	TP	TP	TP	TP	TP	TP
380–5dd	Activity Entry/Exit Inspection Program	GRS 18–8	N/A	K6	K6	K6	K6	K6	K6	K6
380–150d	Atomic information exchanges	NC1–AU–76–51	N/A	K6	K6	K6	K6	K6	K6	K6
380–381j	SAP security management files: Interim security classification guides – sponsoring program/activity (after supersession or final declassification action)	N1–AU–92–1	N/A	KE6	KE6	KE6	KE6	KE6	KE6	KE6
380–381j	SAP security management files: Final security classification guides – Offices with Army-wide responsibility	N1–AU–92–1	N/A							
380–381j	SAP security management files: Final security classification guides – Other offices	N1–AU–92–1	N/A	KE6	KE6	KE6	KE6	KE6	KE6	KE6

Code:
Organizational Level:
A = Company and below
B = Battalion
C = Brigade

Table F–1
File Titles and Dispositions for Records—Continued

MARKS Number	File Title	NARA Authority	Privacy Act Systems Notice	Organizational Level						
				A	B	C	D	E	F	G

D = Division, Installation
E = Corps, Major Subordinate Command
F = Individual Army, Major Command
G = HQDA, Secretariat

Disposition Instruction:
K6 = Keep until no longer needed for conducting business, but not longer than 6 years.
KE6 = After a specific event occurs, keep until no longer needed for conducting business, but not longer than 6 years.
T (followed by a numeral) = Transfer to records holding area when no longer required for conducting business. The time period specified is when the Records Holding Area (RHA) will destroy the record, based on the creation date.
TE (or TE followed by a numeral) = Transfer to the RHA in accordance with event instructions. The time period shown is when the RHA will destroy the record, based on the event date.
TP or TEP = Transfer to Records Holding Area when no longer required for conducting business. The P indicates that these area permanent records. They will be transferred to the National Archives within 30 years in accordance with the governing records retention schedule.
NOTE: Records requiring transfer to the RHA will be prepared and transferred by deployed units monthly and at the end of the deployment. All other units will prepare and transfer annually by fiscal or calendar year. See your Installation Records Manager for instructions on transferring records.

Table F–2
File Numbers and Descriptions for Records

FN: 380–5a
Title: Security briefings and debriefings
Authority: NC1–AU–78–116
Privacy Act: A0380–67DAMI
Description: Information on classified material, to include Sensitive Compartmented Information (SCI), and security briefing and debriefing of personnel authorized access to classified material. Included are briefing statements, debriefing statements and certificates, and related information.
Disposition: Destroy 2 years after transfer or separation of person.

FN: 380–5b
Title: Security inspections and surveys
Authority: NN–173–72
Privacy Act: Not applicable
Description: Information on inspections and surveys that are conducted by security officers. This includes SCI security inspections and surveys, and routine after–duty–hours security inspections conducted under the supervision of a security officer to decide the adequacy of measures taken to protect security information against the hazards of fire, explosion, sabotage, and unauthorized access. Included are reports, recommendations, and related information.
Disposition: Destroy after next comparable inspection or survey.

FN: 380–5d
Title: Classified material access files
Authority: NN–166–204
Privacy Act: OPM/GOVT–1
Description: Information showing authorization to have access to classified files. This includes forms containing person's name and signature, classification of files concerned, information desired, signature of an official authorizing access, and similar data.
Disposition: Destroy on transfer, reassignment, or separation of the person, or when obsolete.

FN: 380–5g
Title: Classified Information Nondisclosure Agreement (NDA)
Authority: GRS 18, Item 25
Privacy Act: A0380–67DAMI
Description: Copies of nondisclosure agreements; such as SF 312 or SF 189 and DD Form 1847–1 (Sensitive Compartmented Information Nondisclosure Statement/SCI NDA or similar forms; signed by military or civilian personnel including employees of contractors, licensees, or grantees with access to information that is classified under standards put forth by Executive Orders governing security classification. These forms should be maintained separately from personnel security clearance files. Agreements for civilian employees working for elements of the intelligence community must be maintained separately from the official personnel folder. For all other persons, these forms may be filed in the individual's official military personnel folder (for uniformed military personnel) or on the right side of the official personnel folder (for civilian employees).
Disposition: a. If maintained separately from the individual's official personnel folder. Destroy when 70 years old.
b. If maintained in the individual's official personnel folder. Apply the disposition for the official personnel folder.

FN: 380–5j
Title: TOP SECRET document records
Authority: GRS 18, Item 5b
Privacy Act: A0001DAMI

Table F–2
File Numbers and Descriptions for Records—Continued

Description: Information used to record the names of persons having had access to TOP SECRET information and copies of extracts distributed.
Disposition: Destroy when related document is downgraded, transferred, or destroyed.

FN: 380–5k
Title: Security classification files
Authority: NC1–AU–78–117
Privacy Act: Not applicable
Description: Information relating to the security classification or grading system involving the classification or downgrading of information. Included are correspondence or memorandums and reports on security classification. It excludes other files described in this record series.
Disposition: a. Offices in charge of issuance: Destroy 10 years after final declassification action.
b. Other offices and TOE units: Destroy after 3 years.

FN: 380–5n
Title: Office nonregistered classified document destruction certificates
Authority: NC1–AU–79–27
Privacy Act: Not applicable
Description: Forms and other types of information that show the destruction of classified information.
Disposition: Destroy after 2 years, or earlier when approved by HQDA (DAMI–CIS) WASH DC 20310.

FN: 380–5r
Title: Security information exchanges
Authority: NC1–AU–78–117
Privacy Act: Not applicable
Description: Information on the exchange of security classified information with other Government agencies, industry, and foreign governments. Included are correspondence on the exchange of information, exchange agreements, and related information.
Disposition: Destroy after 20 years.

FN: 380–5s
Title: Security compromise cases
Authority: NC1–330–76–1
Privacy Act: Not applicable
Description: Information on investigations of alleged security violations. Included are SCI security violations such as missing information, unauthorized disclosure of information, unattended open security containers, and information not properly safeguarded.
Disposition: Destroy 2 years after completion of final corrective or disciplinary action. Records of violations of a sufficiently serious nature to be classified as felonies are permanent.

FN: 380–5u
Title: Security equipment files
Authority: NN–166–204
Privacy Act: Not applicable
Description: Information gathered for the determination of uses and types of security equipment for protecting classified information and materials. They include safes, alarm systems, and other security equipment.
Disposition: Destroy after 10 years. Destroy exceptions to storage standards 10 years after termination of the exception.

FN: 380–5w
Title: Security regrading cases
Authority: NC1–AU–78–117
Privacy Act: Not applicable
Description: Information on the review of specific classified information or equipment for the purpose of regrading the information or equipment.
Disposition: a. Offices in charge of regrading: Destroy after 15 years.
b. Other offices: Destroy after 3 years.

FN: 380–5x
Title: Security information access cases
Authority: NC1–AU–78–117
Privacy Act: A0380–67DAMI
Description: Information on the review of specific requests for access to classified files or equipment for purposes of research and study.
Disposition: a. Offices having Army–wide responsibility: Destroy after 20 years.
b. Other offices: Destroy after 2 years.

FN: 380–5y
Title: Security information releases
Authority: NCI–AU–78–117
Privacy Act: Not applicable
Description: Information on the review of classified or potentially classified documentary materials for dissemination of information to sources outside the Army, such as the review of manuscripts, photography, lectures, radio, and television scripts, and other materials.
Disposition: a. Offices having Army–wide responsibility: Destroy after 20 years.
b. Other offices: Destroy after 2 years.

FN: 380–5z
Title: Noncryptographic registered document accounts
Authority: II–NNA–1002
Privacy Act: A0001DAMI

Table F–2
File Numbers and Descriptions for Records—Continued

Description: Information showing the accountability of non–Army noncryptographic registered information. Included are semiannual inventory or report of transfer, transfer reports, and similar information.
Disposition: Destroy when superseded by a new report if all information referred to is accounted for either by a report of destruction or inclusion in the new report.

FN: 380–5aa
Title: TOP SECRET material accountability
Authority: GRS 18, Item 5a
Privacy Act: A0001DAMI
Description: Information showing the identity, receipt, dispatch, downgrading, source, movement from one office to another, destruction, and current custodian of all TOP SECRET material for which the TOP SECRET control office is responsible.
Disposition: Destroy 5 years after all items on each page have been destroyed, downgraded, dispatched, or when entries are transferred to a new page.

FN: 380–5bb
Title: Industrial information security
Authority: NC1–AU–83–28
Privacy Act: Not applicable
Description: Information on the protection of classified information in the possession of industry, including information on the issuance of clearance certificates, and related information.
Disposition: Permanent.

FN: 380–5dd
Title: Activity Entry and Exit Inspection Program
Authority: GRS 18, Item 8
Privacy Act: Not applicable
Description: Documents collected at MACOMs, SUBMACOMs, and Staff agencies in the conduct of an inspection program to deter and detect unauthorized introduction or removal of classified material from DOD owned or leased installations and facilities. Included are—
a. The date(s) and number of entry and exit inspections conducted by the activity and subordinate elements during the previous quarter.
b. The number of instances during the quarter when persons handcarried classified information without apparent authorization.
c. Problems encountered in the conduct of the entry and exit inspection program.
Note: Use FN 380–5s to file information on investigations on alleged security violations.
Disposition: Cut off at end of calendar year. Destroy 2 years after cut off.

FN: 380–150d
Title: Atomic information exchanges
Authority: NC1–AU–76–51
Privacy Act: Not applicable
Description: Information relating to requests from various foreign governments or allies for atomic information, to include requests for regulations, manuals, reports, and other related information.
Disposition: Destroy after 1 year.

Appendix G
Security Classification Guide Preparation

G–1. Preparation guidance

a. 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.

b. This appendix supplements DOD Directive 5200.1–H. DOD Directive 5200.1–H has not been revised, as of yet, to include new classification criteria and marking requirements of Executive Order 12958. But it still provides useful guidance on preparing classification guides.

c. The question of classifying guides themselves requires careful consideration.

(1) Guides should be published in unclassified form if possible; however, classified guides may be published in classified form 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 Programs (SAPs) information. See appendix I, of this regulation and AR 380–381 for more information.

(2) Preparers of guides must be careful that descriptions of classified information in the guide do not inadvertently disclose classified information.

(3) Like any other classified document, classified guides must be portion marked and marked with the identity of the classifier and declassification instructions.

d. Section II provides instructions on changing and reissuing guides.

e. Section III contains instructions for preparing and submitting DD Form 2024. These instructions supplement those found on the reverse of the form.

f. Figure G–1 is a reprint of DODD 5200.1–H. Note: Except for sections 1, 2, 6, and 7, the sample guide contains only a sampling of topics that normally would be included. Comments are enclosed in parentheses. References are to DODD5200.1–R, tailored as best as possible to this regulation.

G–2. Procedures for changing security classification guides

a. Whenever a security classification involving a guide subject changes, that change must be reflected by revision or reissuance of the guide. It may also be necessary to clarify or correct information in the guide or provide additional information or instructions.

b. The terms "revision" and "reissuance" have specific meanings which must be understood because they are used differently on DD Form 2024.

(1) The term "revision" includes the following three types of actions:

(a) 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).

(b) An errata sheet, which corrects an error (typographical or otherwise) in a guide.

(c) An addendum, which adds new material to a guide. 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.

(2) Revisions will show the date of approval.

c. The term "reissuance" 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 reissuance. The original issue of the guide or the latest prior reissuance (if any) will be shown under "Supersessions."

d. Revisions and reissued guides must be approved, distributed, and reported as required in section 5 of DODD 5200.1–R.

G–3. Instructions for preparing DD Form 2024

a. Submission of DD Form 2024, required by paragraph 2–18d of this regulation, allows the listing of a security classification guide in DODD 5200.1–I.

b. DD Form 2024 must be prepared at least in four copies. One copy is to be retained with the record copy of the SCG. In the case of new guides, revisions, or reissuances, the DD Form 2024 should accompany the copies of the SCG submitted to the Administrator, Defense Technical Information Center (DTIC).

c. The correct edition date for DD Form 2024 is July 1986. Previous editions are obsolete and should not be used.

d. The reverse side of DD Form 2024 provides instructions for completing the form. The following guidance supplements and clarifies these instructions.

(1) Paragraph B of the instructions defines the meanings of the six blocks in Item 1 of the form.

(a) The "new guide" block should be checked when reporting any of the following:

(1) The issue of a guide covering a subject on which no previous guide has been issued.

(2) Reissue of a guide which is not currently indexed in DODD 5200.1–I.

(b) 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.

(2) 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.

(3) 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.

(4) 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.

(5) In Item 7, enter a date two years from the date of issue, reissue, or the last review, whichever is latest.

(6) 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."

(7) 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 DODD 5200.1–I. Carefully study the list of index terms found in DODD 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, HQDA. If none of the current terms are appropriate, submit recommended additions to Headquarters Department of the Army, DCSINT, ATTN: DAMI–CH, 2511 Jefferson Davis Hwy, Suite 9300, Arlington, VA 22202–3910. Ensure that the index terms do not disclose classified information about the SCG subject.

(8) The index sequence number entered in Item 11 is essential to the accuracy of DODD 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 DODD 5200.1–I must be entered in Item 11. Two special circumstances deserve mention:

(a) 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.

(b) In a very few cases, a revision or correction to a recently issued SCG which has not yet been listed in DODD 5200.1–I will be issued. In such cases, leave item 11 blank.

(9) Item 14, "Remarks," may be used to advise the recipients of DD Form 2024 of any additional information considered appropriate. Information placed in Item 14 will not appear in DODD 5200.1–I. Item 14 may be left blank.

(10) DD Form 2024 states that completing Item 16a, "Action Officer," is optional. Within the Department of the Army, an action officer will be indicated in Item 16a each time DD Form 2024 is prepared. The person listed should be the current action officer for the SCG.

e. 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 14 of the DD Form(s) 2024 for the new SCG(s) will not cancel the superseded SCG(s).

f. When the proponent of a SCG changes due to organizational changes or progress in system development, the following instructions apply:

(1) 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.

(2) If responsibility is assumed by a U.S. Army element from an agency outside the U.S. 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. Canceling the old SCG is the responsibility of the former proponent.

(3) 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.

DOD Directive 5200.1-H

DEPARTMENT OF DEFENSE

HANDBOOK FOR WRITING

SECURITY CLASSIFICATION GUIDANCE

1998

THE ASSISTANT SECRETARY OF DEFENSE FOR

COMMAND, CONTROL, COMMUNICATIONS, AND

INTELLIGENCE

FOREWORD

This Handbook is issued under the authority of DoD Directive 5200.1, "DoD Information Security Program, " December 13, 1996. Its purpose is to assist in the development of the security classification guidance required under paragraph 2-500 of DoD Regulation 5200.1-R, for each system, plan, program, or project in which classified information is involved.

DoD 5200.1-H, "Department of Defense Handbook for Writing Security Classification Guidance," March 18, 1986, is hereby canceled.

This Handbook is effective immediately.

Users of this Handbook are encouraged to direct comments to the Director, Security; Office of the Deputy Assistant Secretary of Defense (Security and Information Operations), 6000 Defense, The Pentagon, Washington, DC 20301-6000.

