

# **BALLISTIC MISSILE DEFENSE ORGANIZATION**

## **BMDO COUNTERMEASURES INTEGRATION PROGRAM SECURITY CLASSIFICATION GUIDE**

**BMDO DIRECTIVE NO. 5233R  
March 1995**

**Local reproduction authorized -  
distribution authorized to the Depart-  
ment of Defense and DoD contractors  
only, information protected by  
specific authority, June 1994.**

**This document contains information  
exempt from mandatory disclosure under  
the Freedom of Information Act, 5 USC  
522 (b) (2).**

### **FOR OFFICIAL USE ONLY**

**OFFICE OF PRIMARY RESPONSIBILITY: SECURITY, INTELLIGENCE AND COUNTERMEASURES**

March 1995

FOREWORD

1. DESCRIPTION. The Ballistic Missile Defense Organization (BMDO) Countermeasures Integration Program identifies innovative concepts of how adversaries might attempt to overcome the BMDO missile defense systems; analyzes these concepts through technical studies, modeling, and Red/Blue interchanges; and designs and conducts hardware tests where necessary to investigate feasibility and effectiveness issues. This program is intended to examine and evaluate the possibilities and likelihood of systems, forces, tactics and strategies beyond the established threat parameters that may be used against a BMDO missile defense system.
2. AUTHORITY. This Security Classification Guide (SCG) is issued under authority of Department of Defense (DoD) Regulation 5200.1-R, BMDO Directive Number 5200, and DoD Directive 5141.5.
3. This guide is effective immediately.

APPROVED BY:

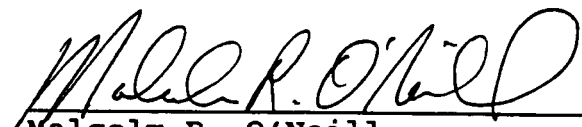
  
\_\_\_\_\_  
Malcolm R. O'Neill  
Lieutenant General, USA  
Director

TABLE OF CONTENTS

SECTION	TITLE	PAGE
I.	GENERAL	
I.1	Purpose	4
I.2	Authority, Applicability, and Scope	4
I.3	Office of Primary Responsibility	4
I.4	Policy	4
I.5	Operations Security	6
I.6	Program Protection Plans	7
I.7	Reproduction and Dissemination	8
I.8	Public Release	8
I.9	Unclassified Technical Data	9
I.10	Foreign Disclosure	10
I.11	Special Access Programs, Sensitive Compartmented Information, and Limited Dissemination Programs	12
I.12	For Official Use Only Caveat	13
I.13	Definitions	13
I.14	Related Classification Guides	16
I.15	Information Not Covered by this Guide	16
I.16	Classification Recommendations	17
I.17	Declassification	17
I.18	Problems/Conflicts	17
II.	TOPICS OF CLASSIFICATION	
II.1	General	18
II.2	Research/Technology	23
II.3	U.S. and Adversary Systems	30
II.4	Operational Factors	33
II.5	Basic Experiment Factors	33
II.6	Non-Military Factors	41
ATTACHMENT 1:	Related Publications	1-1
ATTACHMENT 2:	Distribution	2-1

SECTION I

GENERAL

1. PURPOSE

To provide instructions and guidance for the application of uniform security classification measures to information pertaining to ballistic missile defense countermeasures research, programs, projects, plans, systems, and related technology. This Security Classification Guide (SCG) supersedes the SDI Countermeasures Program Security Classification Guide dated November 1990.

2. AUTHORITY, APPLICABILITY, AND SCOPE

This guide is issued under the authority of DoD Regulation 5200.1-R, Information Security Program Regulation, and DoD Directive 5141.5, Ballistic Missile Defense Organization (BMDO). It applies to all programs, research, analysis, tests, experiments, and reports funded by or under the cognizance of the BMDO Countermeasures Integration Program. This guide does not, and is not intended to, preclude an individual evaluation from requiring greater protective measures than those described herein as each element may be uniquely sensitive and may be protected to a different degree.

3. OFFICE OF PRIMARY RESPONSIBILITY

This guide is issued by the BMDO and any inquiries concerning content and interpretation should be addressed to the:

Ballistic Missile Defense Organization  
Attention: DSIM  
7100 Defense Pentagon  
Washington, D.C. 20301-7100  
Tel: DSN 224-5277  
Commercial (703) 614-5277

4. POLICY

Over the past several years the BMDO, formerly known as the Strategic Defense Initiative Organization, has made significant

progress in extending the United States' technological base. This has accelerated development of the BMD program and provided the hope for important economic benefits for the nation. A major contributor to this accomplishment is the openness of BMD research and the excellent cooperation between BMDO and the supporting scientific community, both domestically and internationally. Recognizing the immense value of this information sharing and open exchange, classification should be avoided in the fundamental research area, to the maximum extent possible. BMDO is committed to maintaining this openness.

Within the context of this commitment, however, BMDO must protect information within the research, development, testing and evaluation process related to military operational capabilities, performance of planned or developing systems, or unique technologies critical to the BMD program. BMDO shall, therefore, apply appropriate classification controls on the disclosure of such information. In addition, as BMD progresses, it will be necessary to apply strict control over technical solutions that are developed and the circumstances under which they could be applied. It is more important to protect those items which an opponent cannot easily find out for himself, such as battle tactics, than it will be to protect those things that will become obvious when a system is deployed, although frequently these may require predeployment protection.

In accordance with this basic policy, it is the intent of this classification guidance to safeguard:

a. Detailed quantitative and qualitative information, to include: performance capabilities, design specifications; parameters, schedules, and dates, pertaining to specific applications; status of development efforts, direction of effort in specific DoD weapon system development programs; and resource expenditures that, because of degree or future projections, reveal the foregoing items.

b. Information concerning breakthroughs and significant technical advances in the area of military systems or space applications programs encompassed by the BMD until evaluated against other topics of this guide.

c. Technical information that could provide another country with significant assistance in the development of similar equipment, thus reducing the requirement for commensurate expenditure of resources compared to United States efforts and reducing U.S. lead time advantage.

d. Information that could significantly assist a potential enemy in the quantitative or qualitative assessment of actual or planned BMD related military or space applications.

e. Quantitative test results from any weapon-like test bed, prototype, or operational weapon system related to the BMD.

f. Information, including test results and theoretical analyses, concerning damage to and vulnerability of, military systems.

g. Quantitative information concerning the development of countermeasures or counter-countermeasures to the extent that it reveals current U.S. concerns or judgments regarding the vulnerability, applications, and efficiency of BMD related systems.

h. Intelligence and threat data that drive BMD research, design, and policy.

## 5. OPERATIONS SECURITY

The President of the U.S. signed a National Security Decision Directive (NSDD), NSDD 298, to establish a National Operations Security Program in 1988. The NSDD directed that all federal agencies implement their own operations security (OPSEC) program. In DoD, operations security programs and procedures to protect classified matters already exist and are governed by DoD Directive 5205.2, DoD Operations Security. However, information generally available to the public as well as certain detectable activities reveal the existence of, and sometimes details about, classified or sensitive information or undertakings. Such indicators may assist those seeking to neutralize or exploit U.S. Government actions in the area of national security. Application of the OPSEC process promotes operational effectiveness by helping prevent the inadvertent compromise of sensitive or classified U.S. Government activities, capabilities, or intentions.

