Defense Intelligence Management Document

15 July 1993
DIAR 50-2

Information Security Program

(Encl 3)

An Open Letter to DIA Personnel:

As members of the Defense Intelligence Agency family, we are entrusted with some of the Nation's most sensitive information. Hence, we each bear an individual responsibility for maintaining that trust and for safeguarding sensitive information vital to our national security.

Each of us must be thoroughly familiar with the policies and procedures for handling classified information. Those policies and procedures historically have been contained in DIA Regulation 50-2, "Information Security Program." In a marked departure from past editions of the regulation, this current edition of DIAR 50-2 is presented as a brief regulation with an accompanying information handbook. The *Information Security Program Handbook* is comprehensive, yet concise, and written in "user friendly" style with the needs of the reader in mind.

(b)(3):10 USC 424

A copy of this regulation and handbook will be issued to every member of DIA and to each new employee. The handbook will be updated on a regular basis. Recommendations on how to improve the product are welcome, and should be forwarded to the

Each member of the Defense Intelligence Agency is responsible for being thoroughly familiar with the contents of both the regulation and the handbook, and for carrying out their provisions.

(b)(3):10 USC 424

A. DENIS CLIFT
Chief of Staff

DEFENSE INTELLIGENCE AGENCY
WASHINGTON, D.C. 20340-0001

REGULATION NO. 50-2
15 July 1993

SECURITY

Information Security

1. Purpose: To implement DoD Regulation 5200.1-R, "Information Security Program," June 1986, and the DoD Directives listed in the reference paragraph below, and to establish uniform compliance within DIA with the DoD Information Security Program.

2. References:

a. DoD Directive 5200.12, "Conduct of Classified Meetings," 27 July 1992.

b. DoD Directive 5220.22, "DoD Industrial Security Program," 8 December 1980.

c. DoD Directive 5230.9, "Clearance of DoD Information for Public Release," 2 April 1982.

d. DoD Instruction 5230.21, Protection of Classified National Security Council and Intelligence Information," 15 March 1982.

3. Applicability: This regulation and the *Information Security Program Handbook* (enclosure 1) apply to all personnel employed by, assigned to, or attached for duty to DIA; to all DIA contractors and consultants; and to all classified defense information processed, produced, used, or stored by DIA.

4. Authority: This regulation is issued under the authority delegated to the Director, Defense Intelligence Agency (DIA), in DoD Directive 5105.21 "Defense Intelligence Agency," 19 May 1977.

5. Supersession: This regulation supersedes DIAR 50-2, "Information Security Program," 27 August 1982; DIAR 50-1, "Release of Intelligence to U.S. Contractors," 24 August 1976; and DIAR 50-10, "Control of Dissemination of Intelligence of Foreign Intelligence," 11 May 1977. Because changes are extensive, they are not so indicated.

6. Policy:

a. DIA will enforce the provisions of DoD Regulation 5200.1-R and the DoD Directives listed in the reference paragraph above.

(b)(3):10 USC 424

OPR:

b. This regulation governs the Information Security Program within DIA and takes precedence over all other DIA regulations with respect to classified information.

c. The *Information Security Program Handbook* supplements this regulation and specifically sets forth security information policies and procedures within the Agency, furnishing guidance which shall be followed by each DIA member and others as cited in paragraph 3 above. The *Information Security Program Handbook* carries the force of a regulatory publication.

d. Security requirements may be modified in areas of combat or combat-related operations to accomplish the military mission.

7. Responsibilities:

a. Individuals are responsible for protecting classified information in their possession or for which they have been given custodial authority. Each individual assigned to, or attached for duty to DIA and all DIA contractors and consultants will comply with the provisions of this regulation and the *Information Security Program Handbook*. Individuals will:

(1) Surrender all classified information in their custody prior to departing DIA or transferring between DIA elements. If the information is required at the next duty assignment, it will be officially requested by and forwarded to the new element or office of assignment.

(2) Store, handle, read, discuss, display or otherwise utilize classified information only in areas and under conditions authorized to protect the information from unauthorized disclosure.

b. The Chief of Staff is the senior official responsible for the Information Security Program within DIA and will oversee and ensure DIA compliance with the Program.

(b)(3):10 USC 424

c. The Director, [redacted] will:

(1) Provide day-to-day oversight and management of the Information Security Program for DIA.

(2) Provide assistance, guidance, and training support to achieve DIA compliance with the Information Security Program.

(3) Serve as point of contact to the Information Security Oversight Office (ISOO) and report significant ISOO requirements to the Deputy Assistant Secretary of Defense (Counterintelligence and Security Countermeasures).

(4) Receive and review requests for waiver to provisions of this regulation and make recommendations to Chief of Staff.

(5) Recommend original TOP SECRET classification authorities and designate original SECRET classification authorities.

d. Senior Office Chiefs will:

(1) Ensure annual security self-inspections are conducted in their areas of responsibility.

(2) Appoint unit security officers and maintain a high state of security awareness for all personnel.

A. DENIS CLIFT
Chief of Staff

Enclosure
Information Security Program Handbook

DISTRIBUTION C, E, F, and G

INFORMATION SECURITY PROGRAM

15 JULY 1993

ENCLOSURE 1

TABLE OF CONTENTS

Page

Chapter 1, Introduction 1-1
Policy 1-1
Purpose 1-1
What the Handbook Covers 1-1
Definitions 1-2
Suggestions for Changes 1-3

Chapter 2, Classification 2-1
Policy 2-1
Classification 2-1
Original Classification Authority 2-2
Derivative Classification 2-3
Challenge to Classification 2-3
Reclassification 2-4
Security Classification Guides 2-4
Appendix A, Classification Guidelines 2-7

Chapter 3, Declassification and Downgrading Authority 3-1
Policy 3-1
Declassification and Downgrading Authority 3-1
Declassification Review 3-2
Downgrading 3-3

Chapter 4, Marking Classified Material 4-1
Policy 4-1
General Provisions 4-1
Basic Markings 4-2
Portion Markings 4-6
Special Types of Documents 4-7
Special Types of Materials 4-9
Foreign Government Information 4-11
Changes in Markings 4-12
Remarking Old Material 4-13
Appendix A, Examples of Properly Marked Classified Material 4-15
Appendix B, Intelligence Control Markings and Warning Notices 4-27
Appendix C, Foreign Government Classifications 4-31

Chapter 5, Document Control 5-1
Policy 5-1
Access 5-1

Dissemination 5-2
Accountability and Control 5-4
Reproduction of Classified Material 5-6
Transmission 5-8
Disposal and Destruction 5-12
Appendix A, Collateral Top Secret Control Program 5-15
Appendix B, Instructions Governing Use of Codewords and Nicknames 5-19
Appendix C, Hand Carrying Classified Information Outside the Washington Local Travel Area and Aboard Commercial Aircraft 5-23

Chapter 6, Storage of Classified Material 6-1
Policy 6-1
Individual Responsibilities 6-1
Storage Requirements 6-2
Combinations 6-3
Lock-Out and Repair of Containers 6-4
Opening, Closing, and Checking Security Containers 6-4
Security Container Turn-In 6-5
Vacating Secure Office Spaces 6-5

Chapter 7, Physical Security 7-1
Policy 7-1
Building Security 7-1
Alarm Systems 7-3
Security of Classified Meetings 7-5

Chapter 8, Compromise of Classified Information 8-1
Policy 8-1
Security Deficiencies 8-1
Espionage 8-3
News Items or Other Disclosures 8-3
Investigations 8-3
Classification Review 8-5
Damage Assessments 8-5
Administrative Sanctions 8-6
Reporting Unauthorized Absences 8-6
Appendix A, Sample Format of Informal Inquiry Report and Damage Assessment of Compromised Information 8-7

Chapter 9, Security Education/Briefings 9-1
Policy 9-1
Security Education Program 9-1
Initial Security Orientation 9-3
Refresher Briefings 9-4

Foreign Travel Briefings 9-4
Termination Briefings 9-5

Chapter 10, Clearance of Information for Public Release 10-1
Policy 10-1
General Guidelines 10-1
Responsibilities 10-3
Procedures 10-4
DIA Contractor Information 10-5

Chapter 11, Additional Controlled Information Systems 11-1
Policy 11-1
For Official Use Only Information 11-1
National Security Council Information 11-4

Annex A, Security/Counterintelligence Interest Areas A-1

Chapter 1

INTRODUCTION

Contents

	Page
Policy	1-1
Purpose	1-1
What the Handbook Covers	1-1
Definitions	1-2
Suggestions for Changes	1-3

Policy

- This handbook applies to all personnel employed by, assigned to, or attached for duty to DIA; to all DIA contractors and consultants; and to all classified defense information processed, produced, used, or stored by DIA.

- Each individual is responsible for protecting classified information in his/her possession and complying with the provisions of the *Information Security Program Handbook*.

Purpose

The national security of the United States is derived from many things, including its information assets. To preserve this security, the Government must protect some information from open or uncontrolled disclosure. Failure to do so can lead to damage to the national security. Executive Order 12356 defines national security as the "national defense or foreign relations of the United States."

Our national security depends on the ability of the United States to provide for the military defense of its territory, citizens, and allies and to carry on foreign relations. The technological lead time that the United States enjoys in many areas of military science enhances the national security. Our foreign intelligence capabilities help to protect against international surprise and provide for arms control verification. All of these things can be and are protected through the security classification system, and to a lesser degree, through other information control systems.

What the Handbook Covers

This handbook sets forth DIA policy for both classified and unclassified information. The term "information" means knowledge in any form including materials like printed documents,

computer media, and electronic devices. For classified information, the handbook establishes a system for classifying, downgrading, and declassifying information; sets forth policies and procedures to safeguard that information; and provides for oversight and administrative sanctions for violations.

The handbook also establishes uniform policies, criteria, and procedures for identifying and protecting unclassified information that is sensitive for reasons other than national security.

Atomic Energy Material. Nothing in this handbook supersedes any requirement related to "Restricted Data" and the Atomic Energy Act of August 30, 1954, as amended, and implementing Department of Energy directives.

Sensitive Compartmented Information (SCI) and Communication Security Information (COMSEC). SCI and COMSEC information shall be handled and controlled according to applicable national policy, DoD Directives and Instructions. Security classification and declassification policy and markings outlined in this handbook apply to SCI and COMSEC information in the same manner as other classified information.

Automated Information Systems. This handbook applies to protection of classified information processed, stored, or used in, or communicated, displayed or disseminated by Automated Information Systems (e.g., Higgins notes, AIM, SAFE, etc).

Definitions

Access. The ability and opportunity to obtain knowledge of classified information.

Original Classification Authority. The authority vested in an official of DIA to make an initial determination that information requires protection against unauthorized disclosure in the interest of national security.

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

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

Senior Office Chief. The head of a DIA office or element who is directly subordinate to the Command Element, the Chief of Staff, or a Center Director.

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

Special Access Program. Any approved program which imposes need-to-know or access controls beyond those normally required for access to CONFIDENTIAL, SECRET, or TOP SECRET information.

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

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

Suggestions for Changes

This handbook is written for DIA users of classified information. Users are encouraged to submit suggestions to improve the handbook, including format, presentation, and content. [redacted] welcomes all suggestions. When possible, key your comments to specific chapters, subsections, and pages.

(b)(3):10 USC 424

(b)(3):10 USC 424

(b)(3):10 USC 424

POC: [redacted]

Chapter 2

CLASSIFICATION

Contents

	Page
Policy	2-1
Classification	2-1
Original Classification Authority	2-2
Derivative Classification	2-3
Challenge to Classification	2-3
Reclassification	2-4
Security Classification Guides	2-4
Appendix A, Classification Guidelines	2-7

Policy

- Information will be classified only if its disclosure reasonably could be expected to cause damage to national security.

- Information will be classified TOP SECRET, SECRET, or CONFIDENTIAL; no other term, such as "sensitive," will be used with classification designations.

- DIA classifiers are responsible and accountable for the accuracy of the classifications they assign, whether by exercise of original or derivative classification authority. A higher level official through or to whom a document or other material passes for signature or approval becomes jointly responsible with the classifier for the classification assigned.

Classification

Information is classified in one of two ways: originally or derivatively. DIA uses derivative classification most frequently; original classification is rare. (See Appendix A for guidelines on classifying information.)

- **Original**--An initial determination that information requires protection against unauthorized disclosure and a determination of the level of protection required.

- **Derivative**--A determination that information is in substance the same as information that is currently classified.

Original Classification Authority

Delegations of original classification authority are limited to the minimum number required for efficient administration and to those officials whose duties involve originating and evaluating information needing classification at the level stated in the delegation of authority. When an original classification authority is absent, the person designated to act in the official's absence may exercise the classification authority.

TOP SECRET. The following officials have original classification authority for TOP SECRET and lower classifications:

Director (DR)
Deputy Director (DD)
Chief of Staff (CS)
Director for Administration (DA)
(b)(3):10 USC 424

(b)(3):10 USC 424

SECRET and CONFIDENTIAL. The Director, (b)(3):10 USC 424 will designate original SECRET and CONFIDENTIAL classification authorities. Call (b)(3):10 USC 424 for information on designated positions.

Requests for Classification Authority. Submit a memorandum request for original classification authority to Provide the organization and position title of the nominee, and a justification for the classification authority. Each request must meet the following conditions: (b)(3):10 USC 424

- Information warranting original classification is developed during normal course of operation.
- The nominee has adequate knowledge to make sound original classification determinations.
- A valid reason exists why designated original classification authorities in the nominee's chain of command cannot issue classification guidance sufficient to meet the nominee's needs.

(b)(3):10 USC 424

Training Requirements. will provide required training to classification

authorities on their responsibilities, the fundamentals of security classification, and the limitations on their authority to classify information. [redacted] will maintain records of original classification authorities who undergo training.

(b)(3):10 USC 424

Derivative Classification

Persons who insert derivative classified information in a document will:

- Respect original classification decisions.
- Verify the current level of classification as far as practicable before applying the markings.
- Carry forward to newly created documents the assigned dates or events for declassification and any additional authorized markings.

Challenge to Classification (b)(3):10 USC 424

If information is believed to be classified improperly, the challenger will contact the classifier to resolve the disagreement informally. [redacted] can provide assistance in resolving the matter. If the informal challenge to classification does not resolve the issue, the challenger may formally contest the classification by following these procedures:

- Submit a memorandum to the classifier through [redacted] (b)(3):10 USC 424
  - Give a description of the information being challenged.
  - State the reason you believe the information is improperly classified.
- Safeguard the information in question at the level of classification initially assigned.

The classifier, within 30 days of receipt of a challenge, will review the contested information and determine whether the challenge is valid. If the challenge is valid, the classifier will:

- Declassify, downgrade, or regrade the challenged information.
- (b)(3):10 USC 424 Notify the challenger, through [redacted] of the change made as a result of the challenge.
- Notify all holders of the information of the change in classification.

If the classifier determines the challenge is not valid, the classifier will give the challenger, (b)(3):10 USC 424 through [redacted] the reason(s) for denying the challenge.

Resolution of Conflicts. If DIA activities cannot agree on a classification action, refer the matter to the lowest original classification authority common to the disagreeing parties. If an agreement cannot be reached at that level, direct the matter to successively higher original classification authorities. If an agreement cannot be reached at the highest level of the disagreeing parties, refer the matter to the Chief of Staff through [redacted] will evaluate and refer, as appropriate, disagreements between DIA and other DoD Components. Suspense for these actions is 30 days. (b)(3):10 USC 424

No adverse action may be taken against an employee or military member of DIA for challenging a classification determination.