//signed//

Christopher K. Mellon

Deputy Assistant Secretary of Defense

(Security and Information Operations)

Figure G-1. DOD Directive 5200.1–H

Distribution of this Handbook is authorized to U.S. Government Agencies and their contractors. Administrative or Operational Use, August 1992 Other requests for this document shall be referred to the Security Programs Directorate, Office of the Deputy Assistant Secretary of Defense (Security and Information Operations), Washington, DC 20301-6000

REFERENCES

(a) Executive Order 12958, "Classified National Security Information," April 20, 1995

(b) Information Security Oversight Office Directive No. I, "Classified National Security Information," October 13,1995

(c) DoD Regulation 5200.1-R, "Information Security Program," January 14, 1997, authorized by DoD Directive 5200.1, December 16, 1996

(d) DoD Regulation 5400.7-R, "DOD Freedom of Information Act Program," May 1997, authorized by DoD Directive 5400.7, "DoD Information Act Program," September 1997

(e) Deputy Secretary of Defense Memorandum, "Web Site Administration," December 1998

Figure G-1. DOD Directive 5200.1–H—Continued

C.1. CHAPTER 1
INTRODUCTION

C.1.1.
Good security classification practice in an organization as large and widespread as the Department of Defense, calls for the timely issuance of comprehensive guidance regarding security classification of information concerning any system, plan, program, or project; the unauthorized disclosure of which reasonably could be expected to cause damage to the 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 interests of national security. Executive Order 12958 (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.

C.1.2.
Information is classified to assist in ensuring that it is provided an appropriate level of protection. Therefore, it is essential that a classification guide be concerned with identifying the specific items of information and the level of protection required, as well as the time period for which protection must be continued.

C.1.3.
A classification guide should be issued as early as practical in the life cycle of the classified system, plan, program or project. Any uncertainty in application of the policies and procedures contained in DOD Regulation 5200.1–R, "Information Security Program," (reference (c)), which implements the provisions of reference (a) and (b) within DOD, 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.

C.1.4.
DOD information that does not, individually or in compilation, qualify for classification, must be reviewed in accordance with DOD Regulation 5400.7 (reference (d)), prior to its release outside DOD. In addition, such information must also be reviewed for compliance with the provisions of Deputy Secretary of Defense Memorandum, dated December 7, 1998 (reference (e)), prior to its placement on any publicly accessible DOD web site.

C.2. Chapter 2
CLASSIFICATION AND DECLASSIFICATION

C.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.

C.2.2. CLASSIFICATION
2.2.1 Basically, information is classified in one of two ways, either originally or derivatively. Original classification occurs when information is developed which intrinsically meets the criteria for classification under Executive Order 12958 (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. Derivative classification occurs when the information under consideration fits the description of information already known to be classified.

2.2.2 Classification may be applied only to information that is owned by, produced by or for, or is under the control of the United States Government. Information may be considered for classification only if it concerns one of the categories specified in Section 1.5a of Executive Order 12958 (reference (a)):

2.2.2.1 Military plans, weapon systems, or operations;

2.2.2.2 Foreign government information;

2.2.2.3 Intelligence activities (including special activities), intelligence sources or methods, or cryptology;

2.2.2.4 Foreign relations or foreign activities of the United States, including confidential sources;

2.2.2.5 Scientific, technological, or economic matters relating to the national security;

2.2.2.6 United States Government programs for safeguarding nuclear materials or facilities; or

2.2.2.7 Vulnerabilities or capabilities of systems, installations, projects or plans relating to the national security.

2.2.3 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 follow. These steps may be laid out as a series of questions.

2.2.3.1 Is the information owned by, produced by or for, or under the control of the United States Government?

2.2.3.2 Does the information fall within one or more of the several categories of information in paragraph C.2.2.1 through C.2.2.7 above? If the answer to this question is "no," the information cannot be classified. If the answer is "yes," then the next question applies.

2.2.3.3 Can the unauthorized disclosure of the information reasonably be expected to cause damage to the national security? If the answer is "no," the information cannot be classified. If the answer is "yes," then the third question applies.

2.2.3.4 What is the degree of damage to the national security that is expected in the event of an unauthorized disclosure

of the information? If the answer to this question is “damage” you have arrived at a decision to classify the information Confidential. If the answer is “serious damage,” you have arrived at a decision to classify the information Secret. If the answer is “exceptionally grave damage,” you have arrived at a decision to classic the information Top Secret.

C.2.3. Declassification

The declassification decision determines duration of protection, and is as important as the original classification determination. At the time an item of information is classified, original classifiers shall:

2.3.1 Assign a date within ten years from the date of classification upon which the information can be automatically declassified;

2.3.2 Determine a specific event, reasonably expected to occur within years, that can beset as the signal for automatic declassification; or

2.3.3 Designate the information as being automatically declassified on a date ten years from the date of its original classification.

2.3.3 An original classifier may extend classification beyond ten years only if:

2.3.3.1 The unauthorized disclosure of the information could reasonably be expected to cause damage to the national security for a period in excess of 10 years, and

2.3.3.2 Release of the information could reasonably be expected to:

2.3.3.2.1 Reveal an intelligence source, method, or activity, or a cryptologic system or activity;

2.3.3.2.2 Reveal information that would assist in the development or use of weapons of mass destruction;

2.3.3.2.3 Reveal information that would impair the development or use of technology within a United States weapon system;

2.3.3.2.4 Reveal United States military plans, or national security emergency preparedness plans;

2.3.3.2.5 Reveal foreign government information;

2.3.3.2.6 Damage relations between the United States and a foreign government, reveal a confidential source, or seriously undermine diplomatic activities that are reasonably expected to be ongoing for a period greater than 10 years;

2.3.3.2.7 Impair the ability of responsible United States Government officials to protect the President, the Vice President, and other individuals for who protection services are authorized;

2.3.3.2.8 Violate a statute, treaty, or international agreement.

C.2.4. DOWNGRADING

Executive Order 12958 (reference (a)) does permit an 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.

C.3. Chapter 3

A PLAN OF ACTION FOR WRITING CLASSIFICATION GUIDES

C.3.1. STEP 1. CONSIDER RELATED CURRENT GUIDANCE

C.3.1.1.

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 system, plan, program or project 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.

C.3.1.2.

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 5200.1–1 (reference (e)) 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 (e), but be aware that some classification guides are too sensitive to be identified in that document. 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. If your activity has an information security specialist, that individual may be a particularly valuable source of advice and assistance.

C.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:

3.2.1 The known or published status, foreign and domestic.

3.2.2 The known but unpublished (probably classified) status in the United States.

3.2.3 The known but unpublished status in friendly and unfriendly countries.

3.2.4 The extent of foreign knowledge of the unpublished status in the United States.

C.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.

3.3.1 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.

3.3.2 Fact of possession by the United States.

3.3.3 Capabilities of the resulting product in terms of quality, quantity, and location.

3.3.4 Performance, including operational performance, as it relates to capabilities.

3.3.5 Vulnerabilities, weaknesses, countermeasures, and counter–countermeasures.

3.3.6 Uniqueness, exclusive knowledge by the United States.

3.3.7 Lead time, which is related to state–of–the–art.

3.3.8 Surprise, which is related to possession and capability to use.

3.3.9 Specifications, which may be indicative of goals, aims, or achievements.

3.3.10 Manufacturing technology. 3.3.11 Associations with other data or activities.

C.3.4. STEP 4. MAKE INITIAL CLASSIFICATION DETERMINATION

Making the analyses outlined in sections C.3.2 and C.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.

C.3.5. STEP 5. IDENTIFY SPECIFIC ITEMS OF INFORMATION THAT REQUIRE CLASSIFICATION

3.5.1 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 subject matter of the guide, or the level at which the classification guide is issued, there are certain identifiable features of the information that create or contribute to actual or expected national security advantage. There also may be certain items of information 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 items of information 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 so as to minimize the probability of error by those who will use the classification guide. (See chap 4 for a complete discussion on classifying hardware items.)

3.5.2 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 provide such guidance will result in users of the guide making their own interpretations which may, or may not, be consistent with your intent.

C.3.6. STEP 6. DETERMINE HOW LONG CLASSIFICATION MUST CONTINUE

3.6.1 Equally important to determinations to classify, are the decision on how long the classification should remain in effect. The following are factors that may influence this decision:

3.6.1.1 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 over time.

3.6.1.2 At certain stages in production, or deployment, it may not be practical or possible to protect certain items of information from disclosure. It is also possible that design improvements may have eliminated exploitable vulnerabilities.

3.6.1.3 Official public releases have a direct affect on the duration of classification.

3.6.2 With these factors in mind, and considering the provisions of Chapter 2.3., proceed with the determination of the appropriate declassification instructions for each item of classified information.

3.6.3 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 when the damage that is expected to result from an unauthorized disclosure will be reduced to a level prescribed for lower classification.

C.3.7. STEP 7. WRITING THE GUIDE

3.7.1 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 that are unclassified as this assures 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, "FA–5B Aircraft Security Classification Guide."

3.7.2 There are a number of administrative requirements for security classification guides. Bear in mind that the security classification guide you are writing must:

3.7.2.1 State precisely the specific information elements to be protected.

3.7.2.2 Identify the classification levels "TS," "S," or "C" and any additional control marking such as Restricted Data (RD), Formerly Restricted Data (FRD) or NO FOREIGN DISSEMINATION (NOFORN), that may apply to each element of information, or when it will serve a useful purpose, specify that the information is unclassified.

3.7.2.3 Identify the reason for classification.

3.7.2.4 Specify the duration of classification for each element of information (except RD and FRD). RD and FRD is subject to the provisions of the Atomic Energy Act, therefore, no declassification determination should be entered for this information.

3.7.2.5 State any downgrading action that is to occur, and when such action is to take place.

3.7.2.6 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 as well as the Office of Primary Responsibility that can be contacted for clarification or additional information.

3.7.2.7 Include amplifying comments whenever appropriate to explain the exact application of classification.

C.4. Chapter 4

CLASSIFYING HARDWARE ITEMS

C.4.1. GENERAL

A piece of hardware may convey information which is every bit as sensitive as words printed upon a piece of paper.

C.4.2. BASIC CONSIDERATIONS

Hardware items may be classified if they reveal information or information can be obtained from them. The following are some basic considerations:

4.2.1 An item of hardware does not necessarily need to be classified simply because it is part of a classified product or effort.

4.2.2 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 are necessary to delineate for users of the guide, what information requires protection.

4.2.3 Frequently, classified information pertaining to a hardware item can be restricted to the paper work associated with the item.

4.2.4 Unusual, unique, or peculiar uses or modifications of ordinarily available unclassified materials or hardware 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 it is the hardware or material that reveals classified information, or that it is the association of use of the hardware with a particular effort that reveals such information.

4.2.5 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.

4.2.6 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 with 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 that may reveal classified information. This is a prime opportunity to identify and isolate classification requirements.

C.4.3. USER CONSIDERATIONS

Know who will be using your classification guide.

4.3.1 Usually management and staff supervisory personnel need to have a fairly broad knowledge of classification requirements. Farther down the line however, foremen and workers 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 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 association.

4.3.2 When planning a production line, careful attention is needed to delay as long as possible the insertion of classified hardware items.

4.3.3 Test equipment rarely embodies classified information. 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.

C.5. CHAPTER 5

CLASSIFYING MILITARY OPERATIONS INFORMATION

C.5.1. GENERAL

The security classification of military operations information is subject to many of the considerations described in Chapter C.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 that can be applied.

C.5.2. MILITARY OPERATIONS INFORMATION

Military operations 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.

C.5.3. MILITARY OPERATIONS CLASSIFICATION CONSIDERATIONS

5.3.1 Successful battle operations depend largely upon our ability to assess correctly the capability and intention of enemy forces at each stage of the battle while concealing our own capabilities and intentions, and to communicate an effective battle doctrine throughout our forces. Classifiable information would include:

5.3.1.1 The number, type, location, and strengths of opposing units.

5.3.1.2 The capabilities and vulnerabilities of weapons in enemy hands, and how he normally applies the weapons.

5.3.1.3 The morale and physical condition of the enemy force.

5.3.2 In considering classification guidance for military operations, there may be good reason to classify more information about the operations 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.

5.3.3 The following are examples of information relating to military operations that may warrant classification:

Table C–1
Classification guidance

TOPIC	CLASS	DECLASS	REMARKS
Overall operational plans	"S"	Date, event, date w/in 10 yrs	
System operational deployment or employment	"C"	After deployment or Employment	
Initial Operational Capability (IOC) Date	"C"	After IOC Date	
Planned location of operational units	"S"	After arrival on site	
Equipage dates, readiness dates, Operational employment dates	"S"	After these events	
Total manpower or personnel Requirements for total operational Force	"C"	After operation	
Coordinates of selected operational sites	"S"	"C" after site activation; "U" on termination of site.	
Specific operational performance Data which relates to the effectiveness of the control of forces and data on specific vulnerabilities and weaknesses.	"S"	Date/event, date w/in ten years	
Existing OPSEC and COMSEC Procedures, projections, and techniques.	"S"	Date/event, date w/in ten years	
Target characteristics	"S"	Date/event, date w/in ten years	

C.6. CHAPTER 6
CLASSIFYING INTELLIGENCE INFORMATION

C.6.1. CLASSIFICATION CONSIDERATIONS
Producers of intelligence must be wary of applying so much security that they are unable to provide a useful product to their consumers. 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 are not necessarily all–inclusive:

6.1.1 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.

6.1.2 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.

6.1.3 Intelligence identifying a sensitive source or method is classified, as well as the evaluation of the particular source or method.

6.1.4 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.

6.1.5 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, whether under a formal government–to–government agreement or, simply with the understanding that the information is provided in confidence, the information must be protected at the level and for the length of time the United States and the transmitting government agree to. If the information is obtained from a foreign government without any agreement or restrictions, the classification, if any, should be based solely on the content of the information provided.

6.1.6 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 enemy intelligence collection and analysis capabilities, efforts, and successes. An integral part of this data is an assessment of enemy human intelligence, signals intelligence, and reconnaissance satellite capabilities.

6.1.7 Security classification assigned to intelligence received from non–Defense sources must be respected by Defense users.

6.1.8 An intelligence estimate is normally classified since it contains sensitive sources, methods, or raw or evaluated intelligence.

6.1.9 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.

6.1.10 The classification of relationships with foreign intelligence organizations is related to the following considerations:

6.1.10.1 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.

6.1.10.2 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.

6.1.10.3 Details of or specifics concerning any intelligence exchange agreements are classified. In some instances, the mere fact of such an agreement may be classified.

6.1.10.4 The identities of foreign governmental or military personnel who provide intelligence under such agreements or liaison relationships may be classified.

6.1.11 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.

6.1.12 Cryptologic information (including cryptologic sources and methods) is classified.

6.1.13 Information concerning electronics intelligence, telemetry intelligence, and electronic warfare is usually classified.

6.1.14 The intelligence community normally considers the following categories of information to be classified:

6.1.14.1 Cryptologic, cryptographic, signals intelligence, or imagery intelligence.

6.1.14.2 Counterintelligence.

6.1.14.3 Special access programs.

6.1.14.4 Information which identifies clandestine organizations, agents, sources, or methods.

6.1.14.5 Information on personnel under official or nonofficial cover, or revelation of a cover arrangement.

6.1.14.6 Covertly obtained intelligence reports and the derivative information which would divulge intelligence sources or methods.