The OPSEC process involves five steps: identification of critical information; analysis of threats; analysis of vulnerabilities; assessment of risks; and application of appropriate protective measures. The process begins with an examination of the totality of an activity to determine what exploitable but unclassified evidence of classified activity could be acquired in light of the known collection capabilities of potential adversaries. Such evidence usually derives from openly available data. Certain indications may be pieced

together or interpreted to discern critical information. Indicators most often stem from the routine administrative, logistical, physical or technical actions taken to prepare for or execute a plan or activity. Once identified, they are analyzed against the threat to determine the extent to which they may reveal critical information. The analysis has two principal results:

a. Security Countermeasures. These are the adjustments made in operations to avoid giving Foreign Intelligence Services (FIS) and other potential adversaries an opportunity to obtain classified information. They also include the adjustments made in the application of traditional security measures to deny or impede FIS access to classified information.

b. Compilation. Rigorous examination of the cumulative sensitivity of all information known or believed to be available to FIS to identify that information or operation which, although not intrinsically sensitive, must be classified to prevent FIS from obtaining or inferring classified information. If the individual elements of information explicitly or implicitly reveal classified information because of the total content or association, FIS will obtain the information and exploit it. The purpose of the OPSEC analysis is to identify those elements of information or operations before they are exposed to FIS and appropriately classify or protect them.

OPSEC is a systematic and proven process by which the U.S. Government and its supporting contractors can deny potential adversaries information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive Government activities.

## 6. PROGRAM PROTECTION PLANS

A 1990 DoD report on security identified vulnerabilities to exploitation by foreign intelligence and other foreign collection activities within the acquisition process. As a result of the study, the Secretary of Defense directed management initiatives to reduce the security vulnerabilities. To meet this requirement, in February 1991, DoD revised its acquisition directives to require that each acquisition program develop and maintain a Program Protection Plan to protect Essential Program Information, Technology, and Systems (EPITS). The EPITS are sensitive, unclassified or classified information, technologies, and systems of a DoD acquisition program, that, if modified,

compromised or destroyed, would degrade the effectiveness or shorten the expected effective operational value of the system.

A Program Protection Plan identifies the EPITS requiring protection for a specific program. It creates an integrated management plan permitting time-phased implementation of specific security measures for the protection of EPITS throughout the acquisition process. A security classification guide is an example of a security measure developed in support of a program protection effort. It must be used in conjunction with other program documents for an integrated protection program. For additional information regarding the Program Protection Plans, contact BMDO/DSIS.

## 7. REPRODUCTION AND DISSEMINATION

Authority is granted to reproduce this guide, in whole or in part, for application by activities involved in this program, including industrial activities. Dissemination is limited to the Department of Defense and DoD contractors and subcontractors.

## 8. PUBLIC RELEASE

The fact that this guide shows certain information to be unclassified does not allow automatic public release of such information. Separate from classification, there are other reasons why information may not be releasable, e.g., under the authorized exemptions of the Freedom of Information Act (FOIA) or under the provisions which apply to technical or other export controlled data. Proposed public disclosures of unclassified information pertaining to BMDO shall be processed through public affairs channels for approval for publication/ presentation. Contractors will submit public release requests through their BMDO contracting officer. The FOIA requests will be processed through established FOIA channels as described in DOD Regulation 5400.7-R and BMDO Directive 5400, Freedom of Information Act.

a. Any proposed release into the public domain of information pertaining to the Countermeasures Integration Program will be forwarded to the Assistant Director for Countermeasures (BMDO/DSIM) for review and further processing. Any information for release which falls under the purview of other federal components (e.g., Army, Air Force, Department of Energy, etc.) must be submitted to their respective public affairs office, who, in turn will submit the information to BMDO/DSIM, if appropriate. The term release includes, but is not limited to, news articles, contract announcements, advertisements, brochures, photographs, motion picture films, scripts, technical papers, speeches,



displays, etc., on any phase of this program. Contractors and participating agencies are responsible for screening information prior to submission and for certifying in their transmittal letters that material is unclassified, technically accurate, and suitable for public release. Material should be submitted in five copies 30 calendar days prior to desired presentation/publication date when intended for domestic release; and in five copies 45 calendar days prior to desired presentation/publication date when intended for foreign release. Transmittal letters also must identify the contract number, type of materials, proposed use, and valid suspense date, if applicable. Internal distribution of the material must be extremely limited and strictly controlled until review is completed.

b. Prior coordination with BMDO/DSIM is required for replies to queries and proposed visits by news media representatives to contractor or operating facilities when the subject of interest involves this program.

c. Only information that has been reviewed and certified for public release may be released. The decision to release such information falls within the purview of BMDO officials who have the responsibility to govern the program for which the material was developed.

d. Information previously cleared for public release may be released without obtaining additional approval. However, new, modified, or additional information developed after the initial clearance for public release requires additional review as outlined above.

e. Information that appears in the public media but has not been officially released may not be confirmed or denied unless approval is obtained through the above public release procedures.

## 9. UNCLASSIFIED TECHNICAL DATA

The Secretary of Defense has statutory authority to withhold from public disclosure certain unclassified technical data with military or space application. DoD Directive 5230.25, Withholding of Unclassified Technical Data for Public Disclosure, sets forth the policies, procedures, and responsibilities for withholding such data. DoD Directive 5230.24, Distribution Statements on Technical Documents, established the marking system for technical documents. In general, unclassified technical data may be withheld from public disclosure when the following

criteria are met. The material: (1) Is in the possession of or under the control of the Department of Defense; (2) Has military or space application; (3) May not be exported lawfully without an approval, authorization, or license under U.S. export control laws; and (4) Discloses critical technology.

BMDO programs and projects are deeply involved in advanced technology, much of it critically important to future defense systems, even though unclassified. The program established by the directives cited above is aimed at protecting such technology from uncontrolled public disclosure and foreign access. At the same time, it provides mechanisms for supplying the data to qualified U.S. firms or institutions for such legitimate purposes as performing on contracts, bidding on contracts, or conducting scientific research. Persons working with BMDO technical documents must be familiar with the control, marking, and distribution procedures. DoD Pamphlet 5230.25-PH, Control of Unclassified Technical Data with Military or Space Application, describes these in layman's language. SDIO Countermeasures Program Guidance for Distribution Statements on Technical Documents, dated August 1990, provides guidance to managers of BMDO/DSIM funded efforts on appropriate distribution statements for technical documents.

## 10. FOREIGN DISCLOSURE

BMD planning includes provisions for substantial foreign participation. Special care must be exercised to assure that each foreign disclosure action is fully in accordance with the National Disclosure Policy (NDP-1) and DoD Directive 5230.11, Disclosure of Classified Military Information to Foreign Governments and International Organizations (BMDO Directive 5210).

A decision to disclose or deny BMDO countermeasures classified and unclassified information of military and commercial application to a foreign government or international organization shall be made only by those BMDO officials specifically delegated disclosure or denial authority, once they have determined that all provisions outlined in BMDO Directive 5210 have been addressed. The BMDO classified information or material authorized for disclosure shall be transmitted to the intended foreign recipient only through government-to-government channels.