Reclassification

Only the Secretary of Defense may reclassify DIA information that has been declassified and disclosed. Send requests for reclassification to [redacted] (b)(3):10 USC 424

Security Classification Guides

Officials responsible for a DIA classified system, program, plan, project, or special access program (SAP) will issue a security classification guide before the initial funding or implementation of the system, program, plan, project, or SAP. [redacted] will provide security policy guidance and assistance and serve as the central point of contact on all administrative matters involving classification guides. (b)(3):10 USC 424

Each security classification guide must be approved, in writing, by the Chief of Staff or the DIA official who has program or supervisory responsibility over the information and who has original classification authority at the level required for the security guide.

DoD Handbook 5200.1-H, "DoD Handbook for Writing Security Classification Guidance," gives specific instructions on writing and formatting security classification guides. Contact [redacted] for further assistance. (b)(3):10 USC 424

Distribution of Security Classification Guides. Forward five copies of each approved collateral classification guide and each approved change to [redacted] will retain one copy and distribute, as appropriate, to the following officials: (b)(3):10 USC 424

- Director of Freedom of Information and Security Review (OASD(PA)), 1 copy.
- Director of Information Systems Security, DASD(CI&SCM), 1 copy.
- Administrator, Defense Technical Information Center, Defense Logistics Agency, 2 copies.

If the classification guide is classified TOP SECRET or is determined by the approval authority to be too sensitive for automatic secondary distribution to DoD Components, the

(b)(3):10 USC 424

originator will report the existence of the guide to the Director of Information Systems Security, DASD(CI&SCM), through [redacted] The report will include the classification guide title, its approval date, its classification level, and the identification of the originating activity. DASD(CI&SCM) will maintain a separate classified list of such classification guides.

Periodic Review of Security Classification Guides. The originator will issue changes as needed and will review classification guides not less than every 2 years for currency of information. [redacted] will notify the originator of the dates and requirements for review.

(b)(3):10 USC 424

Index of Security Classification Guides. Each security classification guide originator will prepare DD Form 2024 (DoD Security Classification Guide Data Elements) when the guide is approved, changed, revised, reissued, or canceled, and during each biennial review. The original and three copies of the form will be forwarded to [redacted] for referral to DASD(CI&SCM).

(b)(3):10 USC 424

(b)(3):10 USC 424 **POC:** [redacted]

Chapter 2

Appendix A

CLASSIFICATION GUIDELINES

Information will be classified only if its disclosure reasonably could be expected to cause damage to the national security. You may use only one of three designations to classify information or material requiring protection in the interest of national security: TOP SECRET, SECRET, or CONFIDENTIAL. The markings FOR OFFICIAL USE ONLY and LIMITED OFFICIAL USE will not be used to identify classified information. (See chapter 11 for use of these terms.) No other term, such as "sensitive," may be used with classification designations.

Classification Planning

Classification planning is an essential part of developing a plan, operation, program, or procurement action involving classified information. Consider classification from the outset to ensure adequate protection of the information and to eliminate impediments to the execution or implementation of the activity.

DIA officials responsible for developing plans, programs, or projects in which classification is a significant factor must develop a classification guide.

Classification Criteria

Original classification authorities must make two decisions in determining whether to classify information: Does the information fit one of the categories identified in E.O. 12356 (listed below)? Could its unauthorized disclosure reasonably be expected to cause damage to national security? The first decision is separate and distinct from the second decision.

Consider information for classification if it concerns:

- Military plans, weapons, or operations.
- Vulnerabilities or capabilities of systems, installations, projects, or plans relating to national security.
- Foreign government information.
- Intelligence activities including special activities or intelligence sources or methods.
- Foreign relations or foreign activities of the United States.

- Scientific, technological, or economic matters relating to the national security.
- U.S. Government programs for safeguarding nuclear materials or facilities.
- Cryptology.
- A confidential source.
- Other categories of information related to national security that require protection against disclosure as determined by the Secretary of Defense.

Forward recommendations for additional categories of information for classification through the Director For to (b)(3):10 USC 424

Presumption of Damage. Unauthorized disclosure of foreign government information, the identity of a confidential foreign source, or intelligence sources and methods is presumed to cause damage to national security.

Classification Designations

TOP SECRET. Identifies information or material which, if disclosed, reasonably could be expected to cause *exceptionally grave damage* to national security. Examples include:

- Armed hostilities against the United States or its allies.
- Disruption of foreign relations vitally affecting the national security.
- Compromise of vital national defense plans or complex cryptologic and communications intelligence systems.
- Revelation of sensitive intelligence operations.
- Disclosure of scientific or technological developments vital to national security.

SECRET. Identifies information or material which, if disclosed, reasonably could be expected to cause *serious damage* to national security. Examples include:

- Disruption of foreign relations significantly affecting national security.
- Significant impairment of a program or policy directly related to national security.
- Revelation of significant military plans or intelligence operations.
- Compromise of significant military plans or intelligence operations.

- Compromise of significant scientific or technological developments relating to national security.

CONFIDENTIAL. Identifies information or material which, if disclosed, could be expected to cause *damage* to the national security. Examples include:

- Compromise of information that indicates strength of ground, air, and naval forces in the United States and overseas.

- Disclosure of technical information used for training, maintenance, and inspection of classified munitions of war.

- Revelation of performance characteristics, test data, design, and production data on munitions of war.

Duration of Original Classification

When a DIA original classification authority determines information should be classified, the authority will set a date or event, consistent with national security, for declassification. If a date or event cannot be determined, the notation "Originating Agency's Determination Required" (OADR) will be used.

Limitations on Classification

Classification cannot be used to limit dissemination of information that is not classifiable under E.O. 12356.

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

References to classified documents may not be classified unless the reference citation, standing alone, reveals classified information.

Basic scientific research information not clearly related to national security may not be classified, except information that meets the definition of RESTRICTED DATA. (RESTRICTED DATA concerns design, manufacture, or utilization of atomic weapons; the production of special nuclear material; or the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the RESTRICTED DATA category under section 142 of DoD 5220.22-M, "Industrial Security Manual for Safeguarding Classified Information.")

Classifying Material Other Than Documents

Classify equipment and other physical objects only if classified information may be derived by visual observation of their structure or by their operation, test, application, or use.

When the mere knowledge that an object exists would compromise national security advantage, the fact that it exists requires classification.

Compilation of Information

Classify a compilation of unclassified items if the compilation provides an added factor that warrants classification. Only an original classification authority may classify a compilation of unclassified information. A written explanation must accompany all classified compilations.

(b)(3):10 USC 424

POC: [redacted]

Chapter 3

DECLASSIFICATION AND DOWNGRADING AUTHORITY

Contents

	Page
Policy	3-1
Declassification and Downgrading Authority	3-1
Declassification Review	3-2
Downgrading	3-3

Policy

- Information will be declassified or downgraded as soon as national security considerations permit.

- Declassification will be coordinated with other DIA elements, DoD Components, and U.S. Government departments or agencies having a direct interest in the subject matter.

- DIA will not declassify or downgrade information originated and classified by another agency without permission of the originating agency.

Declassification and Downgrading Authority

The following officials are authorized to declassify and downgrade DIA classified information:

- The official or successor identified on the "Classified by" line of the document.

- The DIA original classification authority for the element which produced the information, if no classification authority is indicated.

- The original classification authority for the element which has assumed functional interest.

- The supervisor of any of the above officials.

Base declassification decisions on loss of sensitivity of the information with the passage of time or the occurrence of an event that permits declassification.

Declassification Review

U.S. citizens, permanent resident aliens, Federal agencies, and State or local governments may request a mandatory declassification review of DIA information. The originating or responsible DIA activity will conduct the declassification review.

Internal DIA Requests. Submit requests concerning DIA material to Public Liaison (PSL-P), which will forward the requests to the DIA element that originally classified the information or which has cognizance over the subject matter. For non-DIA material, submit the requests through PSL-P to the original classifying agency or the agency most concerned with the subject matter.

Freedom of Information Act/Privacy Act (FOIA/PA). No DIA element in possession of a document will, in response to a request under the Freedom of Information Act, refuse to confirm the existence or nonexistence of a document, unless the fact of its existence is classifiable under this handbook. DIAR 12-39, "Freedom of Information Act Program," provides procedures for processing FOIA/PA requests for mandatory review of DIA classified information. PSL-P can provide assistance in responding to FOIA/PA requests.

Foreign Government and North Atlantic Treaty Organization Information. When foreign government information is involved in a declassification review, consult the Foreign Liaison Staff (PSL-F) and the Defense HUMINT Directorate (CH) before taking final action. When NATO information is involved, contact [redacted] (b)(3):10 USC 424

Information Security Oversight Office (ISOO). If the Director of the ISOO determines information is classified in violation of E.O. 12356, DIA may be required to reclassify or declassify the information. Such requirement may be appealed; contact [redacted] for appeal procedures. (b)(3):10 USC 424

RESTRICTED DATA and FORMERLY RESTRICTED DATA. Coordinate action on these requests, including requests from Presidential libraries, with the Department of Energy.

Transfer for Storage or Retirement. Review classified documents for downgrading or declassification before they are forwarded to [redacted] for storage or to the National Archives and Records Administration (NARA) for permanent preservation. (b)(3):10 USC 424

Classified Information Officially Transferred. When classified information is transferred to DIA in conjunction with a transfer of functions from a DoD agency or component, the receiving DIA activity becomes the original classification authority for downgrading and declassification.

Classified Information Not Officially Transferred. DIA activities become the downgrading and declassification authority for information they possess that originated in an agency outside the DoD that no longer exists if:

- Such information has not been transferred to another agency or department in conjunction with a transfer of functions.

- It is impossible to identify the originating agency.

Downgrading

Automatic Downgrading. Classified information marked for automatic downgrading in accordance with this or prior DIA/DoD regulations or Executive Orders may be downgraded accordingly without notification to holders. See Chapter 4 for downgrade markings.

Downgrading Upon Reconsideration. Classified information not marked for automatic downgrading may be assigned a lower classification designation by an authorized official. Provide prompt notice of such downgrading to known holders of the classified information.

(b)(3):10 USC 424

POCs:

Chapter 4

MARKING CLASSIFIED MATERIAL

Contents

	Page
Policy	4-1
General Provisions	4-1
Basic Markings	4-2
Portion Marking	4-6
Special Types of Documents	4-7
Special Types of Materials	4-9
Foreign Government Information/Documents	4-11
Changes in Markings	4-12
Remarking Old Material	4-13
Appendix A, Examples of Properly Marked Classified Material	4-15
Appendix B, Intelligence Control Markings	4-27
Appendix C, Foreign Government Classifications	4-31

Policy

- Classified material will be identified and marked in a conspicuous manner.
- Original and derivative classifiers are responsible for designating and marking classified information.
- The holder of an improperly marked classified document will contact the document originator to obtain correct markings.

General Provisions

Classified information must be clearly identified. Marking is the principal means of telling holders of classified information about specific protection requirements for that information. Markings serve to:

- Alert holders to the presence of classified information.
- Identify, as specifically as possible, the exact information needing protection.

- Indicate the level of classification assigned to the information.
- Provide guidance on downgrading (if any) and declassification.
- Give information on the source of classification of the information.
- Warn holders of special access, control, or safeguarding requirements.

Exception. Do not apply classification or other security markings to an article or portion of an article appearing in a newspaper, magazine, or other public medium. If an article is reviewed for classified information, keep the results of the review separate from the article.

Basic Markings

Marking requirements vary according to the materials involved. (See figure 1 for a listing of the most common markings used in DIA.) The basic requirements common to all classified material are as follows:

- The overall classification of the document. Mark the overall classification at the top and bottom on the face of the front cover (if any), on the title page (if any), on the first page, and on the outside back cover or the last page. If the last page is used for marking, the page must not contain classified information.

The overall classification marking must be conspicuous enough to alert anyone handling the document that it is classified. If the marking does not attract your attention, it is not conspicuous. Overall classification markings must be **larger** and **bolder** than other text on the page.

- The agency and office of origin.
- The identity of the classification authority.
  - Show original classification authority by position title; for example, "Classified by:
  - Show derivative classification authority if the information comes from a source already classified.
  - Use "multiple sources" if the classification is derived from more than one source. *A listing of the sources must be kept with the record copy of the document.*

(b)(3):10 USC 424

CLASSIFICATIONS, CONTROL MARKINGS, AND WARNING NOTICES	COVER PAGE, TITLE PAGE, OUTSIDE OF BACK COVER OR FIRST PAGE IF NO COVER	PAGE MARKING	SUBJECT, TITLE, PARAGRAPH, SUBPARAGRAPH MARKING
TOP SECRET	TOP SECRET	TOP SECRET	(TS)
SECRET	SECRET	SECRET	(S)
CONFIDENTIAL	CONFIDENTIAL	CONFIDENTIAL	(C)
FOR OFFICIAL USE ONLY	FOR OFFICIAL USE ONLY	FOR OFFICIAL USE ONLY	(FOUO)
Not Releasable to Foreign Nationals	Not Releasable to Foreign Nationals	NOFORN	(NF)
Warning Notice—Intelligence Sources or Methods Involved	Warning Notice—Intelligence Sources or Methods Involved	WNINTEL	(WN)
Not Releasable to Contractors/Consultants	Not Releasable to Contractors/ Consultants	NOCONTRACT	(NC)
Dissemination and Extraction of Information Controlled by Originator	Dissemination and Extraction of Information Controlled by Originator	ORCON	(OC)
Caution—Proprietary Information Involved	Caution—Proprietary Information Involved	PROPIN	(PR)
Authorized for Release to [name of country]	Authorized for Release to [name of country]	REL [country abbr.]	(REL...)
RESTRICTED DATA	RESTRICTED DATA	RESTRICTED DATA	(RD)
Formerly Restricted Data (If a document also contains RESTRICTED DATA, use the RESTRICTED DATA marking.)	Unauthorized disclosure subject to administrative and criminal sanctions. Handle as Restricted Data in foreign dissemination. Section 144.b, Atomic Energy Act, 1954.	FORMERLY RESTRICTED DATA	(FRD)

Figure 1. Intelligence control markings and warning notices.

CLASSIFICATIONS, CONTROL MARKINGS, AND WARNING NOTICES	COVER PAGE, TITLE PAGE, OUTSIDE OF BACK COVER OR FIRST PAGE IF NO COVER	PAGE MARKING	SUBJECT, TITLE, PARAGRAPH, SUBPARAGRAPH MARKING
Critical Nuclear Weapon Design Information	Critical Nuclear Weapon Design Information--DoD Directive 5210.2 applies.	CNWDI	(N)
Communications Security (COMSEC)	COMSEC Material--Access by Contractor Personnel Restricted to U.S. Citizens Holding Final Government Clearance.	n/a	n/a
Foreign Government Documents	Mark only the cover with the equivalent overall U.S. classification.	FGI	(Country/Class.)
Foreign Government Document classified as RESTRICTED	Mark only the cover with the notation: "This classified material is to be safeguarded in accordance with paragraph 11-302b, DoD 5200.1-R."	n/a	n/a
Foreign Government Information in DIA Documents	FOREIGN GOVERNMENT INFORMATION	N/A	(Country/Class.)
Foreign Government RESTRICTED Information used with DIA Unclassified Information	Mark document CONFIDENTIAL.	n/a	(Country/Class.) and (U), as appropriate
NATO Document	Mark cover of document with the classification in English.	n/a	n/a
NATO Information in DIA Documents	This document contains NATO Classified Information.	n/a	(NATO/Class.)
NATO RESTRICTED information in DIA unclassified documents.	This document contains NATO Restricted information and shall be safeguarded as FOR OFFICIAL USE ONLY information.	This page contains NATO RESTRICTED information.	n/a

Figure 1. Continued.