6.1.14.7 Methods or procedures used to acquire, produce, or support intelligence activities.

6.1.14.8 Intelligence organizational structure, size, installations, security, objectives, and budget.

6.1.14.9 Information that would divulge intelligence interests, value, or extent of knowledge on a subject.

6.1.14.10 Training provided to or by an intelligence organization which would indicate its capability or identify personnel.

6.1.14.11 Personnel recruiting, hiring, training, assignment, and evaluation policies.

6.1.14.12 Information that could lead to foreign political, economic, or military action against the United States or its allies.

6.1.14.13 Events leading to international tension that would affect U.S. foreign policy.

6.1.14.14 Diplomatic or economic activities affecting national security or international security negotiations.

6.1.14.15 Information affecting U.S. plans to meet diplomatic contingencies affecting national security.

6.1.14.16 Nonattributable activities conducted abroad in support of U.S. foreign policy.

6.1.14.17 U.S. surreptitious collection in a foreign nation that would affect relation with the country.

6.1.14.18 Covert relationships with international organizations or foreign governments.

6.1.14.19 Information related to political or economic instabilities in a foreign country threatening American lives and installation there.

6.1.14.20 Information divulging U.S. intelligence and assessment capabilities.

6.1.14.21 United States and allies' defense plans and capabilities that enable a foreign entity to develop countermeasures.

6.1.14.22 Information disclosing U.S. systems and weapons capabilities or deployment.

6.1.14.23 Information on research, development, and engineering that enables the United States to maintain an advantage of value to national security.

6.1.14.24 Information on technical systems for collection and production of intelligence.

6.1.14.25 U.S. nuclear programs and facilities.

6.1.14.26 Foreign nuclear programs, facilities, and intentions.

6.1.14.27 Contractual relationships that reveal the specific interest and expertise of an intelligence organization.

6.1.14.28 Information that could result in action placing an individual in jeopardy.

6.1.14.29 Information on secret writing when it relates to specific chemicals, reagents, developing, and microdots.

6.1.14.30 U.S. Military space programs.

C.6.2. INTELLIGENCE DECLASSIFICATION CONSIDERATIONS

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 Chapter 3 of this Handbook on determining how long classification must continue is applicable to all information, including intelligence.

C.6.3. 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 security classification guide. In addition, the following is provided as an example of security classification guidance that might be applied to a Human Intelligence (HUMINT) effort:

Table C–2
HUMINT classification guide

TOPIC	CLASS	DECLASS	REMARKS
Biographic information taken exclusively from open source, where no intelligence connection is shown.	"U"		
Positive identification of an individual as potential source to a U.S. intelligence agency.	"S–TS"	Date/event w/in ten years, or 10 years from origination.	"TS" if identified as an actual source.
Identity of a target installation or target personality when not linked to a specific collection operation.	"S"	Date/event w/in ten years, or 10 years from origination.	"TS" when linked to an actual source or specific collection operation.
Interest in specific events for collection exploitation, including specific areas of technology.	"S"	Date/event w/in ten years, or 10 years from origination.	
Names of collection agency case officers in conjunction with a specific collection operation.	"C"	Date/event w/in ten years, or 10 years from origination.	
Information on collection agency HUMINT policy plans, resources, Methods, or accomplishments.	"S"	Date/event w/in ten years, or 10 years from origination.	

C.7. CHAPTER 7

CLASSIFYING FOREIGN RELATIONS INFORMATION

C.7.1. GENERAL

The Department of State (DoS) is the agency primarily responsible for the development and execution of the foreign policy of the United States, and thus is also the primary agency responsible for the security classification of foreign relations information. Most Defense classification determinations in the area of foreign relations will be derivative in nature. However, there will be instances where Defense projects and programs involve foreign relations information for which security classification guidance must be developed.

C.7.2. FOREIGN RELATIONS CLASSIFICATION CONSIDERATIONS

The following are some of the types of information or material involving foreign relations that warrant classification consideration:

7.2.1 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.

7.2.2 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:

7.2.2.1 A foreign official speaking in a highly critical manner of his own government's policy.

7.2.2.2 A foreign official suggesting how pressure might effectively be brought to bear on another part of his own government.

7.2.2.3 A foreign official acting in unusually close concert with U.S. officials where public knowledge of this might be harmful to that foreign official.

7.2.2.4 A foreign official whose professional advancement would be beneficial to U.S. interest, 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.

7.2.3 All unpublished, adverse comments by U.S. officials on the competence, character, attitudes, or activities of a serving foreign government official.

7.2.4 All material which constitutes or reveals unpublished correspondence between heads of state or heads of government.

7.2.5 Statements of U.S. intent to defend, or not to defend, identifiable areas, or along identifiable lines, in any foreign country or region.

7.2.6 Statements of U.S. intent to attack militarily in stated contingencies, identifiable areas in any foreign country or region.

7.2.7 Statements of U.S. policies or initiatives within collective security organizations, e.g., NATO.

7.2.8 Agreements with foreign countries for the use of, or access to, military or naval facilities.

7.2.9 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.

7.2.10 Defense surveys of foreign territories for purposes of basing or using in contingencies.

7.2.11 Statements relating to any use of foreign bases not authorized under bilateral agreements.

C.7.3. CLASSIFICATION GUIDE ILLUSTRATIONS

7.3.1 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. The following is provided as an example of the impact that foreign government information might have on the development of classification guidance.

7.3.1.1 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.

7.3.1.2 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 ordinarily be 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 description of foreign government information. Thus, a classification guide on the subject might contain the following topics:

Table C–3
Classification of notes and transcripts

TOPIC	CLASS	DECLASS	REMARKS
Apple orchard negotiations with country "X."	"U"		Mere fact of negotiations only, and elaboration may be classified, see next topic.
Transcripts of apple orchard negotiations and substantive notes pertaining to them.	"C"	Requires consultation with foreign government	

7.3.1.3 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.

7.3.1.4 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. Classification guide topics might read as follows:

Table C–4
Classification topics

TOPIC	CLASS	DECLASS	REMARKS
(U) Fact of U.S. overflights – Europe			
a. (S) Country "Y"	"S"	Requires written approval of foreign government involved.	(S) Must be at least 50,000 feet altitude; lower flights not permitted in "Y" and "Z"
b. (C) Country "Z"	"C"		
(U) Other European	"U"		

Notes:

In this example, the guide itself would have to be classified "S" as it reveals the information that country "Y" has determined would result in serious damage.

Appendix A
CLASSIFICATION FACTORS

The following questions, answers, and potential actions will assist in systematically determining whether certain broad aspects of an effort warrant security classification:

CLASSIFICATION FACTORS

The following questions, answers, and potential actions will assist in systematically

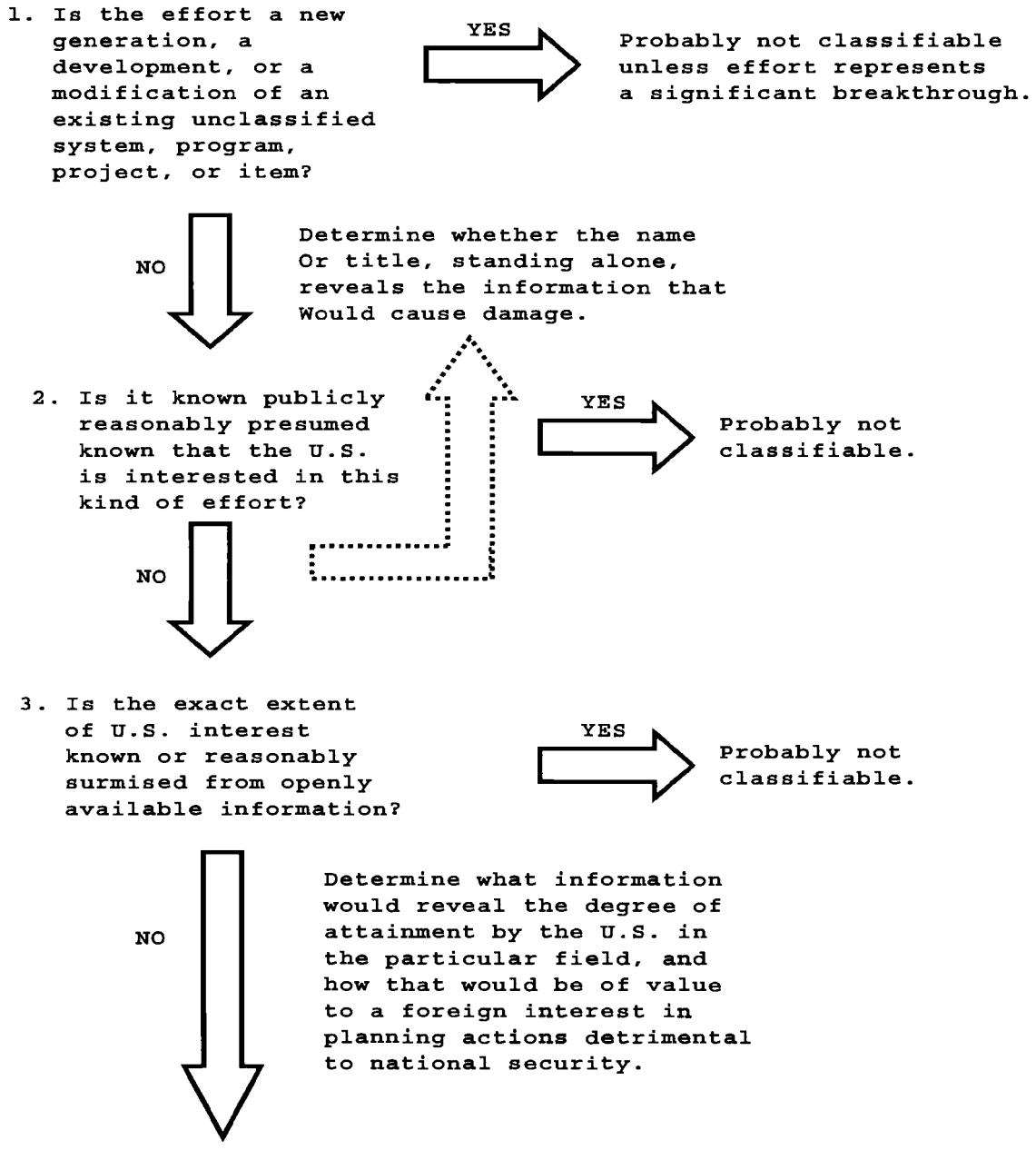


Figure A-1. CLASSIFICATION FACTORS

determining whether certain broad aspects of an effort warrant security classification:

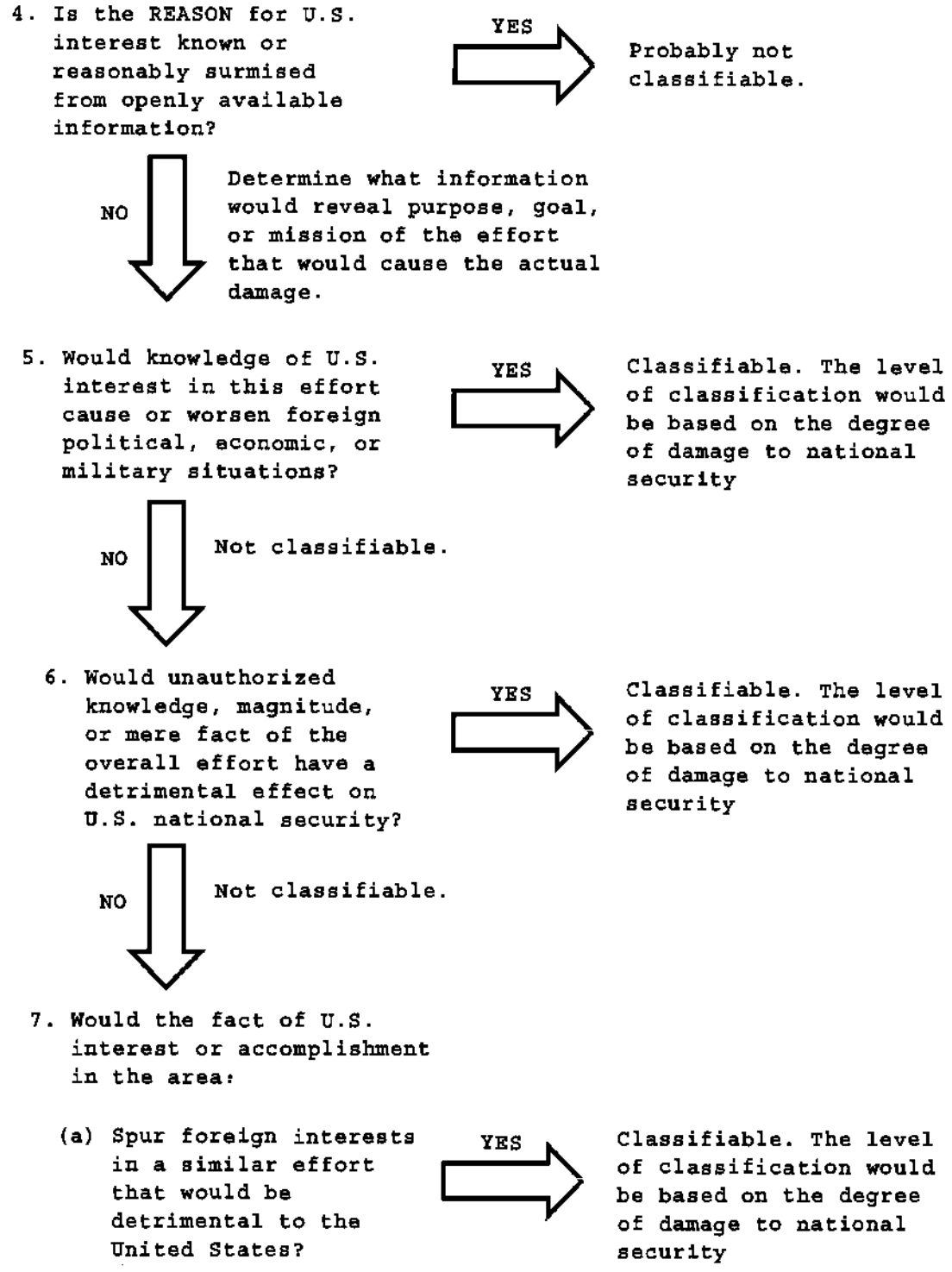


Figure A-1. CLASSIFICATION FACTORS—Continued

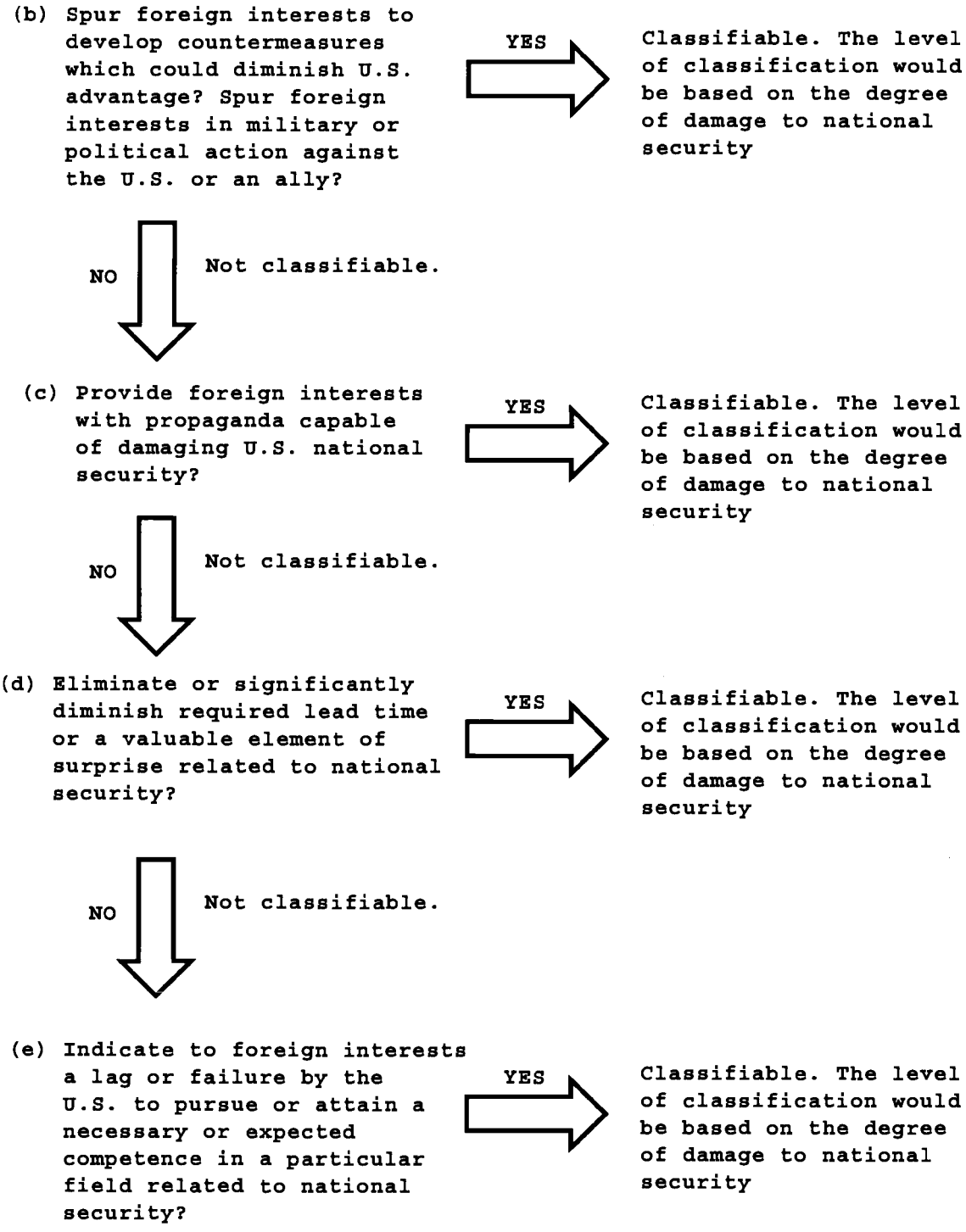


Figure A-1. CLASSIFICATION FACTORS—Continued

Appendix B
CLASSIFYING DETAILS

Having considered the factors involved in making classification determinations 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 to determine security classification. The questions are not presented in any order of priority. A listing of specific items of information to consider is contained in Appendix C.

B.1. PERFORMANCE OR CAPABILITY

b.1.1. 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.1.2. How does this degree or kind of performance contribute to or create a national security advantage? How much of an advantage?

b.1.3. How long can this data be protected? The advantage

b.1.4. How would knowledge of these performance details help an enemy, or damage the success of the effort?

b.1.5. 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?

B.2.. UNIQUENESS

b.2.1. What information pertaining to this effort is know or believed to be the exclusive knowledge of the United States?

b.2.2. Is it known or reasonable to believe that other nations have achieved a comparable degree of success or attainment?

b.2.3. What information, if disclosed, would result in or assist other nations in developing a similar item or arriving at a similar level of achievement?

b.2.4. In what way or ways does the uniqueness of this item contribute to a national security advantage?

b.2.5. In what way or ways has the end product of this effort or any of its parts been modified, developed, or applied so at to be unique to this kind of effort? How unique is this?

b.2.6. 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 of application in this kind of effort?

B.3. TECHNOLOGICAL LEAD TIME

b.3.1. How long did it take to reach this level of performance or achievement?

b.3.2. How much time and effort have been expended? Was this a special concerted effort, or only a gradual developmental type of activity?

b.3.3. 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?

b.3.4. Have other nations reached this level of development or achievement?

b.3.5. Do other nations know how far we have advanced in this kind of effort?

b.3.6. 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?

b.3.7. How important, in terms of anticipated results, is the lead time we think we have gained?

b.3.8. What national security advantage actually results from this lead time?

b.3.9. How long is it practical to believe that this lead time will represent an actual advantage?

b.3.10. How long is it practical to expect to be able to protect this lead time?

B.4. SURPRISE

b.4.1. Do other nations know we have reached this level of development or achievement?

b.4.2. 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?

b.4.3. What is the nature of the advantage resulting from surprise use of this end item?

b.4.4. When will this element of surprise be lost?

B.5. VULNERABILITIES AND WEAKNESSES

b.5.1. What are the weak spots in this effort that make it vulnerable to failure? What is the rate or effect of this failure?

b.5.2. How will the 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?

b.5.3. What elements of this effort are subject to countermeasures?

b.5.4. How would knowledge of these vulnerable elements assist in planning or carrying out countermeasures?

b.5.5. Can information concerning these weak or vulnerable elements be protected from unauthorized disclosure – or are they inherent in the system?

b.5.6. Can these weaknesses or vulnerabilities be exploited to reduce or defeat the success o this effort? How could this be done?

b.5.7. What measures are planned or have been taken to offset these weaknesses or vulnerabilities?

b.5.8. Are the counter–countermeasures obvious, special, unique, unknown to outsiders or other nations?

b.5.9. How would knowledge of these counter–countermeasures assist in carrying out or planning new countering efforts?

b.5.10. Would knowledge of specific performance capabilities assist in developing or applying specific countermeasures? How? What would be the effect on the expected national security advantage?

B.6. SPECIFICATIONS

b.6.1. What would details of specification reveal:

(6.1.1) A special or unusual interest that contributes to the resulting or expected national security advantage?

(6.1.2) Special or unique compositions that contribute to the resulting or expected national security advantage?

(6.1.3) Special or unique levels of performance that are indicative of a classifiable level of achievement or goal?

(6.1.4) Special, or unique use of certain materials that reveals or suggests the source of a national security advantage?

(6.1.5) Special or unique size, weight, or shape that contributes to the resulting or expected national security advantage?

b.6.2. Are any specification details in themselves contributory to the resulting or expected national security advantage? How?

b.6.3. Can details of specifications be protected? For how long?

B.7. CRITICAL ELEMENTS

b.7.1. What are the things that really make this effort work?

b.7.2. Which of these critical elements contribute to the resulting of expected national security advantage? How? To what extent?

b.7.3. Are these critical elements the source of weakness or vulnerability to countermeasures?

b.7.4. What details of information pertaining to these critical elements disclose or reveal the national security advantage, weakness or vulnerability?

b.7.5. Can details of information pertaining to these critical elements be protected by classification? For how long?

B.8. MANUFACTURING TECHNOLOGY

b.8.1. What manufacturing methods, techniques, or modes of operation were developed to meet the requirements of this effort?

b.8.2. Which of these manufacturing innovations are unique to this effort or this product? Are they generally known or suspected?

b.8.3. Are these manufacturing innovations essential to successful production of the product?

b.8.4. What kind of lead time results from these innovations?

B.9. ASSOCIATIONS

b.9.1. Are there any associations between this effort and others that raise classification questions?

b.9.2. Are there associations between information in this effort, and already publicly available information (unclassified), that raise classification problems?

b.9.3. Is it necessary or possible to classify items of information in this effort because of their association with other unclassified or classified information would diminish or result in the loss of a national security advantage?

B.10. PROTECTABILITY

b.10.1. Can the information effectively be protected from unauthorized disclosure by classification? For how long?

b.10.2. If not, what alternative means can be used to ensure protection?

Appendix C
ITEMS OF INFORMATION

Table C–1 shows items of information that may disclose present or future strategic or tactical capabilities and vulnerabilities and which should be considered when preparing classification guidance:

Table C–1
Strategic and Tactical Capabilities and Vulnerabilities

Performance And Capabilities Accuracy
Alert time
Altitude
  Maximum
  Optimum
Ballistics
  Initial
  Terminal
Control
Countermeasures (proven, unproven)
  Counter–countermeasures
  Decoys
  Electronic
  Penetration aids
  Shield materials
Depth/height (also of burst)
  Maximum
  Optimum
Duration (flight)
Effectiveness
Frequencies (bands, specific, command, operating, infrared, microwave, radio, COMSEC)
Heating
Impulse
Intercept
Lethality/critical effects
Lift
Limitations
Maneuverability
Military strength
  Actual
  Planned, predicted, anticipated
Miss distance
Noise Figure
Operational readiness time cycle
Payload
Penetration
Range (range scales)
Rate of fire
Reaction time
Reliability/failure rate data
Resolution
Response time
Sensitivity
Sequence of events
Signature Characteristics
  Acceptance
  Analysis
  Distinguishment
  Identification
Speed/velocity
  Acceleration/deceleration
  Cruise
  Intercept
  Landing
  Maximum
  Minimum
  Optimum
Stability
Target data
  Details
  Identification
  Illumination
  Impact predicted
  Preliminary
Priority
  Range determination
Thresholds
Thrust
Toxicity

SPECIFICATIONS
(Detailed, Basic, Subsidiary)

Balance
Burn rate
Capacity (system)
Center of gravity
Codes
Composition
Configuration/contour
Consumption
Energy requirements
  Specific
  Total
Filler
Loading/loads
Mass factor (propellant)
Moment of inertia
On–station time
Output data
Payload
Power requirements
Purity
Size, weight, shape
Stability (static, dynamic)
Strength of members, frames
Stresses

Table C–1
Strategic and Tactical Capabilities and Vulnerabilities—Continued

TOPIC	CLASS	DECLASS	REMARKS
Fineness	Thickness		
Gain configuration	Tolerance		
Hardness, degree	Type		
Input data			
VULNERABILITY			
Countermeasures/counter Countermeasures	Signature characteristics Acoustic		
Dynamic pressure (supersonic)	Electrical		
EMP (radiation)	Infrared		
Ground or air shock	Magnetic		
Jamming	Pressure		
	Radar		
	Static overpressure		
PROCUREMENT AND PRODUCTION			
Completion date or dates	Progress/schedules (mile–stones)		
Numbers	Stock density		
Dispersion (numbers per unit of force)	Supply plans and status		
On–hand stockpile	Tactical deployment		
Planned or programmed (totals scheduled)			
Rate of delivery or production			
Requirements			
Spares			
OPERATIONS			
Countdown time	Plans		
Deployment data	Command and control		
Environment	Results		
Location	Analysis, Conclusions, reports		
Numbers available	Sequences of events		
Objectives	Staging techniques		
Mission of program	Statement.concept		
Specific or general	Tactical		
Test, broad or detailed	Build–up, units per force activation dates, personnel		

Appendix D
Recommended Format For A Security Classification Guide

This Appendix illustrates a format for a security classification guide. (A cover page is recommended showing essentially the following:)

Section 1
NAME OF THE PROGRAM, PROJECT, SYSTEM OR STUDY

(If necessary, use an acronym, short title or project number in order to keep title unclassified)

SECURITY CLASSIFICATION GUIDE

(Date of the guide)

ISSUED BY: (Name and address of issuing office.)

APPROVED BY: (Original Classification Authority)
(Statement of supersession of any previous guides.)

(Distribution Limitation Statement for the Defense Technical Information Center per DOD Directive 5230.24 (reference (e))

PROGRAM, PROJECT, SYSTEM (ETC.) SECURITY CLASSIFICATION GUIDE
(Date of the guide):

Section I
GENERAL INSTRUCTIONS

1. Purpose.
To provide instructions and guidance on the classification of information involved in (insert name of the program, project, etc., using an unclassified identification of the effort).

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"). 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 (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).

3. Office of Primary Responsibility (OPR):
This guide is issued by, and all inquiries concerning content and interpretation, as well as any recommendations for changes, should be addressed to:

(Name, code, mailing address of issuing office)

(An administrative or security office in the issuing activity may be used. Inclusion of the action officer's name and phone number/fax and e–mail is desirable.)

4. Classification Challenges.
If at any time, any of the security classification guidance contained herein is challenged, the items of information involved shall continue to be protected at the level prescribed by this guide until such time as a final decision is made on the challenge by appropriate authority. Classification challenges should be addressed to the OPR.

5. Reproduction, Extraction and Dissemination.
Authorized recipients of this guide may reproduce, extract, and disseminate the contents of this guide, as necessary, for application by specified groups involved in (identification of the effort), including industrial activities. Copies of separate guides issued to operating activities in application of this guide shall be sent to the OPR.

NOTE: If it is necessary to classify the guide, you may have to modify this paragraph to express any required limitations.

6. Public Release.
The fact that this guide shows certain details of information to be unclassified does not allow automatic public release of this information. Proposed public disclosures of unclassified information regarding (identification of effort) shall be processed through appropriate channels for approval. 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.

(Include in this paragraph the definitions of any items for which there may be various meanings to ensure common understanding of the details of information that are covered by the guide.)

Section II
OVERALL EFFORT

9. Identification.

(Include in this paragraph any necessary statements explaining the classifications, if any, to be assigned to various statements identifying the effort. These statements should be consistent with other program documentation.)

10. Goal, Mission, Purpose.

(Include in this paragraph any necessary statements identifying information concerning the purpose of the effort that can be released as unclassified and that which must be classified. Take care to ensure that unclassified statements do not reveal classified information.)

11. End Item.

(Include in this paragraph statements of the classification to be assigned to the end products of the effort, whether paperwork or hardware. In this connection it is important to distinguish between classification required to protect the fact of the existence of a completed end item, and classification required because of what the end item contains or reveals. 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 any of the parts or materials.)

Section III
PERFORMANCE AND CAPABILITIES

(This section includes characteristics of performance and capability of an end item, or an end item's components, parts, or materials, the performance or capabilities of which require classification In this section, also 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 are unclassified. 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.)

Table D–1
Performance and capabilities topics

TOPIC	CLASS	DECLASS	REMARKS
1. Range			
a. Actual	"S"	15 June 1999	
2. Accuracy/range rate			
a. Predicted	"C"	30 Jan 2000	
3. Altitude: Operational	"C"	30 Jan 2000	
Maximum	"C"	30 Jan 2000	The statement "in excess of 50,000 feet" is "U"
4. Receiver sensitivity, selectivity, and frequency coverage.	"S"	15 Apr 2005	If standard commercial receivers are used, their characteristics are "U" but their application to this effort shall be "S."
5. Resolution Thermal			Planned or actual attained
a. Maximum	"S"	15 Apr 2001	thermal resolutions above
b. Operational optimum	"S"	15 Apr 2001	0.25 degrees C. are "U."