Any proposed agreement by the U.S. to exchange BMDO countermeasure information with foreign governments or international organizations will be forwarded through existing

channels, with appropriate justification, to BMDO/ DSIS and DSIM for approval. Each proposed foreign disclosure involving ballistic missile defense information will be coordinated with BMDO/DSIS. All communications to the BMDO concerning foreign disclosure matters should be addressed to the attention of BMDO/DSIS and DSIM.

All elements of BMDO shall ensure the issue of foreign participation is considered for each program. An analysis shall be made of the extent to which classified information and unclassified export-controlled technical information will be required for Allied participation. Where this analysis reveals a potential for Allied participation, foreign disclosure guidelines must be developed and approved prior to the procurement solicitation date.

In addition, Article IX of the May 26, 1972, Anti-Ballistic Missile Treaty (ABM) places special restrictions on foreign disclosure. It precludes disclosure to foreign nations of technical descriptions or blueprints specially worked out for the construction of ABM systems and components limited by the Treaty. Among the restrictions imposed by the Treaty are:

#### Article IX

To assure the viability and effectiveness of this Treaty, each Party undertakes not to transfer to other states, and not to deploy outside its national territory, ABM systems or their components limited by this Treaty.

#### Interpretation G

The Parties understand that Article IX of the Treaty includes the obligation of the U.S. and U.S.S.R. not to provide to other states technical descriptions or blueprints specially worked out for the construction of ABM systems and their components limited by the Treaty.

The restrictions imposed by the ABM Treaty include the obligation not to provide ABM information to other countries. This restriction includes classified ABM information, materials, drawings, technical descriptions, construction information, and ABM system components, to include similar classified information. Such documents shall be declassified only upon notification from the Director, BMDO.

The Missile Technology Control Regime (MCTR) are guidelines which control the transfer of equipment and technology which

could be used to develop a nuclear weapons delivery system by nations not party to the MCTR. Items subject to control include complete rocket systems and subsystems (ballistic missiles, space launch vehicles, and sounding rockets) and unmanned air vehicle systems and subsystems (cruise missiles and drones) capable of delivering at least a 500 kilogram payload to a range of 300 kilometers.

#### 11. SPECIAL ACCESS PROGRAMS (SAPs), SENSITIVE COMPARTMENTED INFORMATION, AND LIMITED DISSEMINATION PROGRAMS

In exceptional cases, even the strictest application of need-to-know will not provide adequate security, and special access controls must be applied. The requirements for special access programs are set forth in Chapter XII, DoD 5200.1-R, DoD Directive 5205.7, and BMDO Directive 5202. Such programs may be established only when it is clearly shown that:

a. Normal management and safeguarding procedures are not sufficient to limit need-to-know or access; and

b. The number of persons who will need access will be reasonably small and commensurate with the objective of providing extra protection for the information involved.

SAPs that are managed or funded by BMDO require a review by the BMDO SAP Oversight Committee (SAPOC). The Deputy Secretary of Defense (DEPSECDEF) is the approval authority for DoD SAPs. The single point-of-contact within the BMDO for information concerning the establishment and security administration of SAPs is the Assistant Director for Security (BMDO/DSIS). When the need for a Special Access Program is perceived, early coordination with BMDO/DSIS is critical so that the steps can be taken to obtain DEPSECDEF approval and develop the necessary classification guidance, security procedures, and funding authority. Any instance in which a SAP has been established without proper authority will be reported promptly to BMDO/DSIS so that action can be taken to terminate it or, if justified, to process it for approval. SAPs originated by Executing Agencies will be established in accordance with applicable regulations.

A Limited Dissemination (LIMDIS) program imposes controls to enhance normal requirements for access to CONFIDENTIAL, SECRET, or TOP SECRET information that are less stringent than SAP controls. LIMDIS controls are the only security enhancement short of a SAP which may be employed for control over specific information for specified periods of time to enhance and formally

implement need-to-know requirements. Consult with BMDO/DSIS for further guidance on LIMDIS programs.

Sensitive Compartmented Information (SCI) is information and material that requires special controls for restricted handling within compartmented intelligence systems. The requirements for marking, handling, and protecting SCI are established in national and departmental intelligence directives that are available to persons who have been given specific access to SCI. Concerns regarding SCI should be addressed to the BMDO/DSIS Special Security Officer.

## 12. FOR OFFICIAL USE ONLY CAVEAT

For Official Use Only (FOUO) is not a security classification. Information that has not been given a security classification pursuant to the criteria in this guide, but which may be withheld from the public for one or more of the reasons cited in FOIA exemptions 2 - 9, DoD Regulation 5400.7-R, shall be considered as being For Official Use Only. Information designated in the remarks column of this guide that warrants FOUO markings will be handled and protected in accordance with the above cited regulation and BMDO Directive 5400.

All security classification guides which are under the cognizance of BMDO will be marked For Official Use Only, if the guide is unclassified. Classified security classification guides will be marked For Official Use Only if downgraded to unclassified. Security classification guides are in and among themselves not releasable to the public under the Freedom of Information Act.

## 13. DEFINITIONS (Refer to SDI-SE Lexicon, dated January 1989)

### a. Breakthrough

A situation in the course of Research and Development (R&D) when a technological development:

(1) Is imminent or achieved under circumstances that constitute a marked or sudden deviation from a trend; or

(2) Shows unexpected progress in relation to time not predictable qualitatively even by persons trained in the appropriate disciplines; or

(3) Exhibits an increase in performance or capability that appears to open up a field of application to a wide variety of new system uses.

b. Classified Defense Information

U.S. Government information which requires protection against unauthorized disclosure in the interests of national security, and which has been so designated in accordance with the provisions of Executive Order 12356: TOP SECRET, SECRET, CONFIDENTIAL.

c. Classifier

An individual who makes a classification determination and applies a security classification to information or material. A classifier may be a classification authority (e.g., Director, BMDO) or may derivatively assign a security classification based on a properly classified source or a classification guide.

d. Confidential

Information or material, the unauthorized disclosure of which, reasonably could be expected to cause damage to the national security.

e. Constellation Size

The number of defensive weapon satellites placed in orbit about the earth as part of a ballistic missile defense system.

f. Countermeasures

The employment of devices and/or techniques that has as its objective the impairment of the operational effectiveness of enemy activity.

g. Counter-Countermeasures

Measures taken by the defense to defeat offensive countermeasures.

h. Communications Security (COMSEC)

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

cryptosecurity, emission security, transmission security, and physical security of COMSEC material and information.

i. Formerly Restricted Data (FRD)

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

j. Restricted Data (RD)

All data concerning the (1) design, manufacture, or utilization of atomic weapons; (2) production of special nuclear material; or (3) use of special nuclear material in the production of energy, but not including data declassified or removed from the RD category under Section 142 of Public Law 83-703, Atomic Energy Act of August 30, 1954.

k. Secret

Information or material, the unauthorized disclosure of which, reasonably could be expected to cause serious damage to the national security.

1. Significant Technical Advance

Any characteristic of a concept, design, or component that;

(1) Offers a technical advance of enough magnitude to be potentially useful in an operational or advanced system.