CLASSIFICATIONS, CONTROL MARKINGS, AND WARNING NOTICES	COVER PAGE, TITLE PAGE, OUTSIDE OF BACK COVER OR FIRST PAGE IF NO COVER	PAGE MARKING	SUBJECT, TITLE, PARAGRAPH, SUBPARAGRAPH MARKING
Special Dissemination or Reproduction Notice	"Reproduction requires approval of originator or higher DoD Authority" or "Further dissemination only as directed by (insert appropriate office or official or higher DoD authority)."	n/a	n/a

Figure 1. Continued.

- The date or event for automatic declassification or the notation "Originating Agency's Determination Required" (OADR). This information will not be applied to documents containing RESTRICTED DATA or FORMERLY RESTRICTED DATA, which normally is not declassified.

- Any downgrading action to be taken and the date or event for the action, if applicable. Place this on the face of the document. If "multiple sources" is used, use the most remote date or event.

- Intelligence control markings. Place the markings once at the top or bottom on the front cover (in the abbreviated form) and on the title page (spelled out). In correspondence, spell out the markings on the first page.

- Warning notices and other special markings that apply to the document.

Portion Marking

Portion marking eliminates any doubt as to which portions of a document contain or reveal classified information. Mark each page, section, paragraph, subparagraph, enclosures, or similar portion of a classified document to show the classification level of its contents and its association with other information. See Appendix A for samples of properly marked documents and material.

Page.

- Mark each interior page at the top and bottom with the highest classification of the information on the page, including "UNCLASSIFIED" on pages containing no classified information. Alternatively, mark each page with the overall classification of the document to achieve production efficiency.

- Include intelligence control markings and warning notices at the top or bottom of each page on which the markings are used. The preferred order for listing intelligence control markings is NOFORN/WNINTEL/NOCONTRACT/ORCON/PROPIN/REL.

Subject and Title. Mark subjects and titles with a parenthetical marking such as (TS), (S), (C), but place the marking *after* the subject or title.

Paragraph, Section, and Part.

- Place the appropriate classification symbol before the beginning of the portion or immediately following the portion's letter or number.

- Use appropriate abbreviations for intelligence control markings and warning notices. For example, (S/NF) for SECRET information not releasable to foreign nationals. The preferred order for listing intelligence control markings is NF/WN/NC/OC/PR/REL.

(See Appendix B for explanations of intelligence control markings and warning notices.)

Special Categories. Mark illustrations, photographs, figures, graphs, drawings, charts, and similar portions of classified documents to show the classification or unclassified status. Spell out the markings and place them within or adjacent to the applicable portion. Mark captions and titles as required for text portions; the marking will indicate the classification of the caption or title, not of the chart itself. (See Appendix A for examples.)

If parenthetical portion marking is impractical, the face of that document will contain a statement that clearly identifies the information that is classified and the level of classification.

Requests for Waivers. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) (ASD(C^3I)) is the authority for granting waivers to portion marking requirements. Submit requests to (ASD(C^3I)) through [redacted] (b)(3):10 USC 424

Special Types of Documents

Documents with Component Parts. If a classified document has components likely to be removed and used separately, mark each component as a separate document. Examples include annexes or appendices, major parts of a report, reference charts, and enclosures.

If the entire major component is unclassified, mark UNCLASSIFIED on its face, top and bottom, and add the statement: "All portions of this [annex, appendix] are Unclassified."

Transmittal Documents. Transmittal documents are documents that have classified enclosures or attachments. An example is a letter with classified enclosures. Mark transmittal documents as follows:

- If the transmittal document contains classified information as high or higher than the documents being transmitted, mark it as you would any other classified document. Add to the face of the transmittal document any special warning notices in the documents being transmitted.

- If the information in the transmittal document is unclassified or classified at a lower level than one or more of the enclosures:

  - Mark the face of the transmittal document conspicuously, top and bottom, with the highest classification of the documents being transmitted. Example: An unclassified transmittal document has one Secret and two Confidential enclosures. Mark the face of the transmittal document SECRET.

  - Mark the face of the transmittal document to show its status when separated from the classified material. Examples: "UNCLASSIFIED WHEN SEPARATED

FROM CLASSIFIED ENCLOSURES," "UNCLASSIFIED WHEN ENCLOSURE 2 IS REMOVED," "CONFIDENTIAL UPON REMOVAL OF ENCLOSURES."

- Do not portion-mark unclassified transmittal documents, or mark interior pages of an unclassified transmittal document.

Documents Classified by Compilation. Mark the overall classification at the top and bottom of each page and the outside of the front and back covers (if any). Include an explanation of the basis for classification by compilation on the face of the document or in the text.

Special Access Program Documents. Additional markings are required for these documents. Such markings, however, will not serve as the sole basis for continuing the classification; when appropriate, such markings will be removed to ease timely declassification, downgrading, or removal of the material from special control procedures. (See DIAM 56-3, "Special Access Program Procedures Manual.")

Translations. When U.S. classified information is translated into another language, mark the information to show the United States as the country of origin, the appropriate U.S. classification markings, and the foreign language equivalent thereof.

Electronically Transmitted Data.

GENSER and SPINTCOMM Messages. Mark classified messages at the top and bottom with the overall classification and portion-mark as for other documents. The overall classification, spelled out, is the first item of information in the text of the message. The warning notices RESTRICTED DATA, FORMERLY RESTRICTED DATA, and CRITICAL NUCLEAR WEAPONS DESIGN INFORMATION and intelligence control markings are inserted immediately after the classification marking. (For detailed information on message preparation, see "Message Management and Preparation Handbook," 15 June 1990.)

Electronic Mail. Marking requirements for information transmitted via electronic mail are the same as any other classified information. Ensure both the electronic message and the enclosures carry appropriate classification, downgrading, and control markings. Anyone reducing electronic mail to hardcopy is responsible for ensuring the information is properly marked and controlled.

Facsimile Transmission. Documents transmitted by facsimile require the same markings as other classified material. No additional markings are required.

Documents for Training Purposes. Unclassified documents and material for training purposes must clearly show that they are unclassified. Place on each page of the document a marking such as "Classified for Training Only" or "Unclassified Sample."

Special Types of Material

Classified information contained in automated information system products and media, audiovisual media, hardware and equipment, or other media not commonly thought of as documents must be marked to meet the purposes of the *General Provisions* paragraph at the beginning of this chapter. The main concern is that holders and users of the material are clearly warned of the presence of classified information. Portion marking of these items is normally not practical and is not required.

Charts, Maps, and Drawings. Charts, maps, drawings, blueprints, engineer's drawings, and similar items *not contained in a classified document* are marked as follows:

- Apply the overall classification (spelled out) at the top and bottom, if possible.
- Mark the legend or title to show its classification.
- Place the classification markings so they will be visible if the chart or other item is rolled or folded.

Photographs, Negatives, and Unprocessed Film. Photographs and negatives must be marked with the overall classification of information they contain. Mark photographs on the face. If this cannot be done, place the classification marking and other control markings on the reverse side.

Mark negatives and unprocessed film containing classified information with their overall classification. Place the marking on the film itself or on the canister, if one is used. If placed on the film, place the marking at the beginning and the end of the roll.

Slides and Transparencies. Show the classification and control markings in the image area, if possible, and on the border, holder, or frame. If the classification is not shown in the image area, the individual displaying the transparency is responsible for notifying viewers of the classification and warning notices.

Motion Picture Films and Videotapes. Include classification and any appropriate security warning notices at the beginning and end of the played or projected portion. Place other required security markings at the beginning of the played or projected portion. Mark reels, cassettes, and containers with the overall classification.

Recordings. Include a statement at the beginning and the end of sound, magnetic or electronic recordings that will ensure listeners or viewers will know that classified information is involved. Mark reels, cassettes, and containers with the overall classification and associated markings.

Microforms. Mark microfilm, microfiche, and similar media with their overall classification in the image area; apply the marking so it is visible to the unaided eye. Include other required security markings on the item or include them in accompanying documentation.

Removable ADP and Word Processing Storage Media. Removable storage media include magnetic tape reels, disk packs, floppy diskettes of various sizes, removable hard disks, disk cartridges, optical disks, paper tape reels, magnetic cards, tape cassettes and microcassettes, and any other device on which data is stored and which normally is removable from the system by the user or operator. Mark ADP storage media and equipment with the highest classification level and warning notices of information ever contained thereon. Use the following labels as appropriate:

- SF 706 - TOP SECRET
- SF 707 - SECRET
- SF 708 - CONFIDENTIAL
- SF 709 - CLASSIFIED
- SF 710 - UNCLASSIFIED
- SF 711 - DATA DESCRIPTOR
- SF 712 - CLASSIFIED SCI

An SF 711 is required on each medium. When SF 709 and SF 712 labels are used, enter the appropriate security classification and compartment/codeword designators on the SF 711.

Documents Produced by ADP Equipment. The provisions of this paragraph do not apply to documents produced by automated information systems which function as word processing systems. The provisions for protecting information produced on ADP equipment are:

- Mark all interior pages of fan-folded printouts with the overall classification. The equipment may apply these markings even though they may not meet the normal test of being conspicuous.
- Show on the cover (or the first page if there is no cover) special warning notices, classification source, and downgrading and declassification instructions. Alternatively, place the information on a separate "Notice of Declassification Instructions and Other Associated Markings" attached to the front of the printout.
- Treat parts of printouts removed for separate use or maintenance as individual documents.

Foreign Government Information

Except for the foreign classification "RESTRICTED," foreign classification designations, including NATO, generally parallel U.S. classification designations. Appendix C contains a table of equivalent classification designations.

Marking NATO Documents. Classified documents *originated* by NATO, if not already marked, must be marked with the classification in English. Downgrading and declassification markings will not be placed on documents originated by NATO.

Marking NATO Information in DIA Documents. Page markings are not required. Paragraphs, however, must be marked with the foreign classification marking, for example, "(NATO-S)." Mark the cover or, in absence of a cover, the first page with the following notation: "This document contains NATO classified information."

When NATO RESTRICTED information is included in U.S. unclassified documents, place the following statement on the front: "This document contains NATO Restricted information and shall be safeguarded as FOR OFFICIAL USE ONLY information." Mark each page containing NATO RESTRICTED information with "This page contains NATO RESTRICTED information."

Marking Foreign Government Documents. If the foreign classification designation is not shown in English, mark the document with the equivalent overall U.S. classification designation. Do not apply any additional markings. If the document is marked with any of the markings in the last column of Appendix C, an English classification is not required.

Some foreign governments use a fourth classification. Such designations are or equate to the foreign classification RESTRICTED. If documents are marked with any of these classification designations, mark the face of the documents with the notation, "This classified material is to be safeguarded in accordance with paragraph 11-302b, DoD 5200.1-R."

Foreign documents containing foreign government information not classified by the foreign government, but provided to DIA in confidence, will be classified by an original classification authority and marked with the appropriate U.S. classification.

Other marking requirements prescribed by this regulation for U.S. classified documents are not applicable to foreign government documents.

Marking Foreign Government Information in DIA Documents. Foreign government information (FGI) must be marked to prevent premature declassification or unauthorized access by third country nationals. Place the notation **FOREIGN GOVERNMENT INFORMATION** on the face of all documents containing FGI. Mark all portions with the specific source and classification, for example, (UK-C). If identifying the information as FGI would compromise a confidential source or relationship, disregard the FGI marking requirements and mark only the portions with the classification.

When foreign RESTRICTED information is included in an otherwise unclassified DIA document, the DIA document will be marked CONFIDENTIAL. Portion markings such as "(UK-R)" and "(U)" will be applied. In addition, all marking requirements of this chapter apply.

Changes in Markings

Downgrading or Declassifying in Accordance with Markings. A document or material may be downgraded or declassified on the date or event indicated on the face of the document or material. There is no requirement to refer the material to the originator for a decision. If the holder of the material has reason to believe it should not be downgraded or declassified, notify the classifier through

(b)(3):10 USC 424

When a document is *declassified* in accordance with the declassification markings appearing on it, cancel the overall and page markings on the document. If canceling each page is not practical, cancel at least the markings on the cover, title page, and the first page.

If a document is *downgraded* in accordance with its markings, cancel the old classification markings and substitute the new ones. As a minimum, change the markings on the cover, title page, and the first page.

Downgrading and Declassifying Earlier than Scheduled. If a document is declassified or downgraded earlier than indicated by its markings, follow these procedures:

- Cancel the overall and page markings on the document. If canceling each page is not practical, cancel at least the markings on the cover, title page, and the first page.
- Indicate the date of the downgrading or declassification.
- Show the authority for the action (that is, the identify of the original classifier who directed the action, or the identification of the correspondence or classification instruction which required it).
- Identify the name of the person doing the remarking.

Upgrading and Extending Classifications. If a document is upgraded, change all classification markings affected by the upgrading. If classification is extended beyond the date or event indicated on the document, cancel the declassification markings and add the new ones. In both cases, place the following information on the document:

- The date of the remarking.
- The authority for the action (that is, the identity of the original classifier who directed the action, or identification of the correspondence or classification instruction which required it).

· The name of the person doing the remarking.

Marking Bulk Quantities of Material. When the volume of material is such that prompt remarking of each classified item would interfere with operations, attach downgrading and declassification notices to the storage unit. Each notice will specify the authority for the downgrading or declassification action, the date of the action, and the storage unit to which it applies. When individual documents or materials are permanently withdrawn from storage units, remark at the time of removal as prescribed in above paragraphs.

Remarking Old Material

There is no need to remark material marked in accordance with Executive Order 12065 and earlier orders. If the material has automatic downgrading and declassification instructions, honor them. If the material does not have instructions, treat the material as if it were marked "Originating Agency's Determination Required."

(b)(3):10 USC 424

POC: [redacted]

Chapter 4

Appendix A

EXAMPLES OF PROPERLY MARKED CLASSIFIED MATERIAL

Contents

	Page
Portion and Overall Classification Marking	4-16
Transmittal Letters	4-17
Derivative Classification Marking	4-18
Illustrations in Classified Documents	4-19
Charts, Maps, and Drawings Classified as Separate Documents	4-20
Transparencies and Slides	4-21
Photographs	4-21
ADP Storage Media	4-22
Foreign Government Information in a DIA Document	4-23
Restricted Data, Formerly Restricted Data and CNWDI	4-24
Downgrading Instructions	4-25

SECRET

(unclassified sample)

(b)(3):10 USC 424

S-0000

TO: Director
National Security Agency
Fort George G. Meade, Maryland
20755

SUBJECT: Portion Marking (U)

1. (U) This is a sample of a letter with multiple parts. In this sample, paragraph one in its totality contains "Secret" information, but the lines of the opening portion do not. Therefore, this portion will be marked with the designation "U" in parentheses.

a. (S) This subparagraph contains information classified SECRET as indicated by the "S" portion marking.