Table D–1
Performance and capabilities topics—Continued

TOPIC	CLASS	DECLASS	REMARKS
c. Operational attainment	"S"	15 Apr 2001	
6. Speed			
a. Maximum	"S"	15 Jan 2001	Downgrade to "C" upon IOC.
b. Rate of climb	"S"	15 Jan 2001	Reference to "supersonic speed" is "U."
c. Intercept	"S"	15 Jan 2001	

Section IV
SPECIFICATIONS

This section includes items of information describing standards for qualities of materials and parts; methods or modes or 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. (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.)

Table D–2
Specification topics

TOPIC	CLASS	DECLASS	REMARKS
1. Burn rate	"C"	17 Sep 2001	
2. Power requirement	"S"	17 Sep 2001	Only when associated with advanced model ##, otherwise "U."

Section V
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 paragraph each significant item of information peculiar to these critical elements and the classification applicable. Also include in this section the classification to be assigned to information pertaining to components, parts, and materials that are peculiar and critical to the successful operation of the end item in 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 can be included in this section instead of section 3.

Section VI
VULNERABILITIES AND WEAKNESSES

This section is used to specify classification 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. Classification assigned to details of information on countermeasures and counter–countermeasures should be included in this section.

Section VII
ADMINISTRATIVE DATA

This section is used only if particular elements of administrative data, such as program information, procurement schedules, production quantities, schedules, programs, or status of the effort, and data on shipments, deployment, or transportation and manuals (field, training, etc.) warrant classification.

Table D–3
Administrative data topics

TOPIC	CLASS	DECLASS	REMARKS
1. Planned delivery rate.	"C"	13 Mar 2001	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 VIII
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 classification, if any, to be assigned. Any such expansion or elaboration should be fully coordinated the he 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 classification for certain hardware items. In such cases it probably would be advisable to explain why classification is 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.

Table D–4
Hardware classification

INFORMATION REVEALING	CLASS	DECLASS	REMARKS
1. End item hardware:			
a. AN/APR–999	"C"	20 Aug 2000	External views of the assembled AN/AR-999 are "U."
(1) Analyzer unit	"C"	20 Aug 2000	
(2) Threat display	"U"		
(3) Preamplifier	"U"		
b. AN/APR–OOOO	"C"		

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 need 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 later case, the downgrading instruction could be placed in a "Remarks" or "Comments" column.

Table E–1
Format variation topics

Example 1

TOPIC	CLASSIFICATION	DECLASSIFY	COMMENTS
1.4.1 System capacity	"S"	30 Jun 2004	Downgrade to "C" upon TOC
1.4.1 Signature characteristics	"C"	19 Jun 2001	

Example 2

DESCRIPTION	CLASSIFIED	UNTIL	REMARKS
1.4.1 System capacity	"S"	30 Jun 2004	Downgrade to "C" upon IOC.
1.4.2	"C"	19 Jun 2001	

Example 3

INFORMATION		
REVEALING	CLASSIFICATION/DECLASSIFICATION	REMARKS
1.4.1 System capacity	"S" DCL on 30 Jun 2004	Downgrade to "C" upon IOC
4.1 Signature characteristics	"C" DCL on 19 Jun 2001	

COVER BRIEF

TO: SENIOR CIVILIAN OFFICIAL, OASD(C31)

THROUGH: PDASD(C31)

DASD(S&10)
DASD(S&10)

FROM: DIRECTOR, SECURITY PROGRAMS
Prepared by WHBell/695–2686

SUBJECT: Revision of DOD 5200.1–H, "DOD Handbook for Writing Security Classification Guidance – ACTION MEMORANDUM

PURPOSE: To obtain SCO signature on the SD 106 at Tab A.

DISCUSSION:

In implementation of Executive Order 12958, "Classified National Security Information," and Information Security Oversight Office Directive No. 1, DOD Regulation 5200.1–R requires that a security classification guide be issued for each system, plan, program, or project in which classified information is involved. The Handbook provides guidance and illustrations to assist DOD Component personnel in developing such guides. The SD 106 at Tab A has been prepared to obtain DOD Component coordination on the proposed revision of the Handbook.

COORDINATION: OASD(C31)(Policy)_____

RECOMMENDATION:
That the SCO sign the SD 106 at Tab A.

Appendix H
Instructions Governing Use of Code Words, Nicknames, and Exercise Terms

Section I
Definitions

H–1. 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.

H–2. Code Word
Word selected from those listed in Joint Army–Navy–Air Force Publication (JANAP) 299 and later volumes, and assigned a classified meaning by appropriate authority to ensure proper security concerning intentions, and to safeguard information pertaining to actual military plans or operations classified as Confidential or higher. A code word will not be assigned to test, drill or exercise activities. A code word is placed in one of three categories:

a. Available. Allocated to the using component. Available code words individually will be unclassified until placed in the active category.

b. Active. Assigned a classified meaning and current.

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

H–3. 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.

H–4. 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.

Section II
Policy and Procedure

H–5. 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.

a. A permanent record of all code words will be maintained by the Joint Chiefs of Staff.

b. The using component will account for available code words and maintain a record of each active code word. Upon being canceled, the using component will maintain the record for 2 years; thence the record of each code word may be disposed of in accordance with current practices, and the code word returned to the available inventory.

c. 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 Headquarters DA, DAMO–ODS, Washington, D.C. 20310–0440.

H–6. Nicknames
a. 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.

b. Nicknames, improperly selected, can be counterproductive. A nickname must be chosen with sufficient care to ensure that it does not—

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

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

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

c. The following will not be used as nicknames:

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

(2) Combination of words including word "project," "exercise," or "operation."

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

(4) Exotic words, trite expressions, or well–known commercial trademarks.

d. The Joint Chiefs of Staff will—

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

(2) Prescribe a method for the using components to report nicknames used.

e. The heads of DOD components will—

(1) Establish controls within their components for the assignment of nicknames authorized under paragraph H–6a.

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

(3) All requests for and changes in nicknames, including assignments, meanings, changes to meanings, cancellations, deletions, and possible compromises will be submitted in writing to Headquarters DA, DAMO–ODS, Washington, D.C. 20310–0440.

H–7. Exercise terms

a. 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.

b. Selection of exercise terms will follow the same guidance as contained in paragraph 6a.

c. The Joint Chiefs of Staff will—

(1) Establish a procedure by which exercise terms may be authorized for use by DOD components.

(2) Prescribe a method for using components to report exercise terms used.

d. The heads of DOD components will—

(1) Establish controls within their component for the assignment of exercise terms authorized under paragraph 7a.

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

(3) 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 Headquarters DA, DAMO–ODS, Washington, D.C. 20310–0440 in accordance with AR 525–1 and JCS PUB 6, Vol. II.

H–8. Assignment of classified meanings to code words

a. The DOD component responsible for the development of a plan or the execution of an operation will be responsible for determining whether to assign a code word.

b. Code words will 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(1), above; or,

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

c. The using component will assign to a code word a specific meaning classified TOP SECRET, SECRET, or CONFIDENTIAL, commensurate with military security requirements. Code words will not be used to cover unclassified meanings. 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 will 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 will 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 will establish policies and procedures for the control and assignment of classified meanings to code words, subject to applicable rules set forth herein.

H–9. Notice of assignment, dissemination, and cancellation of code words and meanings

a. The using component will promptly notify the Joint Chiefs of Staff when a code word is made active, indicating the word, and its classification. Similar notice will 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 Headquarters DA, DAMO–ODS, Washington, D.C. 20310–0440, of all codeword 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 agency furnishes a word that has a special meaning for use within DOD, recipients will be informed that it originated outside the DOD and is not subject to the DOD'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 canceled code words. This cancellation report is considered final action, and no further reporting or accounting of the status of the canceled code word will be required.

H–10. 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 will have the same classification. When dissemination of the plan to other DOD components or to subordinate echelons of the using component is required, the using component may downgrade the code words assigned below the classification assigned to their meanings in order to facilitate additional planning implementation, and execution by such other components or echelons, but code words will, 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, will be canceled, and classified CONFIDENTIAL for a period of 2 years, after which the code word will become unclassified.

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

d. In every case, whenever a code word is referred to in documents, the security classification of the code word will 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 will declassify the meaning and the code word and return the code word to the available inventory.

H–11. 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 will not be used.

b. In handling correspondence pertaining to active code words, care will 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 will not be used for addresses, return addresses, shipping designators, file indicators, call signs, identification signals, or for other similar purposes.

H–12. Disposition

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

Appendix I
Special Access Programs (SAPs)

Section I
General

I–1. Policy

It is the policy of the Department of the Army to use the security classification categories, and the applicable sections of EO 12958 and its implementing ISOO Directives, to limit access to classified information on a "need–to–know" basis for only those personnel who have been determined to meet requisite personnel security requirements. Further, it is DA policy to rigorously apply the need–to–know principle in the normal course of controlling collateral classified information, so that Special Access Programs (SAPs) controls will be used only when exceptional security measures are required, based on threat and/or vulnerability (e.g. sensitivity or value of the information) associated with the SAPs. The following sections are excerpts from AR 380–381, and should be reviewed prior to initiation of any SAPs.

I–2. Restrictions on using Special Access Programs

a. Only approved Prospective Special Access Programs (PSAPs) and SAPs may use the extraordinary security measures outlined in this regulation and AR 380–381.

b. Proponents of acquisition, intelligence, or operations and support activities, who identify a particularly sensitive piece of information that they believe merits SAPs protection, should report this information, through their chain of command, for a security policy review. If a determination is made that the information warrants SAPs controls, the MACOM/Program Executive Office (PEO) will report this to the Chief, Technology Management Office (TMO), who coordinates a security review at HQDA. Some examples of potential SAPs are–

(1) A specific technology with potential for weaponization that gives the United States a significant technical lead or tactical advantage over potential adversaries.

(2) Sensitive technology that is especially vulnerable to foreign intelligence exploitation without special protection.

(3) An emerging technology, proposed operation, or intelligence activity risking the compromise of other SAPs.

(4) Exposure of sensitive activities that could jeopardize the lives of U.S. citizens.

(5) A capability that is so unique or sensitive that it requires protection beyond normal procedures.

(6) An extremely sensitive activity requiring special protection from disclosure to prevent significant damage to national security or the reputation or interests of the United States.

(7) Methods used to acquire foreign technology or equipment.

(8) Sensitive support to DOD and non–DOD agencies.

c. In compliance with DOD policy, HQDA and its subordinate units and activities will not establish, disestablish, implement, fund, categorize, create carve–out status, or change the mission or scope of a SAP, without written approval of the Deputy Secretary of Defense (DEPSECDEF).

d. The Department of Defense National Industrial Security Program Supplement Overprint, dated February 14, 1998, contains further and more specific guidance, especially regarding the enhanced security requirements, procedures, and options involved with the National Industrial Security Program Operating Manual (NISPOM) for:

(1) Critical restricted data (RD) classified at the Secret and Top Secret levels.

(2) Special Access Programs and SAP–type compartmented efforts established and approved by the Executive Branch.

(3) Sensitive Compartmented Information (SCI) or other DCI SAPs–type compartmented programs under the Director of Central Intelligence which protect intelligence sources and methods.

(4) Acquisition, intelligence and operations and support SAPs.

Section II
Responsibilities

I–3. The Secretary of the Army

The Secretary of the Army (SA) has overall responsibility for SAPs within the Department of the Army. The SA will–

a. Make recommendations to the DEPSECDEF concerning the establishment, disestablishment, categorization, carve–out status, and changes of mission and scope of Army SAPs.

b. Ensure adequate oversight of Army SAPs.

c. Delegate, at SA discretion, management of Army SAPs.

I–4. The Under Secretary of the Army

The Under Secretary of the Army will–

a. Approve SAPs reprogramming actions.

b. Serve as co–chairman of the SAPs Program Performance and Budget Execution Review System (PPBERS).

I–5. The Assistant Secretary of the Army (Acquisition, Logistics and Technology)

The Assistant Secretary of the Army (Acquisition, Logistics and Technology (ASA(ALT)) will–

a. Serve as the Army Acquisition Executive for all Army programs, including SAPs, and as the principal assistant to the SA for matters relating to Acquisition SAPs (AQ–SAPs).

b. Ensure a single subordinate commander of a MACOM or Program Executive Officer is responsible for each AQ–SAPs throughout its life cycle.

c. Conduct periodic reviews of secure environment contracting conducted in support of SAPs.

d. Ensure SAPs protection and procedures for procurement and fielding of systems, components, and modifications are developed and acquired under SAPs provisions.

e. Coordinate with the Office of the Deputy Chief of Staff for Intelligence (ODCSINT) on issues concerning technology transfer.

f. Coordinate within Army and other DOD components to eliminate duplication of effort and ensure consistent security classification for similar technologies.

g. Coordinate technical review of PSAPs.

h. Evaluate proposed acquisition strategies and plans for Army SAPs.

i. Coordinate with Office of the Deputy Chief of Staff for Logistics (ODCSLOG) to integrate logistics support and property accountability considerations into AQ–SAPs efforts and products.

I–6. The Assistant Secretary of the Army (Manpower and Reserve Affairs)

The Assistant Secretary of the Army (Manpower and Reserve Affairs) (ASA(M&RA)) will–

a. Review and assist in developing policy regarding personnel and personnel security support to SAPs.

b. Provide guidance concerning the documentation process to ensure that Tables of Distribution of Allowances (TDA) accurately reflect Army requirements consistent with approved SAPs missions and the Army Authorization Document.

c. Evaluate and approve requests for special pays, as appropriate, in support of SAPs missions.

d. In coordination with the ASA(FM&C), assist in establishing guidance to ensure proper control and accountability of financial data pertaining to Army personnel assigned to SAPs.

I–7. The Assistant Secretary of the Army (Financial Management and Comptroller)

The Assistant Secretary of the Army (Financial Management and Comptroller) (ASA(FM&C)) will–

a. Provide financial and budget policy and guidance for SAPs.

b. Provide liaison with Congress for SAPs budgets.

c. Coordinate with Defense Finance and Accounting (DFAS) to ensure DFAS provides a secure finance and accounting network to process sensitive financial transactions.

d. Provide financial quality assurance oversight through the Special Review Office (SRO).

e. Coordinate the Army's Budget Estimate Submission for SAPs with OSD.

I–8. The Director of Information Systems for Command, Control, Communications, and Computers

The Director of Information Systems for Command, Control, Communications, and Computers (DISC4) will–

a. Coordinate information systems support for SAPs.

b. Assist TMO in developing information systems policy for SAPs.

c. Validate and approve Information System Support Plans (ISSPs).

d. Through USACECOM Technology Applications Office (TAO):

(1) Provide information management support in preparing Information Systems Requirements Packages (ISRPs) and Information Management Support Plans (IMSPs).

(2) Provide technical advice and support in preparing ISRPs and IMSPs.

I–9. The General Counsel

The General Counsel (GC) will–

a. Review Army SAPs and prospective Army SAPs for legality and propriety before submission to OSD.

b. Advise the SA on legal and policy issues.

c. Conduct policy reviews.