(2) Results in a distinct military advantage in areas such as substantially improved performance, substantially increased reliability, or substantially reduced vulnerability.

m. Ballistic Missile Defense Program

A DoD program whose mission is to acquire and develop systems, elements, and architectures to achieve highly effective theater and national missile defense capabilities and to develop and demonstrate advanced technologies for advancing BMD systems. These developments will provide the basis for informed decisions regarding development, production and deployment milestones of

ballistic missile defenses. The program is managed and directed by the Ballistic Missile Defense Organization under the authority of DoD Directive 5141.5.

n. Survivability

The capability of a system to avoid or withstand hostile environments without suffering irreversible impairment or the ability to accomplish its designated mission.

o. System

A collection of elements capable of fulfilling a specified task.

p. Tempest

TEMPEST is an unclassified short name referring to investigation and studies of compromising emanations.

q. Top Secret

Information or material, the unauthorized disclosure of which, reasonably could be expected to cause exceptionally grave damage to the national security.

#### 14. RELATED CLASSIFICATION GUIDES

The officials responsible for programs, projects, plans, or systems that fall within the Countermeasures Integration Program or incorporate countermeasures technology must issue security classification guides that provide sufficient detail for their activities. These guides must be consistent with the policy and topics outlined in Sections I and II and the related publications listed in Attachment 1. To ensure this consistency, related guides will be coordinated with BMDO/DSIM prior to issuance.

#### 15. INFORMATION NOT COVERED BY THIS GUIDE

If a person who does not have original classification authority originates or develops information not covered by this guide but believed to require protection, that person shall safeguard the information in the manner prescribed for the anticipated classification level and forward it, in accordance with the procedures in paragraph 2-600, DoD Regulation 5200.1-R, to an original classification authority for evaluation. If such a query is sent to the BMDO, it should be addressed to the



attention of the BMDO/DSIS, which will coordinate with the appropriate original classification authority within the BMDO.

#### 16. CLASSIFICATION RECOMMENDATIONS

If the security classifications prescribed in this guide impose requirements that are impractical, or if a need for change to this guide is indicated due to the technological changes in the state-of-the-art, progress attained in the ballistic missile defense effort, or other factors, users of this guide should submit recommended changes, with justification, through appropriate channels to BMDO/DSIM. Pending final decision, information shall be handled and protected at the current classification level or the recommended change level, whichever is higher. All users of this guide are encouraged to assist in improving the guidance herein and in maintaining its currency.

#### 17. DECLASSIFICATION

The BMDO is a broad, expanding effort in a constantly changing field and long term significance of information to classified military and space operations is difficult to predict. For that reason, most of the classifications specified in this SCG reflect Originating Agency Determination Required (OADR) as declassification instructions. Nevertheless, some elements of information may be subject to declassification in a relatively short period. When it is known in advance that classification will no longer be required after a specific date or event, that date or event should be specified in program specific classification guides and original documentation.

Decisions to declassify or downgrade BMDO information must be coordinated with BMDO/DSIS. Only the Original Classification Authority may approve declassification/downgrading decisions for information under their cognizance. No decision to declassify or downgrade will occur until coordination with all perspective organizations who may be adversely effected by the decision has taken place. The information, once declassified or downgraded, must not jeopardize U.S. national security interests and must not provide a potential U.S. adversary a military or economic capability which could counter U.S. national security concerns.

#### 18. PROBLEMS/CONFLICTS

If problems or conflicts concerning classification of BMD-related information cannot be resolved promptly through normal channels, pertinent background information should be submitted to BMDO/DSIS for review and decision at the appropriate level.

SECTION II  
TOPICS OF CLASSIFICATION

TOPIC	CLASSIFICATION/ DECLASSIFY	REMARKS
1. GENERAL		
a. The fact that studies of possible adversary countermeasures (CMs) are underway	U	
(1) General statement of purpose of a specific BMDO program	U	Unless classified by program specific SCG.
(2) Identification of BMDO operational architectures to include general descriptions.	U	Such as NMD, TMD, and GMD.
(3) Identification of specific BMDO system elements and architectures.	U	Such as GBI, GBR, THAAD, Patriot, etc.
(4) General BMD system functions.	U	Normally unclassified. However, refer to program specific guidance.
(5) External views, photographs, artists concepts, drawings, etc., of BMD systems.	U	Provided that mission capabilities are not revealed.
(6) Drawings, artists conceptions, etc., of BMD architecture as portrayed in a defensive mode (i.e., NMD architecture).	U	Provided that system capabilities or other information classified by system specific SCGs or other guidance is not revealed.

TOPIC	CLASSIFICATION/ DECLASSIFY	REMARKS
(7) A description of the potential characteristics of BMD weapon systems, if limited to that which could easily be derived by physicists and engineers from well-known physical principles.	U	Unless information concerning nuclear weapons is involved, in which case refer to DOE/DoD guidance (e.g., CG-NDEW-1; CG-W-4/5, Revision 1).
(8) Potential capabilities or limitations of a technology selected for, or being considered for, BMD application.	S/ OADR	
(9) Quantified performance requirements, capabilities or limitations of a BMD system, such as GBI, GBR, etc.	S/ OADR	Such as ranges, intercept altitudes, engagement envelopes, dead zones, etc. System specific SCG may require higher classification.
(10) Detailed description of the ultimate goals, direction of effort, status of achievement and special applications of BMD programs.	S/ OADR	
b. Areas of CM studies		
(1) Expressed in terms of fields of technology; e.g., laser, NEMP, IR, particle beam.	U	Detailed statements which reveal characteristics of U.S. or threat systems may be classified.

TOPIC	CLASSIFICATION/ DECLASSIFY	REMARKS
(2) Expressed in terms of classes of components; e.g., ground-based sensors, space-based directed energy weapons, electronic countermeasures.	U	Quantitative statements of the effectiveness of these countermeasures may be classified.
(3) Expressed in terms of bands, energy levels, altitude ranges, or similar factors when these are openly known to be probable areas of interest and are not related to specific U.S. or adversary systems or their capabilities, vulnerabilities, or limitations	U	
(4) Expressed in terms of bands, energy levels, altitude ranges, or similar factors of interest and related to specific U.S. or adversary systems.	U-TS NOFORN/ OADR	If related to U.S. systems, refer to specific classification guides. If system capabilities, vulnerabilities, or limitations are revealed, classification is S/NOFORN. TS if required by a specific guide or if the information could be used to significantly degrade the effectiveness of a U.S. offensive or defensive system. If information on foreign systems is revealed, classify at level of intelligence source material.

TOPIC	CLASSIFICATION/ DECLASSIFY	REMARKS
c. List of Countermeasures	U-S/ OADR	A list of countermeasures ordered by type (e.g., jammers, decoys, flares), defense system function attacked (e.g., acquire, track, discriminate), or any other organizing principle(s) is unclassified so long as the list does not reveal relative or absolute importance in the view of BMDO or how effective particular countermeasures might be when used against particular defense systems or elements. If the list defines priority or importance to the Countermeasures Integration (CMI) Program, it is CONFIDENTIAL. If the list defines specific system application or describes countermeasures design or function, it is SECRET.
d. Funding		
(1) Funding for the overall CMI Program.	U	Breakdown by fields of technology or classes of components may require classification if they reveal particular concern or rate of progress. Accompanying descriptive data may require classification under other topics. Unclassified budget figures are For Official Use Only (FOUO).