(1) (C) The text in this subparagraph contains information classified CONFIDENTIAL.

SECRET

SECRET

(2) (U) This part of the sample document is unclassified.

b. (S) The text in this subparagraph contains information that is classified SECRET.

2. (U) This part contains no classified information.

a. When a paragraph and all its subparagraphs are unclassified, there is no need to portion mark the subparagraphs.

b. This subparagraph is also unclassified.

FOR THE DIRECTOR:

(Official's name and title)

Classified By: DIA/

(b)(3):10 USC 424

Declassify On: 12 Jan 92

2

SECRET

Portion and overall classification markings.

SECRET

(unclassified sample)

S-

_____
_____
_____
_____

Dear Sir:

_____
_____.
_____
_____.

(Official's name and title)

2 Enclosures
1. xxxxxxxxxxxx (S)

2. xxxxxxxxxxxx (C)

Unclassified when separated
from Classified enclosures

SECRET

Transmittal letters.

SECRET

(unclassified sample)

S-
TO: _____
_____
_____

SUBJECT:_____ (U)
1. (C) _____
_____.

2. (U) _____
_____.

(Official's name and title)

2 Enclosures
1. xxxxxxxxxxxx (S)
2. xxxxxxxxxxxx (C)

Classified By: Multiple Sources
Declassify On: OADR

Downgrade to CONFIDENTIAL when
separated from SECRET enclosure.

SECRET

SECRET

(unclassified sample)

Source 1

Classified By: DIA

(b)(3):10 USC 424

SECRET

SECRET

(unclassified sample)

Source 2

Classified By: CG-DNES-1

SECRET

SECRET

(unclassified sample)

Derivative

Classified By: Multiple Sources

SECRET

SECRET

(unclassified sample)

Read File Copy

Classified By: Multiple Sources

Source 1: DIA Memo, S-0000, 2 Jan 92

Source 2: Classification Guide DNES-1, 12 Oct 88

(b)(3):10 USC 424

SECRET

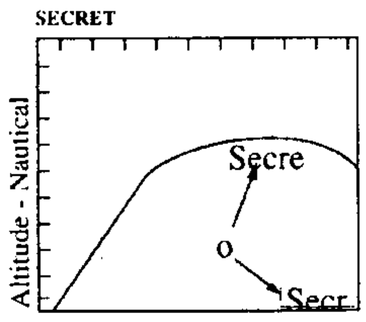
Derivative classification marking.

SECRET
(unclassified sample)

3. (C) _____.

_____.

a. (U) _____.



Range - Nautical Miles
Chart No. 2 (U) Test Results

b. (U)_____.

4. (U) _____.

FOR THE DIRECTOR:

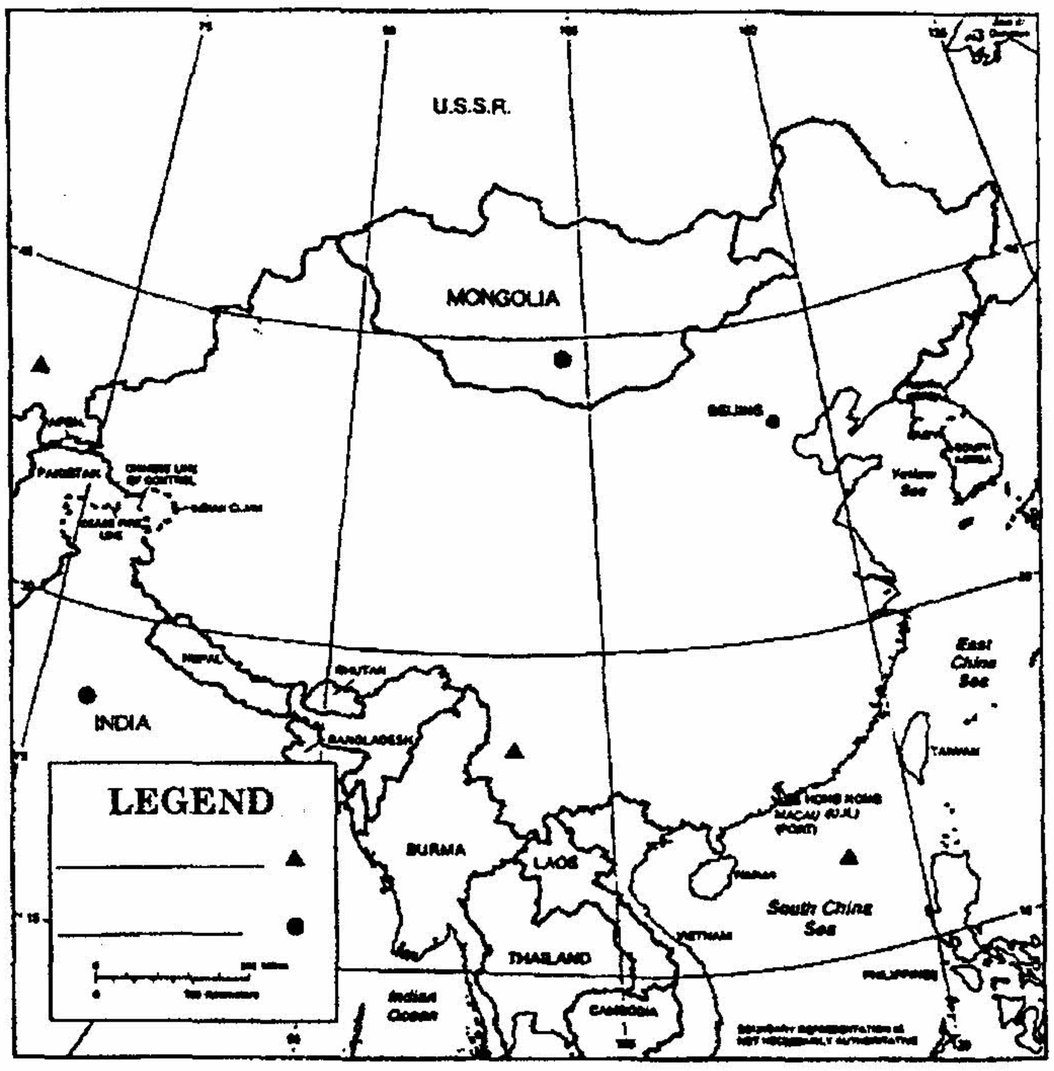
SECRET

Illustrations in classified documents.

SECRET

(unclassified sample)

Title _____ (U)

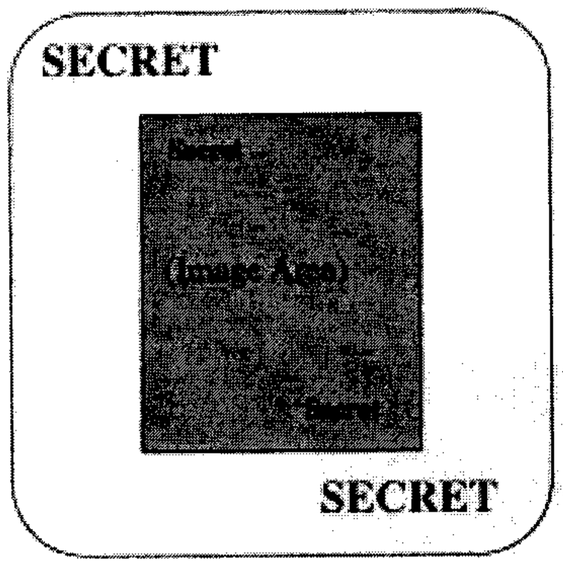


Title and Legend are unclassified

Classified By: DIA [redacted] (b)(3):10 USC 424
Declassify On: OADR

SECRET

Charts, maps, and drawings classified as separate documents.



Transparencies and slides.

SECRET

(FRONT OF PHOTOGRAPH)

SECRET

SECRET

(BACK OF PHOTOGRAPH)

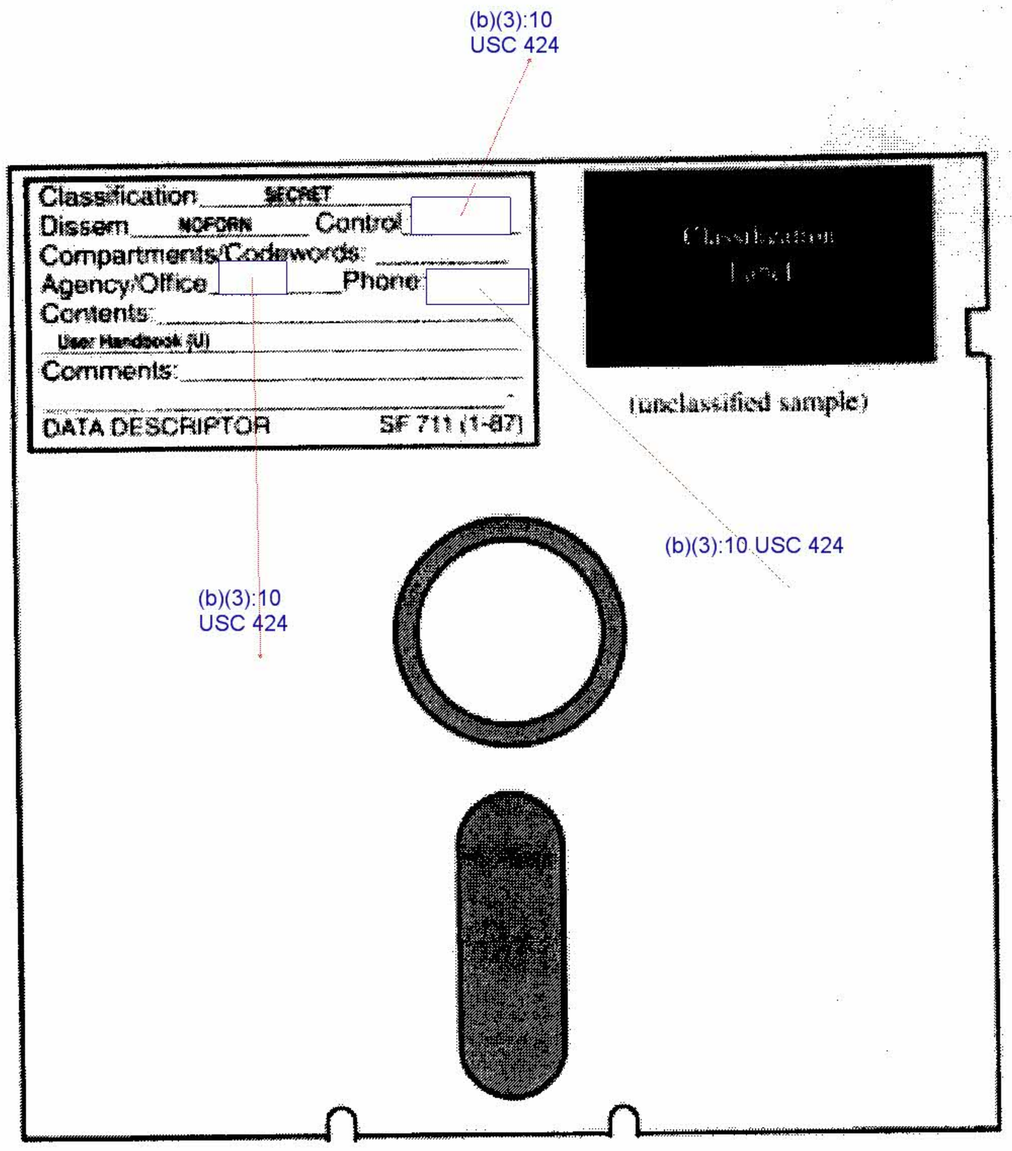
Classified By: B-99 REC A\C SCTY Class Guide
Declassify On: 31 Dec 1998

April 18, 1984

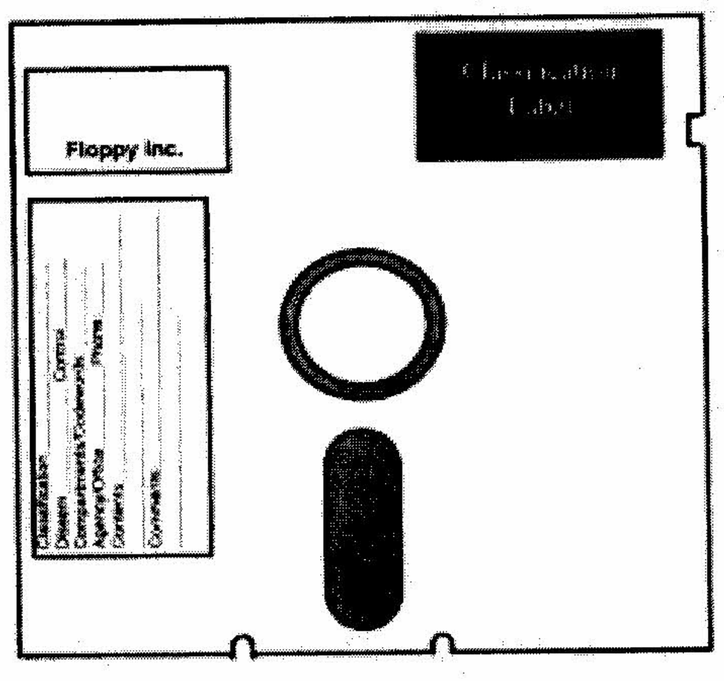
Defense Intelligence Agency
Washington, DC 20340

SECRET

Photographs.



ADP storage media.



SECRET

(unclassified sample)

DEFENSE INTELLIGENCE AGENCY
Washington, D.C. 20340

April 16, 1984

INDUSTRIAL STANDARDS (U)

FOREIGN GOVERNMENT INFORMATION

or

THIS DOCUMENT CONTAINS
GERMAN INFORMATION

or

Classified by: Multiple Sources
Declassify on: OADR

SECRET

Foreign Government Information in a DIA document.

SECRET

(unclassified sample)

1. (GE-S) This sample shows portion markings in a document that contains foreign classified information. This paragraph would contain GERMAN SECRET information.

2. (GE-C) The recipient of a foreign classified document is responsible for ensuring that the classification and the country of origin appear in ENGLISH on the document. This paragraph would contain GERMAN CONFIDENTIAL information.

3. (C) The purpose of the portion markings is to distinguish the foreign information from the U.S. information. This paragraph is marked to show that no foreign classified is contained in it.

SECRET

TOP SECRET

(unclassified sample)

Title (U)

(S/FRD) This paragraph contains "Formerly Restricted Data" classified at the SECRET level.

(TS/RD) This paragraph contains "Restricted Data" classified at the TOP SECRET level.

(S/RD (N)) This paragraph contains "Critical Nuclear Weapon Design Information (CNWDI) Restricted Data" classified at the SECRET level.

TOP SECRET
RESTRICTED DATA/CNWDI

Restricted Data, Formerly Restricted Data and CNWDI.

TOP SECRET

(unclassified sample)

Downgrade To: Secret
On: 1 Jul 94

TOP SECRET

SECRET

(unclassified sample)

Downgrade To: Confidential
On: Completion of Conference

SECRET

Downgrading instructions.

Chapter 4

Appendix B

INTELLIGENCE CONTROL MARKINGS AND WARNING NOTICES

Intelligence control markings and warning notices alert holders that additional protective measures are required, such as restrictions on use, dissemination, extraction, or reproduction. Place these markings on the outside of the front cover or on the first page if there is no front cover.