I–10. The Inspector General

The Inspector General (TIG) will–

a. Evaluate managerial procedures and practices pertaining to operations, personnel, materiel, funding, secure environment, contracting, and security of SAPs.

b. Identify issues, situations, or circumstances that affect SAPs mission performance.

c. Provide a secure system for program personnel to report fraud, waste, and abuse without fear of reprisal or unnecessary disclosure of information.

d. Conduct non–criminal investigations as directed by the Vice Chief of Staff, Army.

e. Inspect Army SAPs and Army involvement in non–Army SAPs.

f. Develop and coordinate an annual inspection plan with TMO, other inspection/audit agencies, MACOMs, and PEOs.

I–11. The Auditor General

The Auditor General (TAG) will–

a. Maintain auditors with appropriate clearance and access to perform audits of SAPs.

b. Coordinate with TMO when performing audits of SAPs.

I–12. Chief of Public Affairs

The Chief of Public Affairs (PA) will–

a. Staff media queries on SAPs and provide releasable information.

b. Provide public affairs guidance on SAPs matters.

I–13. The Chief of Staff, Army

The Chief of Staff, Army (CSA) will develop, coordinate, review, and conduct oversight of all Army SAPs.

I–14. The Vice Chief of Staff, Army

The Vice Chief of Staff, Army (VCSA) will–

a. Review SAPs through the Special Access Programs Oversight Committee (SAPOC) and serve as chairman of the SAPOC.

b. Serve as the chairman of the Executive Fix–It Committee.

c. Serve as the co–chairman of the SAPs PPBERS.

d. Provide guidance and direction to Chief, TMO.

I–15. The Deputy Chief of Staff for Personnel

The Deputy Chief of Staff for Personnel (DCSPER) will–

a. Provide policy on SAPs personnel matters.

b. Coordinate with ODCSOPS to establish procedures ensuring MACOM SAPs properly use allocated personnel spaces to resource the SAPs.

c. Ensure that the U.S. Army Total Personnel Command (PERSCOM) coordinates designated DA approved personnel assignment actions for SAPs.

I–16. The Deputy Chief of Staff for Intelligence

The Deputy Chief of Staff for Intelligence (DCSINT) will–

a. Oversee Army Intelligence SAPs (IN–SAPs) and serve as IN–SAP Army Staff (ARSTAF) proponent.

b. Establish security, counterintelligence, and intelligence policy for SAPs.

c. Coordinate necessary counterintelligence support for the execution of Army SAPs.

d. Provide OPSEC and threat assessments for responsible MACOMs and program managers to SAPs and present these to the Working SAPOC for inclusion in the SAPOC revalidation briefing.

e. Advise the SAPOC on whether a program or activity warrants SAPs protection.

f. Review SAPs security plans and guides for accuracy and completeness.

g. Provide input as requested to Office of the Deputy Under Secretary of Defense for Policy (Policy Support) (ODUSD(P)(PS)) concerning Army SAPs security classification guides.

h. Coordinate intelligence property issues for Army SAPs with DCSLOG.

i. Coordinate policy for polygraph support to Army SAPs.

j. Review and approve disclosure of official Army information (classified and unclassified) for release to foreign governments and international agencies. Coordinate with TMO and Director for Special Programs, Office of the Under Secretary of Defense for Policy (Policy Support) (OTUSD(P)(PS)) for release of information and technology identified by SAPs proponents for release to foreign governments and international agencies.

I–17. The Deputy Chief of Staff for Operations and Plans

The Deputy Chief of Staff for Operations and Plans (DSCOPS) will–

a. Oversee Operations and Support SAPs (OS–SAPs) and serve as the ARSTAF proponent.

b. Provide policy guidance and standards for Operations Security (OPSEC) measures appropriate for Army SAPs.

c. Develop Army policy and guidance for materiel requirements for SAPs.

d. Establish and validate Army acquisition priorities for SAPs.

e. Coordinate and approve manpower requirements, allocate man–power resources, and prepare Tables Of Distribution And Allowances (TDA) documents for SAPs.

f. Conduct manpower and workload validations of SAPs to support HQDA and PEO/PMs.

g. Task U.S. Army Force Management Support Agency (USAFMSA) to provide necessary support and analysis of SAPs manpower requirements.

I–18. The Deputy Chief of Staff for Logistics

The Deputy Chief of Staff for Logistics (DCSLOG) will–

a. Integrate logistics support for all Army materiel development or acquisition for SAPs.

b. Provide policy guidance on property accountability and logistics support for SAPs.

I–19. Chief of Engineers

The Chief of Engineers (COE) will provide secure architectural–engineering, construction, real estate, and contracting support to SAPs as required.

I–20. The Judge Advocate General

The Judge Advocate General (TJAG) will provide legal and policy advice on SAPs matters to CSA and the ARSTAF.

I–21. Chief of Legislative Liaison

The Chief of Legislative Liaison (CLL) will–

a. Coordinate congressional briefings on Army SAPs.

b. Provide required reports to selected congressional committees on Army SAPs.

c. Assist TMO in updating clearance information for individuals in Congress accessed to Army SAPs.

d. Assist TMO in verifying access of individuals in Congress.

I–22. Director, Program Analysis and Evaluation Directorate

The Director, Program Analysis and Evaluation Directorate (PAED), will–

a. Ensure that SAPs compete with other Army programs for resources in the Program Objective Memorandum (POM) development process.

b. Coordinate with the ARSTAF and TMO to develop SAPs program funding profiles and provide copies of approved profiles to TMO.

c. Provide program analyses for reprogramming actions.

d. Coordinate SAPs POM during the program review process with OSD.

I–23. Chief, Technology Management Office

The Chief, Technology Management Office (TMO), will–

a. Serve as the Army primary point of contact for the management and oversight of Army and Army–supported SAPs.

b. Establish policy for the management of SAPs.

c. Coordinate establishment, maintenance, and disestablishment of SAPs.

d. Act as the approval authority for establishment and disestablishment of Army P–SAPs.

e. Approve the creation or closure of SAPs subcompartments when there is no change to the categorization, carve–out status, mission, or scope of the parent SAPs. In cases where creation or closure of a subcompartment will

change the mission or scope of the parent SAPs, Chief, TMO will submit the action through SA to the Deputy Secretary of Defense for approval.

f. Serve as the Executive Secretary for the SAPOC, SAPs PPBERS, and Fix–It committees.

g. Provide quarterly update reviews to the senior Army leadership.

h. Assist CLL in coordinating congressional SAPs access briefings and congressional notifications.

i. Monitor budget and financing associated with SAPs.

j. Review SAPs for compliance with authorizations, legal constraints, funding, and continued enhanced security measures.

k. Serve as the POC for Army sensitive support to DOD and non–DOD agencies.

l. Maintain a registry of Army involvement in SAPs and sensitive activities.

m. Maintain the Army baseline billet roster.

n. Coordinate indoctrination of ARSTAF principals to Army SAPs.

o. Direct the Sensitive Records and Information Agency (SRIA).

I–24. Commanding General, U.S. Army Training and Doctrine Command

The Commanding General, U.S. Army Training and Doctrine Command (CG, TRADOC), will–

a. Institute procedures to ensure early identification and protection of combat developments, concepts, and systems with SAPs potential.

b. Identify support requirements for SAPs–developed products deployed to the field.

I–25. Commanding General, U.S. Army Materiel Command

Commanding General, U.S. Army Materiel Command (CG, AMC), will–

a. Institute procedures to ensure early identification and protection of potential research and development (R&D) breakthroughs that may warrant SAPs protection.

b. Conduct appropriate technology feasibility reviews of AMC SAPs.

c. Provide support and oversight for AMC SAPs.

I–26. Commanding General, Forces Command

The Commanding General, Forces Command (CG, FORSCOM), will institute procedures to ensure early identification and protection of activities, operational concepts, and combat developments requiring SAPs status.

I–27. Commanding General, U.S. Army Space and Missile Defense Command

The Commanding General, U.S. Army Space and Missile Defense Command (USASMDC), will institute procedures to ensure early identification and protection of potential R&D breakthroughs within the USASMDC that may warrant SAPs protection and coordinate potential release of SAPs information through DA, DCSINT to SAAL–SO and TMO prior to initiating or engaging in preliminary discussions with a foreign government or international organization. DA DCSINT will coordinate, as required, with Director for Special Programs, OTUSD(P)(PS), prior to any release.

I–28. Commanding General, U.S. Army Intelligence and Security Command

The Commanding General, U.S. Army Intelligence and Security Command (CG, USAINSCOM), will–

a. Institute procedures to ensure early identification and protection of sensitive intelligence activities that may warrant SAPs protection.

b. Provide dedicated counterintelligence, security, and OPSEC support to commanders, program managers, or heads of DA activities having proponency for Army SAPs or Army supported SAPs. This support includes Counterintelligence (CI) assessments of Army SAPs, P–SAPs and contractor facilities involved in Army SAPs contracts.

c. Provide DCSINT with counterintelligence assessments of the threat posed to SAPs by Foreign Intelligence Services (FIS) and technology assessments of foreign research and development efforts related to SAPs technologies. Coordinate with DCSINT to provide this information to organizations and installations supporting SAPs.

d. Provide to DCSINT an annual counterintelligence evaluation of the OPSEC and security posture of Army SAPs and Army–supported SAPs.

e. Manage and execute the Army polygraph program in support of SAPs.

f. Provide Technical Surveillance Countermeasures (TSCM), TEMPEST, ADP security and Counter–SIGINT support to SAPs.

g. Conduct security reviews of SAPs disestablishment actions, security plans, and CI support plans.

I–29. Commanding General, U.S. Army Criminal Investigation Command

The Commanding General, U.S. Army Criminal Investigation Command (CG, USACIC), will–

a. Maintain criminal investigators with appropriate clearances and access to conduct investigations of criminal activity in or directed against SAPs.

b. Maintain effective liaison, through individuals well acquainted with special access procedures, with TMO to ensure quick response to investigative requirements.

c. Conduct criminal investigations in all instances of suspected criminal activity in or directed against Army SAPs in accordance with applicable federal statutes, DODD 5205.7, DODI 5505.2 and AR 195–2.

d. Conduct periodic economic crime threat assessments.

e. Coordinate with TMO to conduct crime prevention surveys on SAPs.

I–30. Department of the Army Staff

The Department of the Army (ARSTAF) sections having SAPs proponency or support requirements for SAPs will–

a. Designate a central point of contact for SAPs.

b. Provide appropriate staff oversight for the planning, programming, budgeting, and execution of SAPs.

c. Act as SAPs managers when appointed to do so.

I–31. Major Army Commands and Program Executive Officers

The Major Army Commands (MACOMs) and Program Executive Officers (PEOs) who supervise managers of SAPs will–

a. Assist program managers in managing their programs.

b. Establish internal inspection programs for SAPs.

c. Conduct periodic property reviews to validate new requirements and document materiel assets in support of SAPs.

d. Coordinate with ARSTAF proponents and DCSINT for SAPs intelligence, counterintelligence, and threat assessments.

e. Ensure that all SAPs are incorporated into the Internal Review and Audit Compliance (IRAC) program as described in chapter 4, AR 380–381.

f. Coordinate potential release of SAP information through DA DCSINT to SAAL–SO and TMO prior to initiating or engaging in preliminary discussions with a foreign government or international organization. DA DCSINT will coordinate with Director for Special Programs, OTUSD(P)(PS), prior to any release.

g. Coordinate with USAFMSA for manpower support for TDA documentation.

I–32. Program/Project/Product Managers of SAPs

In addition to the duties and responsibilities normally incumbent on managers and those delineated by law and regulation, Program/Project/Product Managers (PMs) of SAPs will–

a. Maintain essential SAPs information including establishment, documentation, security plans, access rosters, and security inspection records.

b. Plan, prepare, and implement security and OPSEC programs designed to protect critical program information.

c. Coordinate with TMO for information systems advice and support.

d. Establish and maintain a viable records management program.

e. Coordinate with SRIA for records management assistance.

f. Coordinate with the Defense Security Service (DSS) for industrial facility reviews.

g. Identify, establish, maintain, and forward to the SAPs Archive, SRIA, appropriate historical record files pertaining to the program and its operations.

h. Coordinate potential release of SAP information through DA DCSINT to SAAL–SO and TMO prior to initiating or engaging in preliminary discussions with a foreign government or international organization. DA DCSINT will coordinate with Director for Special Programs, OTUSD(P)(PS), prior to any release.

I–33. Sensitive Records and Information Agency (SRIA)

The Sensitive Records and Information Agency (SRIA) will–

a. Operate the Army Records Center for Sensitive Records and Information. Accept, review, process, archive, and destroy Army sensitive records in accordance with DODD 5205.7, AR 380–381, and AR 25–400–2. Respond to requests for information. Conduct records review and disposition.

b. Conduct Army–wide document searches for sensitive information. Compile and prepare document indexes and responsive documents for forwarding to requesting agencies. Coordinate declassification reviews.

c. Maintain the Billet Structure Management System (BSMS) for the Army. Develop, maintain and distribute the BSMS system software. Identify BSMS hardware and software system requirements for Army SAPs. Maintain a consolidated BSMS database for Army SAPs. Ensure consistency between program office databases and SRIA master database through regular periodic updates and data transfers.

I–34. Defense Security Service (DSS)

The Defense Security Service (DSS) will–

a. Maintain industrial security inspectors with appropriate clearances and access to perform facility clearance inspections and industrial security reviews of contractor facilities supporting Army SAPs.

b. Coordinate with TMO in the conduct of industrial security reviews.

Section III
SAP Categories and Types

I–35. SAP Categories

DOD recognizes four generic categories of SAPs: Acquisition (AQ–SAPs), Intelligence (IN–SAPs) and Operations and Support (OS–SAPs), and SCI Programs (SCI–SAPs). Within the Army, ASA(ALT) is the proponent for AQ–SAPs, DCSINT for IN–SAPs, and DCSOPS for OS–SAPs.

a. AQ–SAPs protect sensitive Research, Development, Test, and Evaluation (RDT&E), modification or procurement efforts.

b. IN–SAPs protect the planning and execution of especially sensitive intelligence or counterintelligence units or operations, including the collection, analysis, and exploitation of intelligence. IN–SAPs also protect especially sensitive programs to procure and exploit foreign materiel.

c. OS–SAPs protect the planning, execution, and support to especially sensitive military operations. This type of SAPs may protect organizations, property, operational concepts, plans, or activities.

d. SCI–SAPs protect sensitive compartmented information or other Director Central Intelligence programs which protect intelligence sources and methods.

I–36. SAP Categories of Protection

a. Army SAPs. SAPs categories reflect the sensitivity of protected material and the degree of protection needed beyond collateral security management. Categories I through III delineate programs requiring varying degrees of protection with CAT I being the most sensitive and CAT III being the least sensitive. The Army SAPOC determines the category designation for each SAPs. SAPs categories may change as a program matures based on changing needs for protection or the sensitivity of the information being protected. The categories are–

(1) Category I (CAT I): Army SAPs that are extremely sensitive and include only the most critical technical developments and the most sensitive intelligence and operational activities. Compromise would cause exceptionally grave damage to national security. Only Army CAT I SAPs are eligible for consideration for waived SAP status.

(2) Category II (CAT II): Army SAPs that include critical acquisition, intelligence and operational activities that do not meet the criteria for CAT I. Compromise would cause serious damage to national security.

(3) Category III (CAT III): Army SAPs usually having significant non–Army participation, relatively short duration or are not suitable for a billet structure.