TOPIC	CLASSIFICATION/ DECLASSIFY	REMARKS
(2) Outyear figures	U-C/ OADR	Overall CMI Program total, or a breakdown presented by types of efforts (e.g., experiments, database), is unclassified. Breakdown by specific technical efforts is CONFIDENTIAL. UNCLASSIFIED figures are FOUO.
e. List of contractors	U	However, descriptive data concerning contract effort may require classification under other topics if stated more specifically than area of technology or class of components.
f. Program schedules for development, validation, or assessment of countermeasure technology components or systems.	U-S/ OADR	CMI Program schedules are generally FOUO. Schedules are CONFIDENTIAL when they reveal countermeasure priority or importance in the CMI Program and SECRET when they reveal countermeasure specific system application or describe countermeasure design or function. Schedules which reveal BMD system acquisition milestones, deployment dates, or system capabilities shall be classified by specific program guides.

TOPIC	CLASSIFICATION/ DECLASSIFY	REMARKS
2. RESEARCH/TECHNOLOGY		
a. Basic Research	U-S/ OADR	Basic research usually is unclassified. However, classification (S/OADR) is required if the purpose and direction of the research would reveal ballistic missile defense vulnerabilities or critical limitations.
b. Research breakthrough	S/ OADR	A technological development that is a marked or sudden deviation from a trend, shows unexpected progress in relation to time not predictable by trained persons, or represents an increase in performance or capability with application to a wide variety of new military uses, is classified S/OADR pending evaluation by BMDO/DSIM.
c. Applied Research	U-S/ OADR	Applied research is classified or unclassified according to the subtopics below, other topics of this guide, and specific system guides.

For guidance on specific programs and areas of scientific research see SDI SCG, Directive No. 5230-M, June 1990 or relevant program guides.

TOPIC	CLASSIFICATION/ DECLASSIFY	REMARKS
(1) Significant Technical Advance	S/ OADR	A technical advance of sufficient magnitude to have potential for use in an operational or advanced system, resulting in distinctive military advantage.
(2) Research revealing capabilities, vulnerabilities, or survivability of U.S. or adversary systems.	U-TS/ OADR	Classify in accordance with subtopics under Topic 3, U.S. and Adversary Systems, starting on page 25.
(3) Research indicating potential for development of new U.S. counter-countermeasures.	U-S/ OADR	For guidance on specific programs and areas of scientific research, see SDI SCG, Directive No. 5230-M, June 1990 or relevant program guides.
(4) Concepts and Techniques		
(a) Basic concepts that draw only on scientific material readily available in open literature	U	However, classification is required if the parameters of the concept described are designed to coincide with classified characteristics of a U.S. system.
(b) Mathematical models and algorithms	U-S/ OADR	UNCLASSIFIED if developed entirely from unclassified U.S. or adversary systems. However, if parameters of a mathematical model are such that inferences can be drawn concerning classified characteristics of U.S. or adversary systems, the model



TOPIC	CLASSIFICATION/ DECLASSIFY	REMARKS
		must be classified accordingly per source guidance. Discrimination algorithms are SECRET or higher, in accordance with the system guide.
(c) Simulation Systems	U-S/ OADR	Simulation systems are classified at the same level as the item or function simulated. This is true regardless of the nature of the simulation (e.g., hardware, thermal, electromagnetic) and regardless of whether the simulation is of an actual or candidate system or subsystem
(d) Simulations and models that reveal sequencing and processing of threats depicting discrimination techniques, engagement logic, or firing data.	S/ OADR	S/FRD if nuclear weapon technology is involved.
(5) Design/Materials/Measurements		
(a) Types of material considered	U	If materials represent a research breakthrough, subtopic 2..a.(1) applies. If related to a specific system, subtopic (5) (d) below applies.
(b) Generic systems and components considered but not related to a specific BMDO segment or element	U	

TOPIC	CLASSIFICATION/ DECLASSIFY	REMARKS
(c) Hardening or survivability goals and achievements	S/ OADR	For classification of specific system implementation of survivability technologies and techniques, contact the BMDO Deputy for Technology.
(d) Nature and effectiveness of CM related to a specific system	S-TS/ NOFORN OADR	TOP SECRET if information can be exploited to significantly degrade the effectiveness of a U.S. offensive or defensive system. See remarks at 2.b. on page 20.
(e) Manufacturing or materials processing techniques specifically designed for CM or CCM.	S/ OADR	TS classification, FRD, RD, and WNINTEL caveats restricting dissemination may be required by source documents.
(f) Specific fabrication techniques for integration of hardened materials and concepts into hardened systems components.	S/ OADR	See remarks at subtopic (5)(e) above.
(g) Laboratory, ground, or flight test data on countermeasure:		
(1) Characterization data on small test samples	U-S/OADR	See remarks at subtopic (5)(e) above
(2) Performance data on components and systems	U-S/OADR	See remarks at subtopic (5)(e) above.
(3) CM verification data on full or reduced scale countermeasure	S-TS/ OADR	See remarks at subtopic (5)(e) above.

TOPIC	CLASSIFICATION/ DECLASSIFY	REMARKS
(h) Assessments of experimental data on the application of countermeasures to specific military systems that reveal the potential vulnerability of systems, subsystems, or components.	S-TS/ OADR	TOP SECRET if information can be exploited so as to significantly degrade the effectiveness of a U.S. offensive or defensive system.
(6) Low Observable and Counter Low Observable Efforts that affect radar and infrared signatures.	U-TS/ OADR	Classify in accordance with Low Observable (LO) and Counter Low Observable (CLO) Programs, DoD Instruction Number S-5230. 28, December 16, 1992, or other appropriate program or system classification guidance.
(a) Generally known techniques for signature reduction	U	Examples include background matching, shaping, energy absorption, or contrast reduction.
(b) General program description	U-S/ OADR	As determined by content and program classification guidance.
(c) General mission statements, such as, to <i>increase survivability, LO modifications must be considered for all DoD weapon systems.</i>	U	
(d) Requirements, specifications, operational capabilities, and concepts.		
- At U.S. BMD or countermeasure system level	S/ OADR	

TOPIC	CLASSIFICATION/ DECLASSIFY	REMARKS
- At Subsystem and component level	C/ OADR	
- Estimates or proven conclusions as to system capabilities and/or operational limitations other than vulnerability and survivability to specific defenses.	S/ OADR	Refers to capabilities and limitations that could be exploited by an adversary to gain advantage in a combat environment.
(e) Exterior configuration	U-S/ OADR	Depends on what technology is revealed by viewing exterior.
(f) Materials:		
- Commercial products and their mechanical, electromagnetic, thermal, acoustical, and other properties.	U	Commercial products are products developed with non-DoD funding primarily for nonmilitary applications.
- Raw materials used, and their mechanical, electromagnetic, thermal, acoustical, and other properties.	U	
- Materials to enhance LO performance or durability in military environments.	U-C/OADR	CONFIDENTIAL if process is revealed.
- Physical samples of operational hardware and R&D test models used for military observables reduction or control that reveal design features responsible for low signature	U-S/ OADR	Commercially available materials are unclassified until made into a unique part or test sample suitable for signature evaluation.