If it is not possible to display control markings and warnings notices directly on the material, include a written notification of the assigned classification and required control markings with the material.

Intelligence Control Markings and Their Use

Use intelligence control markings only on intelligence products and for the purposes prescribed.

Not Releasable to Foreign Nationals. NOFORN identifies classified intelligence that may not be released in any form to foreign governments, foreign nationals, or non-U.S. citizens without permission of the originator.

Warning Notice—Intelligence Sources or Methods Involved. WNINTEL identifies classified intelligence whose sensitivity constrains its further dissemination and use. This caveat is used only on intelligence that identifies or would reasonably permit identification of an intelligence source or method susceptible to countermeasure that could nullify or reduce its effectiveness. This marking will not be used in conjunction with special access or sensitive compartmented information (SCI) controls.

Not Releasable to Contractors/Consultants. This marking identifies classified intelligence that may not be released to contractors or consultants without the permission of the originating agency.

Dissemination and Extraction of Information Controlled by Originator. ORCON requires the continuing knowledge and supervision by originator of the use made of intelligence. This marking is used only on classified intelligence which clearly identifies or would reasonably permit ready identification of an intelligence source or method that is particularly susceptible to countermeasures that would nullify or measurably reduce its effectiveness.

Caution—Proprietary Information Involved. 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 trade secret or proprietary data believed to have actual or potential value. This marking may be used in conjunction with the NOCONTRACT marking to preclude dissemination to a contractor.

Authorized for Release to (name of country/international organization). This marking identifies classified intelligence that an originator has predetermined to be releasable to the foreign country or international organization indicated.

Markings to identify, control, and protect Sensitive Compartmented Information are contained in DoD C-5105.21-M-1; DoD TS-5105.21-M-2; and DoD TS-5105.21-M-3.

Warning Notices and Their Use

Restricted Data. RESTRICTED DATA identifies data concerning (a) the design, manufacture or utilization of atomic weapons; (b) the production of special nuclear material; or (c) the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted Data category under section 142 of the Atomic Energy Act of 1954, as amended (Title 42, U.S. Code).

Critical Nuclear Design Information (CNWDI). CNWDI is TOP SECRET or SECRET RESTRICTED DATA which reveals the theory of operation or design of the components of a thermonuclear or implosion-type fission bomb, warhead, demolition munitions or test device. Specifically excluded is information concerning arming, fuzing, and firing systems; limited life components; and total contained quantities of fissionable, fusionable, and high explosive materials by type. Among these excluded items are the components which DoD personnel set, maintain, operate, test, or replace.

Formerly Restricted Data (FRD). 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 related primarily to the military utilization of atomic weapons and that such information can be safeguarded adequately as classified defense information. For purposes of foreign dissemination, however, such information is treated in the same manner as Restricted Data. *If a document contains both RESTRICTED DATA AND FORMERLY RESTRICTED DATA, use the RESTRICTED DATA marking.*

Communications Security (COMSEC). COMSEC is protective measures taken to deny unauthorized persons information derived from telecommunications of the United States Government related to national security and to ensure the authenticity of such communications.

Place the following marking on COMSEC documents before release to contractors. Apply it when the document is created if release to contractors is likely.

"COMSEC Material - Access by Contractor Personnel Restricted to U.S. Citizens Holding Final Government Clearance."

Dissemination and Reproduction Notice

Classified information that the DIA originator determines to be subject to special dissemination or reproduction limitations will include, as applicable, a statement on its cover sheet, first page, or in the text, such as the following:

"Reproduction requires approval of originator or higher DoD Authority."

"Further dissemination only as directed by (insert appropriate office or official) or higher DoD Authority."

Chapter 5

DOCUMENT CONTROL

Contents

	Page
Policy	5-1
Access	5-1
Dissemination	5-2
Accountability and Control	5-4
Reproduction of Classified Material	5-6
Transmission	5-8
Disposal and Destruction	5-12
Appendix A, Collateral Top Secret Control Program	5-15
Appendix B, Instructions Governing Use of Codewords and Nicknames	5-19
Appendix C, Hand-Carrying Classified Information Outside the WLTA and Aboard Commercial Aircraft	5-23

Policy

- No person may have access to classified information without the appropriate security clearance and a demonstrated need-to-know.

- No one has a right to have access to classified information solely by virtue of rank or position.

- The responsibility for determining need-to-know rests with the individual who has authorized possession, knowledge, or control of the information.

Access

Access to classified information requires an appropriate security clearance and a demonstrated need-to-know. No one has a right to classified information solely by virtue of rank or position. The final responsibility for determining whether an individual's official duties require access to classified information and whether the individual has the appropriate security clearance, rests with the individual who has authorized possession, knowledge, or control of the information.

Before granting access to non-U.S. citizens with a Limited Access Authorization (LAA), ensure the classified information is within the scope of the approved LAA.

Two-Person Integrity (TPI) Rule. The TPI Rule means there must be at least two employees working in areas where collateral TOP SECRET or special access program information is used, stored, or accessible. This rule no longer applies on a DIA-wide basis. However, because of the importance of collateral TOP SECRET and information controlled within approved Special Access Programs, Senior Office Chiefs may invoke the TPI Rule in selected activities within their area of responsibility based on the threat to that information. All employees in the selected area of responsibility, [redacted] shall be notified of the decision to invoke the TPI Rule.

(b)(3):10 USC 424

Congress and Other Legislative Branch Elements. The Legislative Liaison Staff (PSL-L) is the releasing authority for *all* DIA information. DIAM 56-3 provides policy for Legislative Branch access to special access program material.

Industrial, Educational, and Commercial Entities. Bidders, contractors, grantees, educational, scientific, and industrial organizations may have access to classified information when such access is essential to a function that is in the interest of national security, and the recipients have appropriate security clearances.

Historical Researchers. DIA officials with original classification jurisdiction over the information may grant access to classified information to persons engaged in historical research. However, certain measures must be taken to ensure security of the information. Contact [redacted] for guidance.

(b)(3):10 USC 424

Judicial Proceedings. DIAR 12-13 governs release of classified information in litigation.

Foreign Nationals, Foreign Governments, and International Organizations. DIAR 50-27 governs access to classified information by foreign nationals, foreign governments, and international organizations. National Telecommunications and Information Systems Security Committee policy governs access to COMSEC information.

Other Situations. The Director or Chief of Staff may authorize access by persons outside the Federal Government upon determining that the recipient is trustworthy for the purpose of accomplishing a national security objective and that the recipient will safeguard the information from unauthorized disclosure.

Dissemination

Disseminate classified information only to persons and activities meeting access criteria and having proper storage facilities. The control markings and warning notices described in Chapter 4 assist in properly disseminating intelligence information. Submit Statements of Intelligence Interest to [redacted] to validate an element's standing distribution requirements. Revalidate statements annually.

(b)(3):10 USC 424

Information for public release must undergo a formal security and policy review prior to dissemination. Chapter 10 provides direction for obtaining the reviews.

TOP SECRET Information. TOP SECRET information originated by another DoD Component may not be disseminated outside the DoD without the consent of the originating DoD Component or higher authority. Distribute TOP SECRET information separately if it can be segregated from classified portions bearing lower classifications; dissemination is controlled through the DIA TOP SECRET Control Officer

(b)(3):10 USC 424

SECRET and CONFIDENTIAL Information. SECRET and CONFIDENTIAL information originated within the DoD may be disseminated within the Executive Branch, unless prohibited by the originator. Dissemination is also subject to intelligence control markings and warning notices.

Codewords and Nicknames. Refer to Appendix B for information on codewords and nicknames.

Release of Non-DoD Information. Normally, classified information originating in a non-DoD department or agency will not be disseminated outside DoD without the consent of the originating department or agency. However, unless special caveats are involved, Intelligence Community information may be used in products prepared by and distributed to Intelligence Community components. This consent is subject to restrictions set forth in Director of Central Intelligence Directive 1/7, "Security Controls on the Dissemination of Intelligence Information."

Some information may carry special caveats, such as "Dissemination or Extraction of Information Controlled by Originator" or "ORCON." Obtain permission of the originator before disseminating information with special caveats. Permission granted applies only to the specific purposes agreed to by the originator and does not automatically apply to any other recipient. Originators should sanitize or paraphrase text to make it suitable for release without intelligence control markings.

Release to U.S. Contractors. Refer contractor requests for intelligence information to

(b)(3):10 USC 424

Each Director For, Office Director, and Head of Special Office is authorized to release to contractors intelligence information for which his/her office is the office of primary interest.

The following documents will not be released to contractors. However, information in them may be made available to contractors, provided the information is not identified as national intelligence.

- National Intelligence Estimates.
- Special National Intelligence Estimates.
- Interagency Intelligence Memoranda.

- National Intelligence Analytical Memorandum.

- The DIA Fact Book.

RESTRICTED DATA and FORMERLY RESTRICTED DATA. Do not disseminate outside authorized channels information bearing the RESTRICTED DATA and FORMERLY RESTRICTED DATA warning notices without permission of the originator. Refer to DIAR 55-2 for instructions on CRITICAL NUCLEAR WEAPONS DESIGN INFORMATION.

Release of Other Information. DIA and DoD issue separate regulatory dissemination, handling, and control procedures for specific types of information. Refer to the following publications:

NATO Information	DIAR 50-32
COMSEC Information	DIAR 35-5
Special Access Program Information	DIAM 56-3
Sensitive Compartmented Information	DIAM 50-1
	DoD C-5105.21-M-1
	DoD TS-5105.21-M-2
	DoD TS-5105.21-M-3

Accountability and Control

The DIA accounting and control system for classified information serves to:

- Limit dissemination.

- Prevent unnecessary reproduction.

- Assign responsibility for the material to the appropriate office or person.

- Determine holders of the material so they can be notified of unscheduled changes in the classification of or compromises to the material.

Each DIA employee is responsible and accountable for handling and controlling classified information to prevent its unauthorized disclosure.

(b)(3):10 USC 424

is the central DIA office for the receipt of incoming mail, bulk shipments, and items delivered by courier to DIA, and develops procedures to sort, separate, and disseminate incoming material to ensure it is not subject to unauthorized disclosure.

Each DIA office will establish procedures to ensure incoming material is adequately protected

until a determination is made whether it contains classified information. Each office will ensure classified information is controlled properly and access limited to cleared personnel.

Cover Sheets. Attach cover sheets to classified documents when removing them from classified storage and safekeeping, and when sending them through the DIA mailing system. Use Standard Forms 703, 704, and 705 for TOP SECRET, SECRET and CONFIDENTIAL documents, respectively. Existing supplies of similar purpose forms may no longer be used. Use DA Label 87 FOR OFFICIAL USE ONLY documents.

TOP SECRET Control System. Unauthorized disclosure of TOP SECRET information could cause exceptionally grave damage to national security. Therefore, the TOP SECRET control system monitors each document or material through a continuous chain of receipts from its receipt or creation until its dissemination from DIA or its destruction. The DIA TOP SECRET Control Officer and appointed element control officers coordinate and monitor the activities of the system. Appendix A describes the duties of the control officers and control procedures for TOP SECRET material.

SECRET Information: Unauthorized disclosure of SECRET information could cause serious damage to national security. Use receipts to maintain accountability and control of SECRET material and to ensure proper delivery to the intended recipient. Receipts are required when sending SECRET material outside DIA or between DIA elements located outside the Washington, DC area. Receipts must be signed and returned to the sender. Use the following forms:

- DIA Form 13 (DIA Routing and Control Record). Use this form for transmittal between DIA elements located outside the Washington, DC area and on the outside of envelopes of material being sent outside DIA.

- DIA Form 56 (DIA Document Transmittal). Use this form for material sent outside DIA.

A receipt is not required when--

- SECRET material is sent electronically through communications centers.

- There is a hand-to-hand transfer, provided the receiving party acknowledges responsibility for the material.

Retain receipts for SECRET material for 2 years.

CONFIDENTIAL Information. Unauthorized release of CONFIDENTIAL information could cause damage to the national security. However, receipts for CONFIDENTIAL information are not required except when the information is transmitted to a foreign government or upon request.

Foreign Government Information. Protect foreign government information other than NATO information as prescribed for U.S. classified information of a comparable classification.

Working Papers. Working papers are documents and material accumulated or created in the preparation of finished classified documents and material. To control working papers:

- Date when created.
- Mark with the highest classification of information contained therein.
- Protect according to the assigned classification, to include proper use of cover sheets. TOP SECRET cover sheets must be affixed to all collateral TOP SECRET working papers.
- Destroy when no longer needed.
- Treat as a finished document of same classification when:
  - Releasing the document outside the activity or transmitting electrically through message center channels.
  - Retaining the document more than 90 days from date of origin. (Collateral TOP SECRET working papers within SCI Facilities may be retained for 180 days.)
  - Filing permanently.

Reproduction of Classified Material

Do not reproduce collateral TOP SECRET or special access program information without the consent of the originator or higher authority. Observe all special dissemination or reproduction limitations. When possible, two people should be involved in the reproduction process for collateral TOP SECRET information to help ensure positive control and safeguarding of all copies. The following additional measures apply to the reproduction of classified information:

General.

- The chief, or designated representative, of each DIA branch or higher element will ensure reproduction of classified information complies with this handbook. If the reproduction equipment is used by more than one element, the senior official is responsible for protective measures.
- Copying of documents containing classified information will be minimized.

- Classified documents reproduced for any purpose, including those incorporated in a working paper, are subject to the same controls prescribed for the original documents.

Authority to Reproduce Classified Documents.

- All DIA employees with SCI access are authorized to reproduce SECRET information.

- DIA division chiefs and higher officials may authorize the reproduction of collateral TOP SECRET information. This authority may not be delegated.

Restrictions on Reproduction of Classified Documents.

- TOP SECRET and SECRET information and any CONFIDENTIAL information subject to stated prohibitions against reproduction that is submitted to a DIA service element for publication, printing, or other reproduction will be accompanied by a completed DD Form 844, "Requisition for Local Duplicating Service."

- JCS papers will not be reproduced. (See JCS Memorandum of Policy No. 39.)

- For reproductions requiring prior authorization or special authority, show the approving authority on the face of each reproduced copy. For example:

  Reproduced (date) by (office symbol) by authority of
  (authorizing office symbol or agency)

  Reproduced copy 1 of (insert number) copies.

- When reproducing TOP SECRET material or classified documents covered by special dissemination and reproduction limitations, mark the copies as follows:

  Reproduced (date) by (office symbol)
  Reproduced copy 1 of (insert number) copies.

Records Requirements.

- Maintain receipts for 2 years to show the number and distribution of reproduced copies of all:

  - TOP SECRET documents.

  - Classified documents covered by Special Access Programs.

- SECRET and CONFIDENTIAL documents marked with special dissemination and reproduction limitations.

Reproduction Equipment.

· Use only equipment specifically designated for the reproduction of classified information. Post the rules for reproducing classified information on or near the designated equipment.

· Post notices prohibiting the reproduction of classified information on equipment used for reproducing only unclassified information.

· Follow the proper procedures for secure reproduction. Thoroughly inspect the equipment and surrounding area before leaving and secure all classified information, including the original, reproduced copies, and classified waste.