(4) Unless waived by the SAPOC or the DEPSECDEF, if necessary, CAT I, II and III SAPs follow security procedures listed in AR 380–381.

b. Non–Army SAPs.

(1) Category N (CAT–N) is the category designation for SAPs or sensitive activities where the Army is the executive agent but not the sponsor. Security measures for CAT–N SAPs are in accordance with AR 380–381 as amended by Memoranda of Agreement (MOAs) between Army and the program sponsor. CAT–N programs have the same management oversight as Army SAPs unless otherwise directed by the VCSA.

(2) Army elements may also participate in SAPs that are neither sponsored nor executed (primarily) by Army. Approval for, and management of, Army participation in SAPs executed by other organizations are governed by AR 380–381. Security measures for these SAPs are in accordance with the executing organization's security procedures.

I–37. SAPs Types

a. There are two types of SAPs, acknowledged and unacknowledged. An acknowledged SAPs is a program which may be openly recognized or known, however, specifics are classified within that SAPs. The existence of an unacknowledged SAPs, or an unacknowledged portion of an acknowledged program, will not be made known to any person not authorized for this information.

b. Within DOD, three levels of SAPs protection apply. The three levels are waived SAPs, unacknowledged SAPs, and acknowledged SAPs. These SAPs levels are further explained in DODD 0–5207.7 and DODI 0–5205.11.

Section IV
Security of DA SAPs

I–38. Programs Ineligible for SAP Security

a. The extraordinary security measures approved for use with SAPs may not be used by non–SAPs. No collateral program, including programs with approved limited dissemination controls, may use program access non–disclosure agreements (read–on statements), classified code words for program identification, "Carve–out" contracting, "Special

Access Required" markings or cover sheets, a program billet structure, or personnel security investigative or adjudicative requirements more stringent than those required for a comparable level of classified information. These measures are reserved for SAPs.

b. SAPs derive enhanced security primarily from the restricted access features of these programs. Generally, with respect to other security features (for example, physical security, technical security, and so forth), SAPs are held to the same standards as collateral programs at the same classification level.

I–39. Physical Security

a. Security level. As a general rule, SAPs base the level of physical security on the classification level of the information processed or stored by the SAPs.

(1) Category I SAPs and SAPs processing or storing Sensitive Compartmented Information (SCI) adhere to standards established by DCID 1/21 and the applicable requirements of DOD 5105.21–M–1, DOD TS–5105.21–M–2, and DOD TS–5105.21–M–3.

(2) Category II and III SAPs that do not process or store SCI will follow AR 380–5.

b. Risk assessment.

(1) Program managers of CAT II and III SAPs conduct risk assessments during the PSAPs process to determine whether they must implement physical security measures above the standards prescribed in AR 380–5.

(2) Program offices coordinate this risk assessment with supporting INSCOM CI elements and include the results in their SAPs security plan.

(3) The risk assessment incorporates–

(a) Intelligence Threat Report. This is a multi–disciplined counterintelligence report that addresses the general and specific collection threat to the program.

(b) Counterintelligence Assessment. This is an in–depth analysis of the counterintelligence factors affecting the program's overall security and CI/OPSEC posture. INSCOM normally supports SAPs by developing Intelligence Threat Reports and the Counterintelligence Assessments for the programs at their request.

(c) Program Security Assessment. Program Managers integrate information from the Intelligence Threat Report and the Counterintelligence Assessment to determine whether the program requires further technical protection. If so, the PM requests a TSCM Survey (see AR 380–381, para 5–5).

c. Two Person Integrity (TPI). TPI is required for Category I SAPs only.

d. Entry/Exit Searches. The Entry/Exit Inspection Program (EEIP) is, effective by this regulation, no longer a Department of the Army–wide requirement, however, it remains an effective tool that can be used in command security programs to deter and detect the unauthorized removal of classified information. When effectively implemented the Entry/Exit Inspection Program provides visibility and emphasis to the command security program. Its use is a command option.

I–40. Document/Information Security

a. Marking authors of classified information mark documents in accordance with chapter 4, AR 380–5. Additionally, authors of SAPs material will–

(1) Mark SAPs nicknames at the top and bottom of the outside front cover, title page, all interior pages and on the outside back cover of all documents (for example, SECRET/BROKEN BRIDGE/SPECIAL ACCESS REQUIRED).

(2) Mark the subcompartment nickname in accordance with subparagraph (1) above (for example, SECRET/BROKENBRIDGE/STURDY TWIG/SPECIAL ACCESS REQUIRED). The SAPs nickname and the wording "INCLUSIVE" may be used when a report contains information on all subcompartments (for example, SECRET/BROKENBRIDGE/INCLUSIVE/SPECIAL ACCESS REQUIRED).

(3) Use the caveat "SPECIAL ACCESS REQUIRED" on the top and bottom of all pages that contain SAPs information (for example, SECRET/BROKEN BRIDGE/SPECIAL ACCESS REQUIRED).

(4) Mark the beginning of each paragraph with the initial of the classification and the initials of the unclassified nickname of the SAPs and subcompartment if applicable (for example, S/BB). Programs must include the parent SAPs initials before the subcompartment for portions containing subcompartment information (for example, S/BB/ST). Partial paragraphs which begin a page will be marked with appropriate paragraph markings.

b. Further information on marking SAPs, as well as transmission, dissemination, storage, destruction, accountability, receipting, and reproduction, can be found in AR 380–381.

Glossary

Section I
Abbreviations

AASA
Administrative Assistant to the Secretary of the Army

ADP
Automated Data Processing

AMC
U.S. Army Materiel Command

AR
Army Regulation

ARNG
Army National Guard

ARSTAF
Army Staff

ASA(ALT)
Assistant Secretary of the Army (Acquisition, Logistics, and Technology)

ASA(FM&C)
Assistant Secretary of the Army (Financial Management and Comptroller)

ASA(M&RA)
Assistant Secretary of the Army (Manpower and Reserve Affairs)

ASD(C3I)
Assistant Secretary of Defense for Command, Control, Communications, and Intelligence

CCF
Central Clearance Facility

CCTV
Closed Circuit Television

CFIUS
Counterintelligence Foreign Influence in the U.S.

CG
Commanding General

CI
Counterintelligence

CIA
Central Intelligence Agency

CINC
Commander–in–Chief

CLL
Chief of Legislative Liaison

CNWDI
Critical Nuclear Weapons Design Information

COE
Chief of Engineers

COMINT
Communications Intelligence

COMSEC
Communications Security

CONUS
Continental/Contiguous U.S.

CPO
Civilian Personnel Office

CSA
Chief of Staff, Army

DA
Department of the Army

DCI
Director of Central Intelligence

DCSLOG
Deputy Chief of Staff for Logistics

DCSOPS
Deputy Chief of Staff for Operations

DCSPER
Deputy Chief of Staff for Personnel

DEFCON
Defense Readiness Condition

DEPSECDEF
Deputy Secretary of Defense

DES
Data Encryption Standard

DIS
Defense Investigative Service

DNG
Downgrade to (used in electronic messages)

DOD
Department of Defense

DODD
Department of Defense Directive

DODI
Department of Defense Instruction

DOE
Department of Energy

DOS
Disk Operating System

DTS
Defense Transportation System

EO
Executive Order

ELINT
Electronic Intelligence

ELSEC
Electronic Security

FAA
Federal Aviation Administration

FAX
Facsimile

FMS
Foreign Military Sales

FOA
Field Operating Agency

FOIA
Freedom of Information Act

FORSCOM
U.S. Army Forces Command

FOUO
For Official Use Only

FRD
Formerly Restricted Data

GAO
General Accounting Office

GC
General Counsel

GPO
Government Printing Office

GSA
General Services Administration

JANAP
Joint Army–Navy–Air Force Publication

JCS
Joint Chiefs of Staff

JOPS
Joint Operation Planning System

JSCP
Joint Strategic Capabilities Plan

JSPDSA
Joint Strategic Planning Document Supporting Analysis

MACOM
Major Army Command

MARKS
The Modern Army Recordkeeping System

MOA
Memoranda of Agreement

MOU
Memoranda of Understanding

MSC
Major Subordinate Command

NATO
North Atlantic Treaty Organization

NCA
National Command Authority

NDP
National Disclosure Policy

NIE
National Intelligence Estimate

NSA
National Security Agency

O&M
Operation and Maintenance

OCONUS
Outside Continental U.S.

ODCSOPS
Office of the Deputy Chief of Staff for Operations

OIC
Officer in Charge

OMB
Office of Management and Budget

OPF
Official Personnel File

OPSEC
Operations Security

PA
Public Affairs

PCU
Premise Control Unit

POE
Port of Embarkation

RD
Restricted Data

RDTE
Research, Development, Test, and Evaluation

SAEDA
Subversion and Espionage Directed Against the U.S. Army

SCI
Sensitive Compartmented Information

SF
Standard Form

SIGINT
Signals Intelligence

SIGSEC
Signals Security

SNIEs
Special National Intelligence Estimates

TDA
Tables of Distribution and Allowances

TDY
Temporary Duty

TIG
The Inspector General

TJAG
The Judge Advocate General

TOE
Tables of Organization and Equipment

TRADOC
U.S. Army Training and Doctrine Command

TS
TOP SECRET

TSCO
TOP SECRET Control Officer

TSEC
Telecommunications Security

USC
United States Code

UCMJ
Uniform Code of Military Justice

USAR
U.S. Army Reserve

VCSA
Vice Chief of Staff, Army

WNRC
Washington National Records Center

Section II
Terms

Access
The ability and opportunity to obtain knowledge of classified information.

Acknowledged Special Access Programs (A–SAPs)
A SAP whose existence is known, to include association with another classified program, and which is publicly acknowledged.

Agency
An organization specified as such in EO 12958, as amended by EO 12972. The Army is an agency (an Army command is not an agency, but rather is part of an agency, the Army). Within the Department of Defense (DOD), this term includes the DOD, and the Department of the Army, the Department of the Navy, and the Department of the Air Force.

Applicable Associated Markings
Markings, other than those which designate classification level, that are required to be placed on classified documents. These include the "classified by" line, downgrading and declassification instructions, special warning notices, Special Access Program caveats, etc.

Automated Information System (AIS)
An assembly of computer hardware, software, or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information.

Automatic Declassification
The declassification of information based solely upon: (1) the occurrence of a specific date or event as determined by the original classification authority; or (2) the expiration of a maximum time frame for duration of classification established under EO 12958 (unless an exception or exemption to the automatic declassification has been authorized).

Carve–Out
A classified contract for which the Defense Security Service has been relieved of inspection responsibility in whole or in part.

Classification
The act or process by which information is determined to be classified information.

Classification Guidance
Any instruction or source that prescribes the classification of specific information.

Classification Guide
A documentary form of classification guidance issued by an original classification authority that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element.

Classified National Security Information (or "classified information")
Information and material that has been determined, pursuant to EO 12958 or any predecessor order, to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary or readable form.

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.

Code Word
A single word assigned a classified meaning by appropriate authority to ensure proper security concerning intentions and to safeguard information pertaining to actual, real–world military plans or operations classified as CONFIDENTIAL or higher.

Collateral Information
Information identified as National Security Information under the provisions of EO 12958 but which is not subject to enhanced security protection required for SAP Information.

Command
Headquarters, Department of the Army (HQDA) to include the Office of Secretary of the Army and the Army Staff, Major Commands (MACOMs), Major Subordinate commands and other organizations formed within the Army to support HQDA or a MACOM.

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.

Compilation
Items of information that are individually unclassified can be classified if the combined information reveals an additional association or relationship that matches criteria for classification pursuant to section 2–8 of this regulation.

Compromise
An unauthorized disclosure of classified information.

CONFIDENTIAL
Classification that will be applied to information in which the unauthorized disclosure could reasonably be expected to cause damage to the national security.

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 that the information or relationship, or both, are to be held in confidence.

Continental (or "Contiguous") United States (CONUS)
The 48 contiguous states in the United States territory, including adjacent territorial waters, located within the North American continent, between Canada and Mexico.

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

Controlled Unclassified Information (CUI)
Other types of information that require application of controls and protective measures, for a variety of reasons, not to include those that qualify for formal classification.

Counterintelligence (CI)
Those activities which are concerned with identifying and counteracting the threat to security (of the U.S. Army and U. S. Government to include, but not limited to, its technology or industrial base) posed by foreign intelligence services or organizations, or by individuals engaged in espionage, sabotage, sedition, subversion, or terrorism.

Critical Nuclear Weapon Design Information (CNWDI)
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, fusing, 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.

Cryptoanalysis
The analysis of encrypted messages; the steps or processes involved in converting encrypted messages into plain text without initial knowledge of the system of key employed in the encryption.

Cryptography
The branch of cryptology which treats the principles, means, and methods of designing and using cryptosystems.

Cryptology
The branch of knowledge which treats the principles of cryptography and cryptoanalytics; and the activities involved in producing signals intelligence (SIGINT) and maintaining communications security (COMSEC).

DA Personnel
Includes any active or reserve military personnel or National Guard, assigned or attached to a Department of the Army installation or activity and persons employed by, assigned to, or acting for an activity within the Department of the Army, including contractors, licensees, certificate holders, and grantees, and persons otherwise acting at the direction of such an activity.

Damage to the National Security
Harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information.

Declassification
The authorized change in the status of information from classified information to unclassified information.

Declassification Authority
An official position, in writing, not assigned to a person by name, applied to:
a. The official who authorized the original classification, if that official is still serving in the same position;
b. The originator's current successor in function;
c. A supervisory official of either; or
d. Officials delegated declassification authority in writing by the agency head (Secretary of the Army) or the senior agency official (DAMI–CH).

Declassification Guide
Written instructions issued by a declassification authority that describes the elements of information regarding a specific subject that may be declassified and the elements that must remain classified.

Derivative Classification
The process of determining whether information has already been originally classified and, if it has, ensuring that it continues to be identified as classified by marking or similar means when included in newly created material.

Document
Any physical medium in or on which information is recorded or stored, to include written or printed matter, audiovisual materials, and electromagnetic storage medium or media.

DOD
Abbreviation for the Department of Defense.

DOD Component
The Office of the Secretary of Defense (OSD), the Military Departments, the Organization of the Joint Chiefs of Staff (OJCS), the Unified Combatant Commands, and the Defense Agencies. The Army is a DOD Component.

Downgrading
A determination that information classified at a specific level will be classified at a lower level.

Entry/Exit Inspection Program (EEIP)
An inspection program to deter and detect unauthorized introduction or removal of classified material from DOD

owned or leased installations and facilities. This program did not replace existing programs for facility and installation security and law enforcement inspection requirements. This requirement has since been cancelled.

Event
An occurrence or happening that is reasonably certain to occur and which can be set as the signal for automatic declassification of information.

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.

File Series
Documentary material, regardless of its physical form or characteristics, that is arranged in accordance with a filing system or maintained as a unit because it pertains to the same function or activity.

Foreign Government Information
Information, either in soft–copy or hard–copy form, that is:

a. Government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence;

b. Information produced by the United States pursuant to or as a 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; or

c. Information received and treated as "Foreign Government Information" under the terms of a predecessor order to EO 12958.

Formerly Restricted Data (FRD)
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, this information is treated in the same manner as Restricted Data.

Hard Copy
Printed format output of a document.