TOPIC	CLASSIFICATION/ DECLASSIFY	REMARKS
<ul style="list-style-type: none"> <li>- Radio frequency, electrical, electro-optical, mechanical, and acoustic properties and descriptions (calculated or measured) of military LO materials.</li> </ul>	S/ OADR	Military LO materials are materials developed with DoD funding primarily for military applications.
<ul style="list-style-type: none"> <li>- Mechanical, thermal, and other (non-signature) properties of military LO materials.</li> </ul>	C/ OADR	Unclassified when no indication of association with observables reduction.
(g) Design concepts		
<ul style="list-style-type: none"> <li>- Theoretical studies at level of basic science which simply apply or integrate generally know LO techniques.</li> </ul>	U	Unclassified, provided no association with military application is made. Otherwise, classify according to application.
<ul style="list-style-type: none"> <li>- Results of studies to assess the application of LO technologies that reveal capabilities, operational limitations, or vulnerability and survivability of conceptual system designs associated with military applications.</li> </ul>	S/ OADR	
<ul style="list-style-type: none"> <li>- Conceptual or general designs when identified as dedicated to signature control or reduced signature.</li> </ul>	C/ OADR	

TOPIC	CLASSIFICATION/ DECLASSIFY	REMARKS
- Detailed designs	S/ OADR	"Detailed design" is information sufficiently detailed to allow reproduction of the reduced observable design and/or design signature evaluation. For breakthrough designs, contact Component Director of LO and CLO for further guidance.
3. U.S. AND ADVERSARY SYSTEMS		
a. U.S. Systems		
(1) The fact that ballistic missile defense systems will be designed to defeat current and projected physical and electromagnetic threats	U	Without elaboration.
(2) Assumed threat and threat scenarios	U-TS/ OADR	Classified in accordance with source of information and to which system(s) the threat is applicable (see system specific SCG).
(3) Baseline threat, assessment and estimate of hostile missions required to overcome a defensive objective.	S-TS/ OADR	SCI and/or TS classification, FR, RD, and caveats restricting dissemination may be required by source document.
(4) Present and projected physical and electromagnetic threat.	S/ OADR	See above remarks.

TOPIC	CLASSIFICATION/ DECLASSIFY	REMARKS
(5) Specific characteristics and levels of threat that systems are or will be designed to survive.	S-TS/ OADR	According to individual system guide.
(6) Ballistic missile defense system effectiveness against a specific threat.	S-TS/ OADR	TS if countermeasure to effectiveness can exploit the survivability of a U.S. system.
(7) Vulnerability of a BMD system to possible countermeasures	S-TS/ OADR	Demonstrated vulnerability which could be exploited to seriously degrade or neutralize an entire defense system is TS, otherwise SECRET.
(8) Theoretical or experimental data which reveals the level of survivability of a ballistic missile defense system or component.	S-TS/ OADR	Includes communications links and equipment. TS if information can be exploited so as to defeat the survivability of a U.S. offensive or defensive system.
(9) Vulnerability and survivability measures employed on a BMD system.	S-TS/ OADR	TS if information can be exploited to defeat the survivability of a U.S. system, otherwise SECRET.
(10) Method or procedure by which a vulnerability can be exploited or overcome on a BMD system.	S-TS/ OADR	See above remarks and refer to specific system SCG.
(11) Performance capabilities or limitations of a system.	S-TS/ OADR	See above remarks.

TOPIC	CLASSIFICATION/ DECLASSIFY	REMARKS
(12) The fact that a ballistic missile defense system or component is or will be hardened.	U	Without reference to specific technologies or engineering estimates.
(13) Hardening or survivability goals and achievements.	S/ OADR	
b. Adversary Systems	U-S/ OADR	Classification levels generally are the same level as U.S. systems. However, the governing factor is classification of intelligence source material. Caveats restricting dissemination may apply.
(1) Current or postulated threat or threat target data.	S-TS/ OADR	SCI and/or TS if determined by source of information or TS if identified threat can defeat the survivability of a U.S. System.
(2) Foreign space and missile missions and design data.	S/ OADR	Unclassified if foreign country has openly released the information. May require higher protection if source of information deems necessary.
(3) Foreign test object characteristics.	S/ OADR	See above remarks
(4) Names and locations of foreign space and missile facilities.	S/ OADR	See above remarks.



TOPIC	CLASSIFICATION/ DECLASSIFY	REMARKS
4. OPERATIONAL FACTORS		
a. Generic factors that only contain data readily available from open sources and not related to a specific system; (e.g., ICBM flight time of 30 minutes; atmospheric density variation by altitude).	U	
b. Factors applied to a specific concept, system, or function (e.g., time lines, specific altitudes or areas, tactics, launch sequences, etc.).	S-TS/ OADR	TOP SECRET if required by specific system guides or if derived from TOP SECRET sources.

5. BASIC EXPERIMENT FACTORS

NOTE: This section provides basic security classification guidance for experiments conducted by or in support of the BMDO CMI Program. Officials responsible for experiments must review the basic guidance and issue supplemental security classification guidance as appropriate. Users of this SCG should consult specific guidance for each experiment.

a. General Mission Description

- |   |   |
|---|---|
| (1) The experiment name   | U |
| (2) The fact that testing of possible adversary countermeasures (CMs) are underway. | U |

TOPIC	CLASSIFICATION/ DECLASSIFY	REMARKS
(3) The fact that the named experiment is a general phenomenology-level test.	U	
(4) The fact that the named experiment is sponsored by the Countermeasures Integration Program (BMDO/DSIM)	U	
(5) The dates or times of flight tests and mission milestones from which one can deduce the launch date (see below).	U-S/ OADR	
- Experiment launch date or mission readiness dates from which one can deduce the launch date	U-S/ OADR	Classification of launch dates can range from U-S, as set by the specific experiment security classification guide and based on the results of the security threat assessment for that experiment. Prior to completion of the security threat assessment, the launch year and quarter of an experiment is U, the month is U and the date (or launch window) is S. The launch date is unclassified when disassociated from BMDO/DSIM sponsorship, the objective and experiment objectives. However, if BMD system IOC or FOC dates can be deduced from the test schedule, the schedule must be classified S.

TOPIC	CLASSIFICATION/ DECLASSIFY	REMARKS
- Experiment launch time of day.	U	
(6) The launch vehicle type (e.g., Terrier/Malamute combination, etc.) and performance parameters.	U-S/ OADR	UNCLASSIFIED for U.S. sounding rockets. SECRET for operational U.S. ICBMs. UNCLASSIFIED-SECRET for hardware acquired from foreign sources. Consult specific guidance for each flight test.
(7) Areas of CM testing:		
(a) Expressed in general terms of fields of technology being tested, e.g., maskers, ECM, decoys.	U	
(b) Expressed in general terms of targeted architectures, i.e., TMD, NMD.	U	
(c) Expressed in terms of data collection bands, altitudes, geometries, or similar factors.	U-S/ OADR	Consult specific guidance for each experiment.
(8) Countermeasures to be tested by name or numbers, e.g., inflatable balloon decoys, flares, chaff.	U-C/ OADR	Unclassified as a list of test objects, without reference to their estimated effectiveness, priority, or importance within the Countermeasures Integration Program. Consult specific guidance for each experiment.