Transmission

Classified information may be transmitted by hand carrying, mail/distribution centers, electronically, secure telephone, or other approved secure means. [redacted] is responsible for courier and mail services; [redacted] is responsible for message center operations. (b)(3):10 USC 424 (b)(3):10 USC 424

Refer to DIAR 12-30, "Mail and Distribution Management Program," for detailed procedures for mailing classified information. Use packaging material of such strength and durability as to:

· Provide security protection while in transit.

· Prevent items from breaking out of the container.

· Facilitate the detection of any tampering with the container.

· Conceal all classified characteristics.

Sealed envelopes are not required when transmitting classified information within secure areas. If the face of a document contains classified information, use an appropriate cover sheet to conceal the information. Persons hand-carrying the classified information must have a security clearance at least as high as the classified information in their possession.

When classified material is too large for envelopes, use two opaque sealed containers, such as boxes, cartons or heavy wrappings. If the classified information is an internal part of a piece of equipment or is an item that cannot reasonably be packaged, the outside shell may serve as a sufficient covering. However, if the shell reveals classified information, it must be concealed.

Conditions for Hand-Carrying. Hand-carrying classified information is subject to the following conditions:

- A time-critical or emergency situation exists and all other methods of transmission are impractical. It is specifically prohibited to delay preparing classified information for transmittal or to neglect using one of the preferred methods of transmittal in order to create an artificial time-critical situation.

- The courier has a security clearance equal to or higher than the classification of the information being hand-carried.

- The storage provisions of Chapter 6 apply at all stops en route to the destination.

- For overnight trips, advance arrangements for the proper overnight storage are made with a U.S. Government facility or, within the United States, a cleared contractor's facility.

- Classified information will not be read, studied, displayed, or used in any manner in public conveyances or places.

- When classified information is carried in a private, public, or Government conveyance, it will not be placed in any detachable storage compartment such as automobile trailers, luggage racks, aircraft travel pods, or drop tanks, nor, under any circumstances, left unattended.

Procedures For Hand-Carrying Classified Information. Written authorization is not required to hand-carry collateral information *except* aboard commercial airline. Written authorization is required for SCI information.

Washington Local Travel Area. Obtain a DIA SCI courier authorization card from (b)(3):10 USC 424 and have the card in your possession. Ensure classified information is properly wrapped; keep the material in your possession at all times. Obtain signed receipts, if required, at point of destination. The Washington local travel area includes:

- The District of Columbia

- Maryland—The counties of Montgomery, Prince Georges, Anne Arundel, Baltimore, Charles, Calvert, Howard, Frederick, St. Mary's, Harford, Carroll, and Washington; the city of Baltimore; and all cities existing within the geographic boundaries of the above counties.

- Virginia—The counties of Arlington, Fairfax, Loudoun, Fauquier, Prince William, Culpepper, Orange, Stafford, Spotsylvania, King George, Madison, Green, Albermarle, and Clarke counties; the cities of Alexandria, Fairfax, Falls Church, Richmond, and Fredericksburg; and all cities existing within the geographic

boundaries of the above counties.

- Pennsylvania—Adams County.

Outside the Washington Local Travel Area. Ensure the conditions for hand-carrying classified information, listed above, are met. Obtain a courier authorization letter signed by the authorized official (see page 5-11).

Round-trip hand-carrying of classified information is the exception rather than the rule. If the classified information is to be returned to the DIA activity, it should be returned by more secure means such as the Defense Courier Service, Diplomatic Pouch, or U.S. mail, if appropriate for the classification level. If round-trip hand-carrying is required, specific justification must be provided.

Non-DIA personnel will not be granted authority by DIA to hand-carry classified information aboard commercial passenger aircraft without prior permission of their parent agency or service.

Restrictions on Hand-Carrying Classified Information Aboard Commercial Passenger Aircraft. Classified information will not be hand-carried aboard commercial passenger aircraft *unless*:

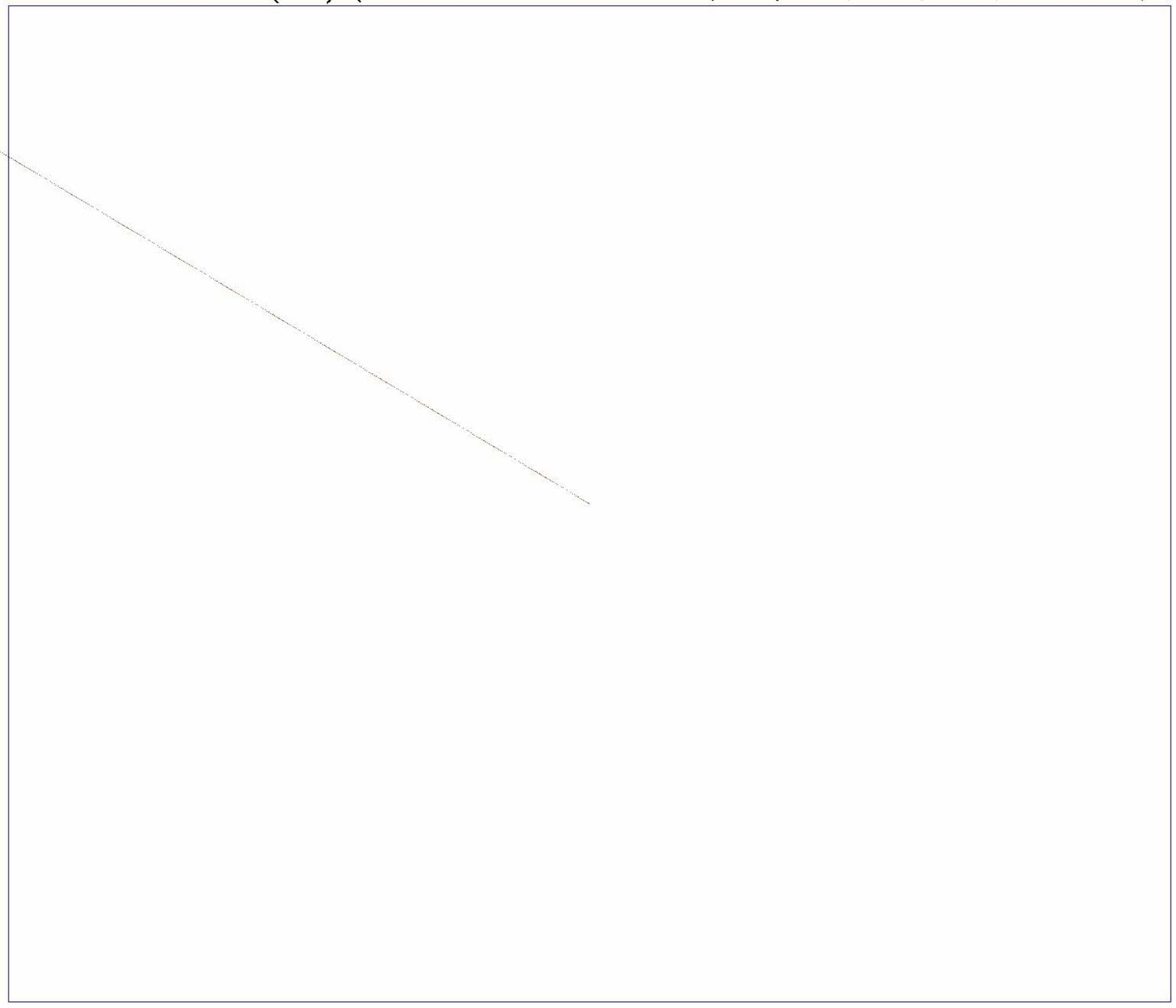
- The information is not available at the destination.
- The threat posed by terrorist or hijackers is considered low risk; if indications exist of possible terrorist activities, the travel will be canceled, postponed, rerouted or otherwise changed to avoid the indicated danger.
- The information cannot be sent via a secure facsimile transmission or there is no time to move the information by other secure means.
- The hand-carrying has been authorized by the appropriate official.
- Arrangements have been made to process material through customs, border, postal, or other inspectors, either U.S. or foreign.
- The hand-carrying is accomplished aboard a U.S. carrier. Foreign carriers will be used only when no U.S. carrier is available; the approving official must ensure the information will remain in the custody and physical control of the U.S. courier at all times.

Procedures for Requesting Authorization to Hand-Carry. DIA elements may establish internal administrative procedures for requesting authorization to hand-carry SCI outside the Washington local travel area or any classified information aboard commercial airlines. Appendix C gives courier instructions, format for staff summary sheets and courier letters, and a courier acknowledgment statement.

Approval Authority. The following officials are delegated approving authority for requests to escort or hand-carry classified information aboard commercial aircraft. In the absence of the approval authority, the person acting for the official may sign courier letters.

Chief of Staff (CS) (for Command Element, ES, EO, OC, GC, and DM)

(b)(3):10 USC 424



(b)(3):10 USC 424 will process courier letters for the Inspector General (IG), the DOD POW/MIA Central Documentation Office (CDO), and for DIA elements whose approval authority is unavailable. The Team Chief, National Military Joint Intelligence Center has signature authority for courier letters that must be processed during non-duty hours.

Facsimile. The sender must:

- Adhere to classification limitations displayed on the STU III or other equipment.

- Ensure documents have proper classification and control markings.

- Verify the intended recipient has the appropriate security clearance and need-to-know. In the case of transmitting TOP SECRET material, ensure the intended recipient is personally available to receive the transmission. Refer to Chapter 11 for transmission of FOR OFFICIAL USE ONLY information.

- Obtain receipts for SECRET and TOP SECRET transmissions.

Disposal and Destruction

Classified documents that are not permanently valuable records of the Government will not be retained more than 5 years from the date of origin unless such retention is authorized in DIAM 13-1. Dispose of non-record copies of documents and material when no longer required. Early destruction of unnecessary classified material assists in reducing security costs and provides better protection for necessary material. Refer to DIAM 13-1, for disposal of official record copies of documents; DoD TS-5105.21-M-1, for SCI material; and DIAM 56-3, for SAP material.

Annual Clean-Out Day. DIA elements will designate 1 day each year as a clean-out day and devote a portion of the day to the destruction of unneeded documents.

Laser Toner Cartridges. Within CONUS, Alaska, and Hawaii, sanitize the cartridge by running at least five full pages of unclassified, randomly generated text through the printer before the cartridge is removed; the random text should not include any blank spaces or solid black areas. Return the sanitized cartridge to the central supply store for recycling.

At overseas locations, in addition to the sanitization procedures described above, render the drum unusable by scoring it with an abrasive substance, such as sandpaper, to further reduce the possibility of image recovery.

(b)(3):10 USC 424

Equipment. Obtain [redacted] approval prior to purchasing information processing equipment with a latent image capability, including copiers and facsimile machines. Remove classified information prior to equipment turn-in or disposal. If parts with an image capability cannot be sanitized, destroy them as non-pulpable classified waste.

Records of Destruction. Use DIA Form 13, DIA Form 36, or DIA Form 79, and record the date of destruction, burn bag number, and destruction/witnessing official. Destruction records are not required unless an item of waste has been entered into accountability records. Retain records of destruction 2 years.

TOP SECRET. Records of destruction are required; two persons cleared for TOP SECRET must date and sign the form at the time of destruction.

SECRET and CONFIDENTIAL. Records of destruction are not required, except for NATO SECRET and designated Special Access Programs and some compartments of SCI. (DIAR 50-32 provides guidance on the destruction of NATO classified material.)

Method of Destruction. Destroy classified material by burning, melting, chemical decomposition, pulping, pulverizing, or cross-cut shredding. Burn bags and shredders are most frequently used in DIA. Coordinate purchase of destruction equipment with [redacted] (b)(3):10 USC 424

Burn Bags. For pulpable classified waste, use a pre-printed red and white striped bag. For non-pulpable classified waste, such as plastic, film, magnetic tape, viewgraphs, typewriter ribbons, and floppy disks, use a pre-printed blue and white bag, containing the word "NON-PULPABLE". Burn bags are available at the self-service supply centers or through [redacted] (b)(3):10 USC 424 As a substitute, mark plain brown bags marked with bold red (or blue for non-pulpable) stripes. To use burn bags:

- Mark the outer bag, when placed in use, with the office symbol and telephone number of the using office, the highest classification of material to be placed in the bag, the name of the primary person using the bag, and serial number (by year).
- Record the serial number, level of classification, and user's office symbol in a log book.
- Fill the bag to one-half of the bag's capacity, but not exceeding 10 pounds. Securely seal the bag with one-inch combustible (masking) tape.
- Deliver bags to [redacted] collection points after checking them off the log book. (b)(3):10 USC 424

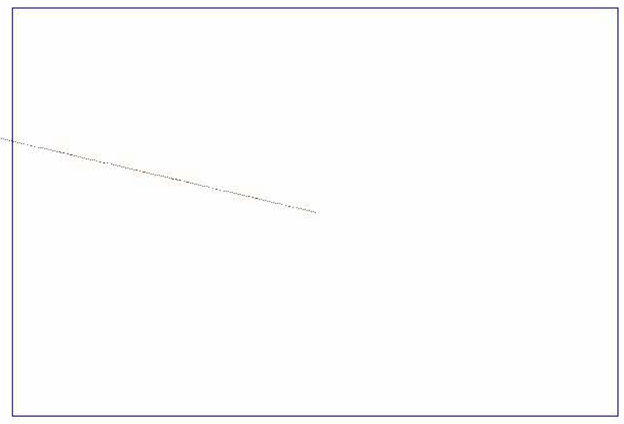
Do not place unclassified papers, discarded food and beverage containers, glass, metal, newspapers, magazines, or similar items in burn bags. Some of these items could create health and safety hazards for employees at the destruction facilities.

Do not use burn bags for any purpose other than disposing of classified material. This prohibition includes the use of burn bags to transmit classified information not intended for delivery to a destruction facility or to carry personal items.

Shredders. Different shredding requirements exist for collateral and SCI materials. [redacted] (b)(3):10 USC 424 maintains current listings of shredders approved for these materials. Elements should purchase shredders which produce unclassified material. Close the bag of shredded waste with tape or by tying and dispose of it as normal trash through recycling. If shredders do not produce unclassified waste, place the material in a burn bag and dispose of it as described above. [redacted] (b)(3):10 USC 424

POC: (b)(3):10 USC 424

(b)(3):10 USC 424



Chapter 5

Appendix A

COLLATERAL TOP SECRET CONTROL PROGRAM

TOP SECRET information, if disclosed, could cause exceptionally grave damage to the security of the United States. Therefore, DIA has implemented additional accountability and control procedures known as the Collateral TOP SECRET Control Program.

The program controls TOP SECRET documents and material through Major Control Point Accounts for each major office. All materials are disseminated through TOP SECRET control officers at the various organizational levels of DIA. The control officers account for the documents from time of receipt or creation in DIA through transfer out of DIA or destruction.

TOP SECRET Control Officers

DIA TOP SECRET Control Officer. The DIA TOP SECRET Control Officer (TSCO) is the primary control officer for the Agency, and resides in [redacted] The DIA TSCO:

(b)(3):10 USC 424

- Coordinates and monitors the activities of the Collateral TOP SECRET Control Program; provides technical guidance and assistance to Major Office TSCO; and maintains a roster of TSCOs, alternates, and agents.

- Receives and distributes all collateral TOP SECRET documents, messages, and registered publications to and from DIA and maintains required receipts.