Homepage (or "home page")
The single, top–level, webpage designed to be the first file accessed by a user visiting a website; also known as an "index" or "default" page.

Information
Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the United States Government. "Control" means the authority of the agency that originates information, or its successor in function, (proponent), to regulate access to the information.

Information Security (INFOSEC)
The system of policies, procedures, and requirements established under the authority of EO 12958 to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to the national security.

Infraction
Any knowing, willful, or negligent action contrary to the requirements of EO 12958 or its implementing directives that does not comprise a violation as defined below.

Integrity
The state that exists when information is unchanged from its source and has not been accidentally or intentionally modified, altered, or destroyed.

Intelligence Activity
An activity that an agency within the Intelligence Community is authorized to conduct under EO 12333.

Lost Cluster
A group of disk sectors. The operating system assigns a unique number to each cluster and then keeps track of files according to which clusters they use. Occasionally, the operating system marks a cluster as being used even though it is not assigned to any file. This is called a lost cluster.

Mandatory Declassification Review
Review for declassification of classified information in response to a request for declassification that meets the requirements under section 3.6 of EO 12958.

Material
Any product or substance on or in which information is embodied or associated.

Multiple Sources
Two or more source documents, classification guides, or a combination of both.

National Security
The national defense or foreign relations of the United States.

Need–to–Know (or "need–to–know")
A determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

Network
A system of two or more computers that can exchange data or information.

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

Operations Security (OPSEC)
The process of denying adversaries information about friendly capabilities and intentions by identifying, controlling, and protecting indicators associated with the planning and conducting of military operations and other activities.

Original Classification
An initial determination that information requires, in the interest of national security, protection against unauthorized disclosure.

Original Classification Authority (OCA)
An individual's position, which has been authorized in writing, either by the President, Secretary of the Army, or the HQDA, DCSINT, to originally classify information up to and including a certain classification level.

Permanent Historical Value
Those records that have been identified in an agency records schedule as being permanently valuable. For Army records, see AR 25–400–2, The Modern Army Recordkeeping System (MARKS).

Personal Identifier
Any grouping of letters or numbers, used in an organization code, that the command uses to identify a particular position.

Prospective Special Access Programs (P–SAPs)
An Army program or activity for which enhanced security measures have been proposed and approved to facilitate security protection prior to establishing the effort as an Army SAPs.

Protective Security Service
A transportation protective Service provided by a cleared commercial carrier qualified by the Military Traffic Management Command (MTMC) to transport shipments up to and including the SECRET classification level. The carrier must provide continuous attendance and surveillance of the shipment by qualified carrier representatives and maintain a signature and tally record. In the case of air movement, however, observation of the shipment is not required during the period it is stored in the carrier's aircraft in connection with flight, provided the shipment is loaded into a compartment that is not accessible to an unauthorized person aboard. Conversely, if the shipment is loaded into a compartment of the

aircraft that is accessible to an unauthorized person aboard, the shipment must remain under the constant surveillance of a cleared escort or qualified carrier representative.

Regrade
To raise or lower the classification assigned to an item of information.

Restricted Data (RD)
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 will not include data declassified or removed from the Restricted Data category under section 142 of the Atomic Energy Act of 1954, as amended.

Safeguarding
Measures and controls that are prescribed to protect classified information. Safeguarding and protection of classified information are synonymous terms.

SECRET
Level of classification that will be applied to information in which the unauthorized disclosure could reasonably be expected to cause serious damage to the national security.

Security Clearance
A determination that a person is eligible under the standards of AR 380–67 (implementation for DOD Directive 5200. 2–R) for access to classified information.

Security In–Depth
A determination by an authorized command official (Commander or Security Manager or other official where so designated) that a facility's security program consists of layered and complementary security controls sufficient to deter and detect unauthorized entry and movement within the facility. Examples include, but are not limited to use of perimeter fences, employee and visitor access controls, use of an Intrusion Detection System, random guard patrols throughout the facility especially during non–working hours, closed circuit video monitoring or other safeguards that mitigate the vulnerability of unalarmed storage areas and security storage cabinets during non–working hours.

Self–Inspection
The internal review and evaluation of the individual command's activities and the command as a whole (to include subordinate elements) with respect to the implementation of the Information Security Program and this regulation which implements the requirements established under EO 12958 and its implementing directives.

Senior Agency Official (or "Senior Official")
An official appointed, in writing, by the head of an agency, under the provisions of section 5.6.c of EO 12958, to be responsible for direction and administration of the Information Security Program. Within the Department of the Army, the Secretary of the Army has appointed the HQDA, Deputy Chief of Staff for Intelligence (DCSINT) as the Senior Agency Official.

Senior Official of the Intelligence Community (SOIC)
The head of an agency, office, bureau, or other intelligence element as identified in section 3 of the National Security Act of 1947, as amended, 50 USC 401a(4), and section 3.4(f) (1 through 6) of Executive Order 12333.

Sensitive But Unclassified (SBU)
Information originated within the Department of State which warrants a degree of protection and administrative control and meets the criteria for exemption from mandatory public disclosure under the Freedom of Information Act.

Sensitive Compartmented Information (SCI)
Classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of Central Intelligence.

Sensitive Compartmented Information Facility (SCIF)
A physical space which has been designated as an area containing safeguards and security interests which dictate the need for the imposition of physical protection measures, as a minimum entailing control of access to and from the

designated area, in order to protect DA interests. Functionally specialized security areas where measures applicable to each type of security area are tailored to the protection needs of the security interests contained therein.

Slack Space
Data that is located in the space, or the empty space itself, between the "End of File" marker and the end of the cluster. The DOS and Windows file systems use fixed–size clusters. DOS and older Windows systems use a 16–bit file allocation table (FAT), which results in very large cluster sizes for large partitions. Even if the actual data being stored requires less storage than the cluster size, an entire cluster is reserved for the file. Unless a file is EXACTLY one or more clusters in length, which is unlikely, there will always be space between the file's "End of File" marker and the end of the cluster associated with that file. Any data that is located in that space, or the empty space itself, is referred to as file slack.

Soft Copy
A document that is in digital format, either on an AIS or storage media.

Source Document
An existing document that contains classified information that is incorporated, paraphrased, restated, or generated in new form into a new document.

Special Access Programs (SAPs)
Any DOD program or activity (as authorized in E.0. 12958), employing enhanced security measures (e.g., safeguarding, access requirements, etc.) exceeding those normally required for information at the same level. The term "activity" is not in this section meant to be construed as organizational activity (such as a command). Policy and procedures for enhanced protection measures for that command that do not exceed beyond a command are at command discretion and are not to be confused with SAPs. See AR 380–381 for Army policy on SAPs.

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 United States is neither apparent nor acknowledged publicly; but that is not intended to influence US political processes, public opinion, policies, or media, and does not include diplomatic activities or the collection and production of intelligence or related support functions.

Systematic Declassification Review
The review process for declassification of classified information contained in records that have been determined by the Archivist of the United States ("Archivist") to have permanent historical value in accordance with chapter 33 of title 44, United States Code.

Telecommunications
The preparation, transmission, or communication of information by electronic means.

TCP/IP Network
A data communication network that uses Transport Control Protocol/Internet Protocol (TCP/IP); the public internet and the DOD Non–Classified IP Router Network (NIPRNET) are examples of TCP/IP networks.

TOP SECRET
Level of classification that will be applied to information in which the unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security.

Two–Person Integrity (TPI)
Condition by which an individual was allowed to work with TOP SECRET material as long as another cleared individual was present. In the past, because of the extreme importance to the national security of Top Secret information and information controlled within approved Special Access Programs, employees were not permitted to work alone in areas where such information is in use or stored and accessible by those employees. This requirement has since been cancelled.

Unacknowledged Special Access Programs (U–SAPs)
A SAPs, the existence of which is not acknowledged, affirmed, or made known to any person not authorized for access.

Unallocated Space
The space on a storage medium that the disk operating system (DOS) regards as available for use when needed. As far

as DOS is concerned, the space is empty. In actuality the space may contain deleted files, which are not gone until they are overwritten, or partial fragments of old files to include old file slack.

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

Upgrade
To raise the classification of an item of information from one level to a higher one.

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.

Violation
Condition by which:

a. Any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information;

b. Any knowing, willful, or negligent action to classify or continue the classification of information contrary to the requirements of EO 12958 or its implementing directives; or

c. Any knowing, willful, or negligent action to create or continue Special Access Programs contrary to the requirements of EO 12958.

Waived Special Access Programs (W–SAPs)
A SAPs for which the Secretary of Defense has waived applicable reporting requirements of section 1 19. Title 10, USC, is identified as a "Waived SAPs" and therefore has more restrictive reporting and access controls.

Webpage (or "web page")
An individual HTML–compliant electronic file accessible through a TCP/IP network.

Website (or "web site")
A collection of HTML–compliant electronic files designed to provide information, services, or goods to users through a TCP/IP network.

Section III
Special Abbreviations and Terms

This publication uses the following abbreviations, brevity codes, or acronyms not contained in AR 310–50. These include use for electronic publishing media and computer terminology.

AECS
Automated Entry Control System

AIMA
Army Intelligence Materiel Activity

AIRMP
Army Information Resources Management Program

AIS
Automated Information Systems

AQ–SAP
Acquisition SAP

AT/FP
Antiterrorism/Force Protection

B&P
Bid and Proposal

BMS
Balanced Magnetic Switch

BSMS
Billet Structure Management System

C
CONFIDENTIAL

C3I
Command, Control, Communications & Intelligence

CAPCO
Controlled Access Program Coordination Office

CCO
Handle Via COMINT Channels Only

CGI
Common Gateway Interface

CLAS
Classified by (used in electronic messages)

COMPUSEC
Computer Security

CS
Chief of Staff

CSA
Cognizant Security Agency

CSM
Command Security Manager

CSS
Constant Surveillance Service

CUI
Controlled Unclassified Information

DAMI–CH
Chief of the Counterintelligence, Human Intelligence Division

DCAA
Defense Contract Audit Agency

DCID
Director of Central Intelligence Directive

DCMC
Defense Contract Management Command

DCS
Defense Courier Service

DCSINT
Deputy Chief of Staff for Intelligence

DEA
Drug Enforcement Administration

DECL
Declassify on (used in electronic messages)

DERV
Derived from (used in electronic messages)

DISC4
Director of Information Systems for Command, Control, Communications, and Computers

DODPSP
Department of Defense Personnel Security Program

DSI
Defense Security Institute

DSS
Defense Security Service

DSSTO
Defense Security Service Training Office

DTIC
Defense Technical Information Center

EEIP
Entry/Exit Inspection Program

E–mail or e–mail
Electronic Mail

ENDEX
End of Exercise

FAT
File Allocation Table

FGI
Foreign Government Information

FIS
Foreign Intelligence Services

FISINT
Foreign Instrumentation Signals Intelligence

GILS
Government Information Locator Service

GO/SES
General Officer/Senior Executive

HQDA
Headquarters, Department of the Army

HTML
Hypertext Markup Language

HVCCO
Handle Via COMINT Channels Only

IACSE
Interagency Advisory Committee on Security Equipment

ID
Identification

IDE
Intrusion Detection Equipment

IDS
Intrusion Detection System

IMA
Intelligence Materiel Activity

IMD
Intelligence Materiel Division

INFOSEC
Information Security/Information Systems Security

IN–SAPs
Army Intelligence SAPs

IR&D
Independent Research and Development

ISCAP
Interagency Security Classification Appeals Panel

ISDN
Integrated Service Digital Network

ISOO
Information Security Oversight Office

ISPAC
Information Security Policy Advisory Council

ISS
Information Systems Security

IRR
Individual Ready Reserve

JER
Joint Ethics Regulation

JSPS
Joint Strategic Planning System

LAN
Local Area Network

LOA
Letter of Offer and Acceptance

LOU
Limited Official Use (obsolete)

MCA
Management Control Administrators

MSM
Magnetic Storage Media

NACSI
National Communications Security Instruction

NC
Not releasable to Contractors/Consultants

NDA
Nondisclosure Agreement

NFESC
Naval Facilities Engineering Service Center

NIPRNET
Non–Classified IP Router Network

NISP
National Industrial Security Program

NISPOM
National Industrial Security Program Operating Manual

NISPOMSUP
National Industrial Security Program, Operating Manual Supplement

NIST
National Institute of Standards

NOCONTRACT
Not Releasable to Contractors/Consultants

NOFORN
Not Releasable to Foreign Nationals

NRC
Nuclear Regulatory Commission

NSTS
National Secure Telephone System

NTISSC
National Telecommunications and Information Systems Security Committee

OADR
Originating Agency's Determination Required (obsolete)

OASD(C3I)
Director, Counterintelligence and Security Programs

OC
Dissemination and extraction of information controlled by originator

OCA
Original Classification Authority

ODUSD(P)
Office of the Deputy Under Secretary of Defense (Policy)

OJCS
Office of the Joint Chief Secretariat

ORCON
Dissemination and extraction of information controlled by originator

OS–SAP
Operations and Support SAP

OUSD
Office of the Under Secretary of Defense

PAED
Director, Program Analysis and Evaluation Directorate

PEO
Program Executive Office

PIN
Personal Identification Number

PR
Proprietary Information

PROPIN
Proprietary Information Involved

PSS
Protective Security Service

REL TO
Authorized for release to

S
SECRET

S&G
Sargent and Greenleaf

SA
Secretary of the Army

SAPOC
SAP Oversight Committee

SAPs
Special Access Programs

SBU
Sensitive But Unclassified

SCG
Security Classification Guide

SCI–SAP
SCI Programs SAP

SEALS
Security Equipment and Locking Systems

SECARMY
Secretary of the Army

SNM
Special Nuclear Material

SOIC
Senior Official of the Intelligence Community

SPB
Security Policy Board

SPM
Special Program Manager

SRG
Senior Review Group

SRIA
Sensitive Records and Information Agency

SSO
Special Security Office/Officer

STU
Secure Telephone Unit

TA
Traffic Analysis

TAG
The Auditor General

TCP/IP
Transport Control Protocol/Internet Protocol

TDS
Technical Data Sheet

TPI
Two–Person Integrity

TSCM
Technical Surveillance Countermeasures

U
UNCLASSIFIED

UCNI
Unclassified Controlled Nuclear Information

UN
United Nations

URL
Universal Resource Locator

USACIC
U.S. Army Criminal Investigation Command

USAINSCOM
U.S. Army Intelligence and Security Command

USASMDC
U.S. Army Space and Missile Defense Command

USD(P)
Under Secretary of Defense for Policy

USD(SP)
Under Secretary of Defense (Special Programs)

W3C
World Wide Web Consortium

WAN
Wide Area Network

Webmaster
Website Manager

WHS
Washington Headquarters Service

WNINTEL
Warning Notice – Intelligence Sources or Methods Involved (obsolete)

WWW
World Wide Web

Index

This index is organized alphabetically by topic and subtopic. Topics and Subtopics are identified by paragraph number.

USAPA

ELECTRONIC PUBLISHING SYSTEM
OneCol FORMATTER .WIN32 Version 141

PIN: 004067–000
DATE: 03- 5-01
TIME: 10:19:31
PAGES SET: 299

DATA FILE: C:\wincomp\sue.fil
DOCUMENT: AR 380–5
DOC STATUS: NEW PUBLICATION