TOPIC	CLASSIFICATION/ DECLASSIFY	REMARKS
(9) Characteristic comparisons between the target and threat.	S/ OADR	Comparison of unclassified target data with threat data is classified. Classify according to threat data source documents.
(10) Launch site, predicted booster and test object trajectories and body motions (state vectors)	U	
(11) Identification and number of target complex objects.	U-S/ OADR	Normally the number and identification of test objects is unclassified, but may be SECRET if the number of test objects is an integral part of a classified design.
(12) All experiment flight-event timelines and locations.	U-C/ OADR	UNCLASSIFIED provided launch date is not revealed. CONFIDENTIAL if timeline reveals significant facet of countermeasure.
(13) Experiment participants	U-S/ OADR	Usually the association of the programs participating in an experiment is unclassified. However, always consult specific guidance for each experiment.
(14) Funding	U	Unclassified budget year figures are FOUO.

TOPIC

CLASSIFICATION/  
DECLASSIFY

REMARKS

b. Test Objectives and Requirements

(1) Experiment objectives, when they express general, qualitative achievement of Countermeasures Integration Program mission functions, e.g.:

U

- To measure the radar and optical characteristics of flares.

- To investigate endoatmospheric flare phenomenology.

(2) Experiment objectives, when they reveal critical technical issues of the Countermeasures Integration Program regarding the feasibility of countermeasure concepts or approaches.

C-S/  
OADR

CM test objectives are CONFIDENTIAL whenever they reveal the key issues regarding development of effective countermeasures to a ballistic missile defense system. Objectives are SECRET when they reveal quantitative performance characteristics or limitations of the BMD system.

(3) Quantitative definition of critical technical issues of the Countermeasures Integration Program.

S/  
OADR

CM test requirements are SECRET whenever they quantify the projected performance, or the achievable performance limits, of potential adversary CM threats.

TOPIC	CLASSIFICATION/ DECLASSIFY	REMARKS
(4) Explicit or quantitative definition of CM performance requirements as driven by ballistic missile defense system capabilities or vulnerabilities.	S/ OADR	CM test objectives are classified SECRET whenever they define, or from which one can infer, ballistic missile defense system capability or vulnerability limits.
c. Signature Predictions		
(1) Radiometric characteristics of all test objects, in general.	U-S/ OADR	UNCLASSIFIED, except when they are expressed in terms that correlate with classified architecture or program parameters, then SECRET (see 5a(7) and 5a(9), on pages 29 and 30).
(2) Expressed in terms of achievable threat CM performance.	S/ OADR	See 5b(3), above.
(3) Expressed in terms of defense system capability to handle.	S/ OADR	See 5b(4) above.
d. Flight Conditions		
Weather, such as atmosphere or sea conditions, quantitatively or qualitatively.	U	
e. Go/No-go Launch Criterion in general		
	U-C/ OADR	UNCLASSIFIED, except when they conflict with other sensitive mission aspects, such as classified parameters or disposition of experiment participants. Consult specific guidance for each experiment.

TOPIC	CLASSIFICATION/ DECLASSIFY	REMARKS
f. Flight Test Operations		
(1) Range support configuration, such as sensor locations or engagement geometries and distances.	U-S/ OADR	UNCLASSIFIED, except when they are expressed in terms that correlate with sensitive architecture or program parameters, then SECRET. Consult specific guidance for each experiment.
(2) RF operations for range radars, communication links, and telemetry (TM) relays (including signal strengths, frequencies, bandwidths, etc.)	U	
(3) Whether or not the experiment telemetry data is encrypted.	U	
g. Flight Test Hardware		
(1) Physical characteristics of all platform hardware, including attitude control system and booster payload section, except for the payload.	U	Consult specific guidance for each experiment. The subtopics in this section are examples only.

TOPIC	CLASSIFICATION/ DECLASSIFY	REMARKS
(2) Physical characteristics of decoys, both instrumented and uninstrumented.	U-S/ OADR	The measured moments of inertia of the decoys, including distribution of the instrumentation system components for instrumented decoys, are CONFIDENTIAL. Other parameters, such as weights, materials, or visual appearance, are unclassified. Design information sufficiently detailed to allow reproduction of a flight test object (e.g., decoy, flare) or evaluate its performance is classified SECRET.
(3) Payload hardware.	U-S/ OADR	Usually, payload hardware should be handled as For Official Use Only materials. Classification guidance for a particular experiment may require a classification of CONFIDENTIAL or SECRET.
(4) Exact chemical makeup of active flare materials.	U-C/ OADR	Identity of chemical components is UNCLASSIFIED. Percent composition of the chemicals in the mixture is CONFIDENTIAL.
h. Flight Experiment Data		
(1) Health and status data.	U-S/ OADR	Normally, classified SECRET for operational systems; UNCLASSIFIED for applied research or Dem/Val programs. Consult specific guidance for each experiment.



TOPIC	CLASSIFICATION/ DECLASSIFY	REMARKS
(2) Raw telemetry data not in engineering units.	U	
(3) Reduced signature data collected on the experiments by primary range or associated sensor operations.	U-S/ OADR	Consult specific guidance for each experiment.
(4) Tracking and telemetry data which reflects performance data in engineering units.	S/ OADR	
(5) Data analyses results, findings.	U-S/ OADR	Data analysis will be classified according to the sensitivity of the results, as per SDI Security Classification Guide, Directive Number 5230-M, June 1990. In addition, analyses will conform to the classification guidance of the originating collection asset, when continued sensitivity is directed. Consult specific guidance for each experiment.

**6. NON-MILITARY FACTORS**

Note: Non-military items could have relevance to issues regarding proliferation and the capability of rest-of-world (ROW) countries (e.g., technology transfer, import and export, economics, alliances, etc.).

TOPIC	CLASSIFICATION/ DECLASSIFY	REMARKS
a. Domestic	U-S/ OADR	Raw data used to study domestic factors will be classified or unclassified on the basis of data sources. Studies derived from unclassified data may require classification under other topics if they present conclusions, involve comparisons with classified data, or present recommendations on how to proceed with future actions or research.
b. International	U-S/ OADR	See remarks under Topic 1 and a. above. Data pertaining to international factors will be classified more often than that dealing with domestic factors and caveats placing special restrictions on dissemination may apply.