- Conducts an inventory of registered publications and Department of Energy and Defense Nuclear Agency TOP SECRET documents within DIA, as required. Confirms the accuracy of annual inventory reports and investigates any discrepancies; and maintains annual reports for 5 years.

- Provides statistical analysis to the Office of the Secretary of Defense concerning active documents held by DIA.

- Approves any waiver to the control of collateral TOP SECRET documents.

Major Element TOP SECRET Control Officer. Each Director For, Office Director, and Head of Special Office appoints, in writing, a Major Element TSCO and alternate. (Send a copy of the appointment memorandum to the DIA TSCO.) The Major Office TSCO:

- Receives and dispatches all collateral TOP SECRET documents transmitted to or from the organizational element; maintains required receipts; and maintains TOP SECRET accountability registers.

- Ensures personnel who have custody of TOP SECRET documents are properly cleared of accountability for such material when they leave the element or no longer have need for the material.

- Submits to the DIA TSCO, in writing, all appointments of TSCOs, alternates, and TOP SECRET Control Agents.

- Serves as a certifying official for destruction of TOP SECRET documents in the Major Office. If the volume of documents or other factors require the destruction of TOP SECRET documents by a subordinate office, the chief of the Major Office may authorize the Subordinate Element TSCO to act as the certifying official.

- Reports to the Chief of the Major Office any violations of the rules for safeguarding and controlling TOP SECRET information or any condition that might lead to loss of control over such information.

Subordinate Element TOP SECRET Control Officers. Subordinate Element TSCOs will be appointed, in writing, as necessary for efficiency of operation within the Major Element TSCO account. (Subordinate element TSCOs may be designated as Major Element TSCOs due to the volume of material they receive or their physical location.) The Subordinate Element TSCO:

- Controls documents routed to the subordinate element from the Major Office TSCO.

- Maintains TOP SECRET accountability registers.

- Dispatches to the Major Office TSCO, TOP SECRET documents designated for transfer to an office outside the element.

- Transfers to the Major Office TSCO documents designated for destruction. If authorized to certify destruction, provides copies of destruction certificates to the Major Office TSCO.

TOP SECRET Control Agents (TSCAs). TSCAs may be appointed, in writing, as necessary for efficiency of operation within the Major Element TSCO account. TSCAs may also be appointed to assist a Subordinate Element TSCO. A TSCA:

- Receives from and transmits TOP SECRET documents to the Major Element or Subordinate Element TSCO.

- Maintains TOP SECRET accountability registers.

- Performs these functions through the appropriate Major Office or Subordinate Element TSCO.

Document Control

Retain TOP SECRET documents only to the extent necessary to satisfy current requirements; destroy non-record copies of TOP SECRET documents when no longer needed. When appropriate, downgrade, declassify, or retire documents that cannot be destroyed. Control dissemination of TOP SECRET documents through a continuous chain of receipts.

TOP SECRET Registers. Each TSCO or TSCA maintains an active and an inactive register for TOP SECRET documents within their element. Each DIA Form 125 is considered a register page; a compilation of the forms constitutes the TOP SECRET accountability register.

Active Register. Active registers reflect the status of all TOP SECRET documents currently held in the element. Maintain active registers by:

- Numbering the pages sequentially by year.
- Transferring pages to the inactive register after destroying, declassifying, downgrading, or transferring the document.

If a register page lists several items and some have been destroyed or processed out of the TSCO's control, draw a line across the page and enter below the line all active items. The consolidation of active items will expedite annual inventory procedures.

Inactive Register. This register reflects actions on documents no longer held in the element—documents were transferred out of the element, declassified, or destroyed. File this register by year, and retain for 5 years.

Numbering Documents. Number TOP SECRET documents and material in sequential order and mark each document with a copy number, for example, copy 1 of 2 copies.

Disclosure Records. Each individual, including clerical and administrative personnel, receiving access to a TOP SECRET document will sign DIA Form 189-1 (TOP SECRET Access and Control Record). Disclosures to individuals who may have had access to containers in which TOP SECRET information is stored, or who regularly handle a large volume of such information need not sign the access record. Such individuals, when identified on a roster, are deemed to have had access to such information.

When the document is destroyed, declassified, downgraded, or transferred outside of DIA, detach DIA Form 189-1 and attach it to the register page maintained for the document. Retain disclosure records for 5 years after the documents are transferred, downgraded, or destroyed.

Inventory. All TOP SECRET control accounts will be inventoried the first quarter of each calendar year or upon change of TSCO. Major Office TSCOs who do not have active TOP SECRET documents will submit a report reflecting that fact.

Purpose. The inventory will determine if the TSCO is following proper procedures, that documents entered in the register are active and properly accounted for, and that all TOP SECRET material throughout the office(s) served by the account is properly entered in the register.

Inventory Team. Directors For, Office Directors, or Heads of Special Offices will appoint, in writing, personnel from their element to serve on the inventory team. (Send a copy of the appointment letter to the DIA TSCO.) Each member will possess a final TOP SECRET clearance. Neither the Major Office TSCO, Subordinate Element TSCO, alternate TSCOs, nor TOP SECRET Control Agents will be a member of the inventory team. As an exception to this policy, change of custodian inventories will, whenever possible, be conducted jointly by the incoming and outgoing TSCOs to ensure complete reconciliation of the account and to avoid subsequent allegations that the account was incomplete at the time of transfer.

Inventory Procedure. The inventory team will do the following:

- Count register pages to verify completeness of the register.

- View all documents in the register. For Major Office accounts with subordinate offices, account for documents through sighting a receipt or destruction certificate from the subordinate TSCO. Initial register pages with drawn lines after verifying accuracy of the page.

- Review enough receipts and certificates of destruction to verify correct procedures.

- Review inactive register; verify that documents listed are no longer the responsibility of the office being inspected; mark "audited" on the page and have one team member initial and date the page. Entries so marked will not be reinspected on subsequent inspections.

- Attempt to resolve any discrepancies noted during the inventory, and treat as a possible security violation the inability to account for a document.

- Submit a written report of the inventory to the DIA TSCO not later than 31 March, and provide a copy to the responsible TSCO who will retain the report for 5 years.

Chapter 5

Appendix B

INSTRUCTIONS GOVERNING USE OF CODEWORDS AND NICKNAMES

Definitions

Using Element. The DIA element to which a codeword or nickname is allocated for use.

Codeword. A single word selected from blocks of codewords assigned by the Joint Chiefs of Staff (JCS) and assigned a classified meaning by appropriate authority. A codeword is placed in one of three categories:

Available. Allocated to DIA. Available codewords individually are unclassified until placed in the active category.

Active. Assigned a classified meaning and current.

Canceled. Formerly active, but discontinued due to compromise, suspected compromise, cessation, or completion of the operation to which the codeword pertained. A canceled codeword is generally unclassified and remains so until returned to the available category.

Nickname. A combination of two separate, unclassified words. The words have an unclassified meaning and are assigned to any classified activity where there is a frequent need to make unclassified references to the activity.

Policy

Codewords. Use codewords to ensure proper security concerning intentions and to safeguard information pertaining to actual plans or operations classified as CONFIDENTIAL or higher. Within DIA, codewords normally designate a special access program or related special activity. Words selected as codewords will not suggest the nature of its meaning.

Nicknames. Use nicknames for actual, real world events, projects, or other activities involving elements of information of any classification category. However, 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.*

Classification and Downgrading Instructions

The using element will assign a specific, classified meaning to a codeword, commensurate with security requirements. Codewords shall not be used to cover unclassified meanings. The assigned meaning need not be classified as high as the classification assigned to the plan or operation as a whole.

When a codeword is referred to in documents, place the security classification of the codeword in parentheses immediately following the codeword, for example, "Label (C)." Use the meaning of a codeword and the codeword together only when it is essential to do so.

Classification. The codeword and its meaning shall have the same classification. At a minimum, classify codewords CONFIDENTIAL.

Downgrading. When a special access program is discontinued or completed, and is not replaced by a similar program but the meaning cannot be declassified, cancel the codeword and downgrade the classification to a minimum of CONFIDENTIAL. Notify [redacted] of the cancellation. [redacted] will transfer the codeword to the "canceled" category for 2 years before declassifying and moving it to the "available" category.

(b)(3):10 USC 424

(b)(3):10 USC 424

A codeword replaced by another codeword due to a compromise or suspected compromise, or for any other reason, shall be canceled, and classified CONFIDENTIAL for 2 years.

Procedures

[redacted] is the DIA point of contact with the Joint Chiefs of Staff on all matters pertaining to codewords and nicknames, and allocates them to DIA elements upon written request.

(b)(3):10 USC 424

To request a codeword or nickname, send a memorandum signed by a division chief or higher official to [redacted] Classify and mark the memorandum in the appropriate manner for classified correspondence. Provide the following information:

(b)(3):10 USC 424

- Identify what the request is for—codeword or nickname.
- The name and telephone number of the element's point of contact.
- The classification to be assigned the (unstated) codeword. Nicknames are unclassified.
- The meaning of the codeword or nickname.
  - *Codeword.* The classified meaning should be specific, but not detailed. For example, "invasion of France," would have been a specific, but not detailed meaning of Operation OVERLORD. "Troop movement" would not have been a specific meaning.

- *Nickname*. The unclassified meaning may be non-specific, for example, "collection project," or "exchange agreement."

- The date the codeword or nickname becomes active. This date may be earlier than the date of the request.

(b)(3):10 USC 424

The requesting office will notify [redacted] when the classification of a codeword or its meaning is upgraded or downgraded, when a codeword is canceled or compromised, or when the responsibility for a codeword is transferred to another element. Also notify [redacted] upon the termination, supersession, or transfer of nicknames.

(b)(3):10 USC 424

Chapter 5

APPENDIX C

HAND-CARRYING CLASSIFIED INFORMATION OUTSIDE THE WASHINGTON LOCAL TRAVEL AREA AND ABOARD COMMERCIAL AIRCRAFT

Contents

	Page
Special Instructions for Courier	5-24
Format for Staff Summary Sheet	5-28
Courier Letter of Authorization	5-29
Courier Acknowledgement Statement	5-31

Special Instructions for Courier of Classified Information Outside the Washington Local Travel Area and Aboard Commercial Aircraft

As an official courier for classified material, you are responsible for the protection of the material in your custody. You must avoid all places, situations, and circumstances which could compromise your ability to protect the documents. You will have discharged your responsibilities when you release the material to the authorized recipient or the Special Security Office (for SCI) at your destination.

The following information is provided to enable you to carry out your duties:

(b)(3):10 USC 424

Prior to hand-carrying/couriering classified information outside the U.S., obtain a threat briefing of possible activities that could pose a threat to you or the classified information. (Within the Washington, DC area, [redacted] provides the briefing. Outside the Washington, D.C. area, contact the nearest military service counterintelligence element, the U.S. Embassy, or U.S. Consul.) If information indicates a definite threat, your travel plans must be changed to avoid the threat.

You should not use foreign-registered aircraft unless a U.S. airline or U.S. military aircraft is not available. Aircraft of countries presumably unfriendly to the U.S. should never be used.

You (or your activity) are responsible for making arrangements to preclude customs, postal or other inspections, both U.S. and foreign. Within the United States and at ports of entry to the United States, your Courier Letter of Authorization should suffice. However, this letter most likely will not be honored overseas. When travelling outside the U.S., you should contact the party to be visited in advance of the trip, advise them that you will be carrying classified information, and request their assistance in passing the classified information through inspection points. If you are detained at an inspection point, request to be put in contact with the party to be visited or, if at an intermediate destination, with the U.S. Embassy, U.S. Consul or nearest U.S. military installation.

The possibility exists that you may become involved in a hijacking or hostage-type situation. All hostage type situations are unique. Use caution and common sense to judge the actions which will best contribute to your survival and the protection of the classified information involved. The following guidance must be considered in light of the realities of the actual situation:

- Your personal safety takes precedence over the security of the classified information.

- Do nothing to call attention to yourself or the classified information. Model your conduct on that of the other passengers. If required to identify yourself, do not display your Courier Letter of Authorization.

- If you can move away from the classified information without calling attention to

yourself, do so. (But keep track of it for possible retrieval later.)

- Do not try to use force to protect the classified information.

- Do not attempt to destroy or dispose of the classified information unless you can do so in complete safety.

- If you can escape or when you are released, you should bring the classified information with you, if you can do so without endangering or delaying your escape or release.

- If the classified information has been compromised or if it is left behind, notify [redacted] and your activity as soon as possible through the nearest U.S. diplomatic or military channels so that action can be taken to preclude or limit the impact of the compromise. (b)(3):10 USC 424

Retain classified material in your personal possession and under your constant surveillance at all times. Do not leave classified material in locked automobiles, quarters, hotel rooms, train compartments, or other such places, or stored in automobile trunks or in any detachable storage compartment. If the container is too large to carry on board, the courier will witness storage of material and the securing of the compartment prior to boarding the aircraft for departure, and will witness the unloading of material upon arrival. If intermittent stops are made between origin of flight and final destination, the courier will witness the opening/closing of the storage compartment at each stop.

If an overnight stop or unforeseen delay is encountered while en route and an accredited facility is not available, the material may be stored at a Defense Courier Service (DCS) Transfer Station, if available. If DCS is used for overnight storage, obtain a signed receipt. If none of these facilities is available, you must retain the material in your personal possession and properly safeguard it during the period of delay.

Federal Air Regulations require all passengers and their carry-on items be screened before boarding military or commercial aircraft. You should routinely offer briefcases or pouches for inspection; show the courier letter, if requested. The contents of briefcases and pouches may go through metal detection devices, unopened. If the person conducting the screening is not satisfied, and there is doubt as to the contents of the envelopes, you will not be permitted to board with the briefcase. ***Never allow screening personnel to open envelopes containing classified material.*** In the event you are not allowed to board the aircraft, contact [redacted] (b)(3):10 USC 424 (b)(3):10 USC 424

Wrapping Instructions for Collateral Classified Information.

- Double-wrap collateral classified documents; use opaque envelopes or kraft wrapping paper; tape all seams with reinforced paper or plastic tape. Package bulky material in durable fiberboard, cardboard, or wooden boxes.

- Place proper security classification markings on both sides, top and bottom, of the

innermost wrapper.

· Label the inner wrapper as follows:

IF FOUND, DO NOT OPEN. IMMEDIATELY NOTIFY

(b)(3):10 USC 424

[redacted]

· Affix a courier tag to the outer envelope of each package. Do not affix a courier tag to the outside of a briefcase, attache case, or to a carton or container being escorted, as this would draw attention to the classified material.

· Leave with your office a copy of DIA Form 56.

· If possible, carry collateral material in a locked briefcase. However, the briefcase cannot serve as the outer wrapper.

Wrapping Instructions for Sensitive Compartmented Information (SCI).

· Ensure all material such as slides, briefing papers, and working papers are properly marked and listed on DIA Form 56.

· At least 2 hours before departure time, take the material, Courier Letter of Authorization, and transmittal letter or DIA Form 56 to the SCI control office in the Pentagon or the DIAC. The material will be controlled and properly packaged for you.

(b)(3):10 USC 424

- Pentagon. SSO DIA [redacted] Hours of Operation: 0730-1400, Monday-Friday. [redacted] to arrange for service at times other than those listed or for short notice requirements.