RELATED PUBLICATIONS

- A. Executive Order 12356, *National Security Information*
- B. National Security Decision Directive 189
- C. National Security Directive 298, *National Operational Security Program*
- D. Atomic Energy Act of 1954.
- E. The 26 May 1972 Anti-Ballistic Missile Treaty (ABM)
- F. Director of Central Intelligence Directive 1/7, *Security Controls on the Dissemination of Intelligence Information*
- G. National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations (Short Title: National Disclosure Policy (NDP-1)).
- H. Amendment to DoD Space Policy of 4 February 1987, 15 December 1992 (Implemented by BMDO Memorandum, Implementation of Amendment to DoD Space Policy of February 4, 1987, February 15, 1993).
- I. DoD Directive 5141.5, *Ballistic Missile Defense Organization*
- J. DoD Handbook 5200.1-H, *DoD Handbook for Writing Security Classification Guidance*
- K. DoD Index 5200.1-I, *Index of Security Classification Guides*
- L. DoD Directive 5200.1-R, *Information Security Program Regulation*, (BMDO Directive 5200)
- M. DoD Directive 5000.1, *Defense Acquisition*
- N. DoD Directive 5000.2, *Defense Acquisition Management Policies and Procedures*

ATTACHMENT 1

- O. DoD Directive 5205.2, *DoD Operations Security Program (BMDO Directive 5205)*
- P. DoD Directive 5210.2, *Access to and Dissemination of Restricted Data (BMDO Directive 5214)*
- Q. DoD 5220.22-M, *Industrial Security Manual*
- R. DoD 5220.22-R, *Industrial Security Regulation*
- S. DoD Instruction 5210.85, *Umbrella Security Classification Guide for High Technology Information*
- T. DoD Directive 5230.9, *Clearance of DoD Information for Public Release*
- U. DoD Directive 5230.11, *Disclosure of Classified Military Information to Foreign Governments and International Organizations (BMDO Directive 5210)*
- V. DoD Directive 5230.24, *Distribution Statements on Technical Documents*
- W. DoD Directive 5230.25, *Withholding of Unclassified Technical Data from Public Disclosure ; SDIO Countermeasures Program Guidance for Distribution Statements on Technical Documents, August 1990*
- X. DoD Pamphlet 5230.25-PH, *Control of Unclassified Technical Data with Military or Space Application*
- Y. DoD Regulation 5400.7-R, *Freedom of Information Act, (BMDO Directive 5400)*
- Z. Joint Pub 1-02, *DoD Dictionary of Military and Associated Terms, 1 December 1989*
- AA. BMD Directive 5204, *Program Protection for BMD Programs*
- BB. SDI-SE Lexicon, January 1989
- CC. Strategic Defense System Glossary, 1 April 1988
- DD. Military Standard 1785, *System Security Engineering Program Management Requirements, 20 June 1988*
- EE. Air Force Space Command Message, date/time group 051457Z April 1989, *Classification of AFSPACECOM Support to SDI Experiments (U)*

- FF. Air Force Space Systems Division course handbook entitled *Managing Security in Systems Acquisition* , 16 July 1989
- GG. *SDI Security Classification Guide*, Directive Number 5230-M, June 1990
- HH. *Low Observable (LO) and Counter Low Observable Programs*, DoD Instruction Number S-5230.28, December 16, 1992

Note: For related security classification guides, consult Section II, Attachment 1, *BMD Security Classification Guide*, Directive Number 5230-M

DISTRIBUTION

Mr. Don Adams, USA PEO/MD	Dr. Greg Foltz, SNL
Dr. Roy Adams, USASSDC	Mr. Russell Foos, SRS
Mr. James Alexander, BMDO/TRS	Mr. James Foshee, USASSDC
Dr. John Allen, Allen Associates	MG Eugene Fox, USA, Ret.
Mr. Jorge Alvarez, PRC	Ms. Teri Frederick, NTF/MST
Ms. Elaine Alspach, USASSDC	Dr. William Frederick, BMDO/TR
Mr. Paul Ammann, SRS	Mr. William French, NAVSEA
Mr. Sonny Anderson, USASSDC	Dr. Barry Fridling, IDA
Mr. Lloyd Apirian, ILT Research Inst.	Mr. Jim Gamble, USASSDC
Mr. Al Aragon, DOE	Mr. Andrus Garay, WSMR
Mr. James Aycock, TBE	Mr. Charlie Garcia, WSMR
Mr. Lynwood Bailey, USA PEO/MD	Mr. Bron Gervais, Booz-Allen & Hamilton
Mr. Robert Balla, USA PEO/MD	Mr. Alexander Gilmore, USA PEO/MD
Mr. Melvin Barefoot, USASSDC	Mr. John Glidewell, USASSDC
Mr. Richard Bartle, Def.Group, Inc.	Dr. Ted Gold, SAIC
CDR Daniel Beach, BMDO/AQQ	Dr. Leon Goure, SAIC
BG Richard Black, USA PEO/MD	Maj, Ronald Graves, BMDO/AQQ
Mr. Mick Blackledge, BMDO/TR	Mr. Sidney Graybeal, SAIC
Mr. Ellery Block, SAIC	Mr. Neil Griff, BMDO/TRD
Mr. Doug Bonforte, BMDO/AQI	COL Walter Grimes, BMDO/TRN
Mr. Lou Bosi, ANSER	Ms. Cheryl L. Gmuer, AMSAA
Capt Steve Burton, 45th RANS/DOR	Mr. Donald Gurney, SPC
Mr. Albino Bustamante, SNL	Mr. Ronald Halahan, USASSDC
Mr. John Canning, NSWC	LTC Alan Hammond, USASSDC
Ms. Kathy Carpenter, USASSDC	COL Allen Hasbrouck, USAADASCH
COL Perry Casto, BMDO/AQQ	Mr. Bruce Haselman, TRW
Dr. Len Caveny, BMDO/TRI	Col Michael Heil, BMDO/DSIM
Ms. Kathy Chaney, ONI	Ms. Gail Heim, SPC
Mr. Mark Chapman, ONI	Mr. Thomas Hill, SAIC
Mr. Miles Clements, Lockheed Martin	Maj Ken Hodgen, PL/VT-B
Dr. Rankin A. Clinton	Mr. Mike Holtcamp, USA PEO/MD
Dr. Donald Coe, MTI/LL	Mr. Andy Hood, ONI
LTC John Como, USA PEO/MD	Mr. James Hood, ANSER
Mr. William Cooper, USASSDC	RADM John T. Hood, PEO for TAD
Ms. Rebecca M. Cowen-Hirsch, JSC/CF	Mr. Andrew Hill, IDA
Mr. David D'Unger	Mr. Thomas Hill, SAIC
Mr. Fred Daum, Raytheon Equip. Div	Capt. Dunning Idle, PL/LIAF
Mr. J. L. Dawson, Pacific MRF	Dr. Charles Infosino, BMDO/AQ
Dr. Lawrence Delancy, Montgomery & Associates	Mr. Howard Irick, USASSDC
Mr. Paul Demmie, SNL/POET	Mr. Dan Jackson, USASSDC
Mr. John Dennis, SPARTA	Mr. Mark Jenkins, B-K Dynamics
Mr. Joseph DeStasio, SMC/MGI	Mr. Charles Jennings, USASSDC
Mr. Pat Duggan, USASSDC	Mr. Mark Jobe, ONI
Dr. Keh-Ping Dunn, MIT/LL	Mr. Max Jones, USASSDC
Dr. Dwight Duston, BMDO/DRI	Cdr Steve Jones, PRC, Inc.
Mr. David Eissler, POET	Mr. Peter Jung, NCCOSC, RDTE Div
Dr. John Ellis, Automated Sciences Group	COL Walter Kilgore, USA PEO/MD
Mr. Keith Englander, BMDO/TRE	Dr. Chuck Kincaid, SAIC
COL Vincent Faggioli, BMDO/DGC	Mr. Bob Kinney, SPARTA
COL Andrew Fallon, BMDO/AQQ	Mr. Alan Klier, Photon Research Associates
Mr. Robert Feldhuhn, AMSAA	Dr. Wade Korngay, MIT/LL

ATTACHMENT 2