(b)(3):10 USC 424

(b)(3):10 USC 424

- DIAC. [redacted] Hours of Operation: 0700-1500 hours.

· Affix a courier tag to the outer envelope of each package. Do not affix a courier tag to the outside of a briefcase, attache case, or to a carton or container being escorted, as this would draw attention to the classified material.

· Leave with your office a copy of DIAR Form 56.

· Carry SCI material in a locked briefcase or pouch. The briefcase serves as the third wrapping.

· Ensure material is stored with a servicing SSO at the TDY location and is given to that

SSO for wrapping, controlling, and shipping by DCS to Washington, DC. If material must be carried round-trip, have the SSO at the TDY location wrap and control the material.

Format for Staff Summary Sheet

Prepare a DIA Form 1 (Staff Summary Sheet) to request approval to courier SCI material outside the WLTA and to courier collateral aboard commercial aircraft. The Staff Summary Sheet will:

1. State the purpose of the request.

2. Provide background as to why material must be hand-carried.

3. Provide justification as to why the classified information could not be sent to the TDY location in advance of travel via mail/DCS.

4. Provide courier name(s), complete itinerary, flight information (if appropriate) to include time/date/place of departure; airline and flight number; all intermediate stops, to include time/date/place of arrival and departure and, as applicable, new airline and flight number; and time/date/place of arrival at the final destination.

5. For destinations outside the United States, its territories and Canada, provide a statement to the effect that arrangements have been made to preclude customs, postal or other inspections, both U.S. and foreign.

6. If round trip authorization is being requested, full justification must be provided as to why the classified information cannot be returned from the destination by more secure means.

15 July 1993 DIAR 50-2

Courier Letter of Authorization

(b)(3):10 USC 424

U-XXXX

TO: WHOM IT MAY CONCERN

SUBJECT: Courier Letter of Authorization

1. This letter certifies that the person whose name appears below and whose identity may be verified by the credentials described is:

a. A member of the *(insert applicable agency, i.e., Defense Intelligence Agency, Office of the Secretary of Defense, or Organization of the Joint Chiefs of Staff)*, Department of Defense, United States of America.

b. An official courier or escort for the *(insert applicable agency as above).*

c. Required to *(escort or hand-carry)* the *(parcel or carton/container)* as described from Washington, DC to the destination(s) shown *(add "and return to Washington, DC" if round trip hand-carrying is requested).*

2. Name, Grade, and Service of courier: *(e.g., DOE, John R., GS-14, Department of Defense civilian, or DOE, John R., Major, U.S. Army.)*

3. Identification: *(e.g., U.S. Passport Number or DD Form 2, Armed Forces Identification Card Number or DD Form 1466, Pentagon Building pass number, etc. If the identification does not contain the escort or courier's date of birth, height, weight or signature, include those items in this paragraph.)*

4. Destination to include transfer points and date(s): *(e.g., Washington, DC non-stop to New York City, NY, 2 July 1991 or Washington, DC via New York City, NY 1 July 1991 to Frankfurt, GE, 2 July 1991. Return from Frankfurt non-stop to Washington, DC, 5 July 1991.* ***DO NOT LIST FLIGHT NUMBERS.****)*

(b)(3):10 USC 424

5. Description of container(s): *(e.g., one sealed envelope addressed to: CDR, USAREUR, Attn: AERP, APO NY 09407; from DIA, ATTN: Wash, DC 20340, in a locked briefcase; or one carton, 12' x 12' x 12', addressed to: ...).*

6. Effective Period of Time: *(e.g., 1 through 5 July 1991)*

7. Confirmation of Authority may be made by calling the Defense Intelligence Agency *(Director For telephone number)* during the hours of 0730 through 1600 hours, Monday through Friday; or [redacted] during non-duty hours.

(b)(3):10 USC 424

FOR THE DIRECTOR:

(Approving Authority signature block)

Courier Acknowledgement Statement

I fully understand the security implications and responsibilities involved in serving as a courier of classified material required for the following trip and will observe all precautions prescribed by DIAR 50-2, SCI security directives, and DIAM 50-1.

NAME OF COURIER (PLEASE PRINT): _____
METHOD OF TRANSPORTATION: _____
DATE OF TRAVEL: _____
DESTINATION: _____

SIGNATURE AND DATE: _____

Chapter 6

STORAGE OF CLASSIFIED MATERIAL

Contents

	Page
Policy	6-1
Individual Responsibilities	6-1
Storage Requirement	6-2
Combinations	6-3
Lock-out and Repair of Containers	6-4
Opening, Closing, and Checking Security Containers	6-4
Security Container Turn-In	6-5
Vacating Secure Office Spaces	6-5

Policy

- Classified information shall be stored only under conditions adequate to prevent unauthorized persons from gaining access.

Supervisors will ensure classified information is stored in the manner prescribed by this chapter when it is not under the personal observation of cleared personnel.

Valuables such as money and weapons will not be stored with classified information because of the increased risk of security containers being opened, resulting in compromise of the information.

Individual Responsibilities

Responsibility and accountability for protecting classified information rests with the individual. All DIA personnel will surrender all classified information in their custody prior to departing DIA or transferring between DIA elements. If the information is required at the next duty assignment, the new element or office of assignment will officially request the information.

Classified information in the possession of DIA personnel at the time of their arrival in DIA will be immediately brought under control of their element. If excess to official element needs, destroy the information or transfer it to the appropriate DIA element.

Classified information is Government property and in no circumstances does it become the personal property of an individual. DIA personnel will not take classified information home for any reason.

Storage Requirements

The General Services Administration (GSA) sets minimum standards, specifications, and supply schedules for containers, vaults, alarm systems, and other security devices suitable for the storage and protection of classified material. Cabinets conforming to Federal specifications bear a test certification label on the locking drawer or outside of the top drawer. (On some older cabinets the label is affixed on the inside of the locking drawer compartment.) There will be no external marking on a security container showing the level of classified information stored therein.

TOP SECRET. Store TOP SECRET material in:

- A GSA-approved security container with a Group 1R, three-position, dial-type combination lock or other approved lock. Within closed-storage SCIFs in the DIAC and (b)(3):10 USC 424 TOP SECRET material may be stored in locked filing cabinets. Within open-storage SCIFs, TOP SECRET may be stored as any other classified document.

- An alarmed area that affords protection equal to or better than a GSA-approved security container. The physical barrier must be such that forcible attack will result in evidence of attempted entry into the room or area. The alarm system must provide immediate notice to a security force of attempted entry.

SECRET and CONFIDENTIAL. This material may be stored in:

- The manner prescribed for TOP SECRET.

- A Class B vault or a vault-type room or strongroom.

- A steel filing cabinet having a built-in, three-position, dial-type combination lock (until these cabinets are phased out).

- An existing steel filing cabinet equipped with a steel lock bar, provided it is secured by a GSA-approved changeable combination padlock. The keeper(s) and staple(s) must be secured to the cabinet by welding, rivets, or peened bolts. This storage should be used as a last resort and only within secure areas.

Storage areas for bulky SECRET and CONFIDENTIAL material will have access openings secured by GSA-approved changeable combination padlocks or key-operated padlocks with high security cylinders. *Key-operated high security padlocks will not be used within DIA without*

written approval of [redacted] When using approved key-operated high security padlocks, follow these security procedures: (b)(3):10 USC 424

- Appoint a key and lock custodian to ensure proper custody and handling of keys and locks.

- Control the keys as classified information with classification equal to the highest classification of the information being protected.

- Maintain a key and lock control register to identify keys for each lock and their current location and custody; master keying is prohibited.

- Store keys and spare locks in a secure container; keys will not be removed from the premises.

- Inventory keys and locks each month and with each change of custodian.

- Change or rotate locks at least annually and replace them upon loss or compromise of their keys.

Combinations

Combinations carry a security classification equal to the highest classified information authorized to be stored therein. Access to the combination will be given only to those individuals who are authorized access to the information. DIA Special Agents are authorized access to all vault and secure area combinations for the purpose of conducting after-hours security inspections and official investigations.

Changing Combinations. Combinations to security containers and entrance doors will be changed by individuals assigned that responsibility, who have appropriate security clearances. Contact [redacted] for assistance from the DIA locksmith or the contractor locksmith. Change combinations: (b)(3):10 USC 424

- When container is placed in use.

- When an individual knowing the combination no longer requires access.

- When the combination has been subject to possible compromise.

- At least annually. (Change combinations to containers storing cryptographic or NATO material at least semiannually.)

- When taken out of service. Reset built-in combination locks to the standard combination 50-25-50; combination padlocks to the standard combination 10-20-30.

Mark the standard combination on a tag or masking tape securely fastened to the container or padlock.

Recording the Combination. Individuals shall not retain combinations in writing; combinations may be kept only in authorized containers. Use Standard Form 700 (Security Container Information) to record information about the vault or security container. Follow the instructions printed on the SF 700 and forward Part 2 of the form within one workday to the appropriate central repository listed below:

(b)(3):10 USC 424

- DIAC: DIAC Security Control,
- Pentagon:
  - Command Element:
  - Others: DIA (b)(3):10 USC 424
- (b)(3):10 USC 424
- DIA and other remote locations: DIA guard posts.
- DIA Special Access Programs: DIAC.

Lock-out and Repair of Containers

(b)(3):10 USC 424 Contact for contractor service to repair security containers or to open a container because of lock-out. If a lock-out occurs because the custodian failed to store the combination in established combination repositories, the Division Chief, or higher, will conduct an inquiry to determine any negligence or pecuniary liability for the costs to the Agency of neutralizing the lock-out and repairing or, if necessary, replacing the container. Forward reports of inquiries to (b)(3):10 USC 424 and an information copy to

(b)(3):10 USC 424 Repair of damage which affects the integrity of a security container will be by appropriately cleared or continuously escorted personnel specifically trained in the approved methods. DoD 5200.1-R, "Information Security Program Regulation," contains procedures for properly repairing damaged security containers.

Opening, Closing, and Checking Security Containers

Affix a Standard Form 702 (Security Container Check Sheet) to each security container. At the end of each day, one person will lock the security container, and another person will double check it. During non-duty hours, the person locking a security container will make all reasonable attempts to obtain the assistance of a second person to double check the security container. If such assistance is not available, the person locking the container will wait one to two minutes and then perform the double check.

Opening. Complete the "Opened By" column of SF 702 each time the container is unlocked.

Closing. To secure the container:

- Close all drawers (close the combination drawer last).
- Engage the locking mechanism on the combination drawer.
- Slowly turn the combination dial at least four complete turns in one direction.
- Attempt to open all drawers while holding the combination drawer handle down.
- Complete the "Locked By" column of the SF 702.

Checking.

- Slowly turn the combination dial at least four complete turns in one direction.
- Attempt to open all drawers while holding the combination drawer handle down.
- Complete the "Checked By" column of SF 702.

If a security container was not opened during a duty day, the person charged with locking the security container will attempt to open the drawers while holding the combination drawer handle down; write "Not Opened" in the "Opened By" column, and complete the "Checked By" column.

If, at any time, a security container must be left unattended, it will be locked and double checked. However, a double check is not required in case of emergencies such as fire or bomb threats.

Security Container Turn-In

Prior to turn-in or transfer of furniture or containers used to store classified materials, thoroughly search the item to ensure it does not contain classified material. As appropriate and necessary, remove drawers and search the drawer compartment and other recesses. Complete a DIA Form 169 (Certificate of Inspection) and attach it to the equipment or furnishing. Reset the combinations on safes; see "Changing Combinations," above.

Vacating Secure Office Spaces

When a DIA element vacates an existing office space, all classified material must be properly transferred or disposed of. Notify [redacted] at least two weeks in advance of scheduled move

(b)(3):10 USC 424

to arrange a security inspection. Elements will provide sufficient personnel to augment [redacted] directed security inspections. (b)(3):10 USC 424

Before vacating, the last occupant will thoroughly inspect all spaces and remaining equipment and furniture for any classified material which may have been overlooked. Inspections will include visual observation of furniture/equipment interiors, through removal of drawers if necessary. Use DIA Form 169 to certify each piece of equipment or furniture is free of classified material. An appointed element representative will double check each piece of equipment or furniture and sign the DIA 169.

(b)(3):10 USC 424 **POC:** [redacted]

Chapter 7

PHYSICAL SECURITY

Contents

	Page
Policy	7-1
Building Security	7-1
Alarm Systems	7-3
Security of Classified Meetings	7-5

Policy

- Each DIA facility will establish an inspection program to encourage compliance with this handbook and security regulations.

- Safes, file cabinets, storage facilities, and personal property within DIA workspaces are subject to inspection for security, health, safety, and for other official purposes.

  Alarm equipment for protection against unauthorized or forced entry will be kept to a minimum consistent with the operational requirements of the DIA element concerned.

Building Security

The inspection program at each DIA facility helps to deter and detect unauthorized introduction or removal of classified information and contraband, such as firearms. DIA personnel located in other Government facilities will comply with that facility's inspection program.

DIA employees who need to remove classified information from a DIA facility will be issued a DIA Form 42-A (Courier Authorization). However, possession of a courier authorization card will not preclude a person from undergoing package inspection.

Package Inspections. Inspections will be limited to that which is necessary to determine if classified material or contraband is contained in briefcases, luggage, athletic bags, packages, or similar containers being taken into or removed from DIA premises.

During 0600 to 1800, Monday through Friday, security personnel conduct package inspections on a random, irregular basis. During 1800 to 0600 and weekends and holidays, inspections are conducted on a continuous basis at all entry/exit points, and include everyone entering or leaving a classified work area of a facility owned or leased by DIA.

Work Area Inspections. DIA work areas and equipment are subject to inspection. DIA work areas include all locations to which personnel have been granted access for performance of duties. Equipment includes computers, computer equipment and disks, safes, desks, file cabinets, bookcases, other storage facilities, and any other equipment located in the work area.

Personal property brought into DIA workspaces is subject to inspection by appropriate DIA management or security officials.

Inspections may extend to private property, including, but not limited to, computer disks, briefcases, tool boxes, luggage, packages, carrying cases, bags, and nonofficial documents brought into a DIA workspace. All items present in a DIA work area are subject to being seized, inspected, read, and analyzed. Property determined by the inspecting official to be inappropriately within a DIA work area may be secured. Evidence of regulatory or legal misconduct will be subject to review and action by administrative and/or legal authorities.

Property Pass. Removing Government property or personal property not accompanied by a sales document or proof of ownership requires a property pass (Optional Form 7). Obtain the property pass from the element's property custodian or from [redacted] (b)(3):10 USC 424

Prohibited Items. Because of the sensitivity of the work DIA employees perform, certain items are prohibited in DIA workspaces. These items are:

- Personally-owned photographic, video, and audio recording equipment. As an exception, personal cameras may be brought into DIA areas if:
  - An official event such as an awards ceremony is taking place and no official photographer is available.
  - The element chief with responsibility for the area(s) involved authorizes the introduction in writing.
  - Sufficient measures are taken to preclude the deliberate or inadvertent photography of classified information.
  - [redacted] concurs in writing with the above. In the Pentagon, obtain authorization from the Director, Washington Headquarters Service. (b)(3):10 USC 424
- Personally-owned computers and associated media.

Allowable Items. Certain personally-owned electronic equipment is permitted in DIA workspaces; however, the equipment is not to be routinely carried into and out of the workspace due to the possibility of technical compromise. Any electronic equipment introduced into DIA